Fundamental of Adhoc and Sensor Network

Dr. Jasleen Kaur
Dr. Balkar Singh
Dr. Anuj Kumar
Dr. Ram Paul

Xoffencer

FUNDAMENTAL OF ADHOC AND SENSOR NETWORK

Authors:

- Dr. Jasleen Kaur
- Dr. Balkar Singh
- Dr. Anuj Kumar
- Dr. Ram Paul

Xoffencer

www.xoffencerpublication.in

ISBN-13: 978-81-19534-43-2 (Paperback)

Publication Date: 08 February 2024

MRP: ₹550/-

Published by:

Xoffencer International Publication

Behind Shyam Vihar Vatika, Laxmi Colony

Dabra, Gwalior, M.P. – 475110

Cover Page Designed by:

Satyam soni

Contact us:

Email: mr.xoffencer@gmail.com

Visit us: www.xofferncerpublication.in

Author Details

Dr. Jasleen Kaur

Dr. Jasleen Kaur is working as an Assistant Professor in the Post Graduate Department of Computer Science at Gujranwala Guru Nanak Khalsa College Ludhiana, Punjab, India. She received her Ph.D. degree in Sensor Network from the CT University, Ludhiana, Punjab, India. Her research interests include deep learning, sensor network and information security. She has around 20 years of teaching and 6 years of research experience. She has published 5 research papers in reputed International Journals and Conferences.

Dr. Balkar Singh

Dr. Balkar Singh is working as an Assistant Professor in Post Graduate Department of Computer Science at Gujranwala Guru Nanak Khalsa College Ludhiana, Punjab, India. He received his Ph.D. degree in Image Processing from the Thapar Institute of Engineering and Technology, Patiala, Punjab, India. His research interests include deep learning, image processing, sensor network and information security. He has around 12 years of teaching and 8 years of research experience. He has published 15 research papers in reputed International Journals and Conferences.

Dr. Anuj Kumar

Dr. Anuj Kumar is an Assistant Professor in the Department of Computer Science and Engineering at the School of Engineering and Technology, Sharda University, Uttar Pradesh, India. He holds a Postgraduate Degree (M-Tech in Software Engineering) from G.B.U. G.B.Nagar, and a Doctorate Degree (PhD in Computer Science and Engineering) from A.K.T.U. Lucknow, India. With a strong background in teaching and industry exposure, he is actively engaged in research in the fields of Software Testing, AI, and Machine Learning.

Dr. Ram Paul

Dr. Ram Paul is working as an Assistant Professor at Amity School of Engineering and Technology, Amity University, Uttar Pradesh, Noida. He received his Ph.D. degree in Image Processing from the Thapar Institute of Engineering and Technology (formly Thapar University), Patiala, Punjab, India. His research interests are Digital Image Processing, Machine Learning and Mobile Communication. He completed his M.Tech(CSE) degree from the Guru Jambheshwar University of Science & Technology, Hisar, Haryana, India in 2005. He has around 18 years of teaching and 8 years of research experience. He has published 19 research papers in reputed International Journals and Conferences.

Preface

The text has been written in simple language and style in well organized and systematic way and utmost care has been taken to cover the entire prescribed procedures for Science Students.

We express our sincere gratitude to the authors not only for their effort in preparing the procedures for the present volume, but also their patience in waiting to see their work in print. Finally, we are also thankful to our publishers **Xoffencer Publishers, Gwalior, Madhya Pradesh** for taking all the efforts in bringing out this volume in short span time.

Contents

CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION

The industry dealing with wireless communications has experienced an unprecedented boom throughout the past several years. Thanks to the possibilities of wireless technology, it is feasible to connect with almost every point on Earth's surface from almost anywhere. Hundreds of millions of people use the internet to communicate and exchange data every day. A variety of wireless communication devices, including pagers, mobile phones, laptops, and PDAs, are utilised by these individuals for this purpose. The phenomenal success of wireless phone and message services makes the transition to wireless communication in the realm of personal and corporate computers all the more predictable.

Because there will be no longer be any restrictions imposed by wired networks, people will be able to access and exchange information globally from almost any place they can imagine. Alternatively stated, a Mobile Ad hoc Network (MANET) [Agrawal2002, Cordeiro2002, Perkins2001] is a network that may be instantaneously formed without relying on preexisting infrastructure or additional permanent stations. Put simply, it is a network that can be constructed as needed. To give this argument more structure, we can say that an ad hoc network (abbreviated as "ad hoc") is a self-governing system consisting of mobile hosts (MHs) that act as routers and are linked to each other via wireless connections. The combination of different MHs yields a communication network represented by an arbitrary communication graph.

In contrast, by repurposing base stations (BSs) as access points, the famous single-hop cellular network architecture may meet the needs of wireless communication. That is not the case, though, as was previously stated. The only means for two mobile nodes in a modern cellular network to communicate with each other are through the cable backbone and the fixed base

stations. A MANET lacks this kind of infrastructure, and the topology of the network might alter in an unforeseen way due to its increased dynamic nature, as nodes are free to move around. This is due to the fact that MANETs are more dynamic.

Regarding their mode of operation, ad hoc networks are essentially just peer-to-peer multi-hop mobile wireless networks. As seen in Figure 1.1, these networks are designed to carry data packets using a store-and-forward technique, which involves transferring them from one location to another via intermediate nodes. Packet forwarding over the network does this. Since the MHs are in motion, the other nodes in the network must be informed of the ensuing topological change. This occurs as a result of the MHs' mobility. Because of this, you can choose to keep the old topological data or delete it. When nodes in the network change their point of attachment, like the MH2 node in Figure 1.1 does, from MH3 to MH4, other nodes should utilise this new channel to send packets to the MH2 node.

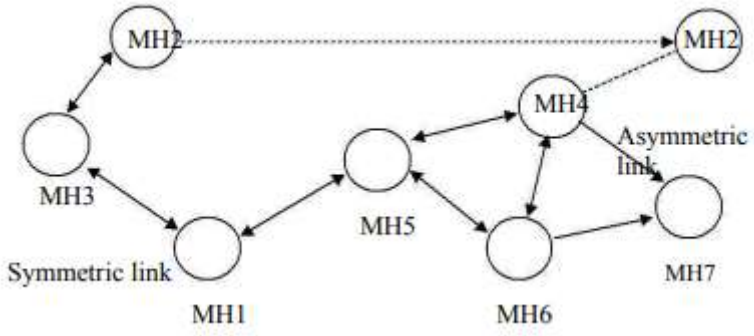

Fig.: 1.1 A mobile ad hoc network (MANET)

Source: Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

Keep in mind that we are assuming, both here and in Figure 1.1, that it is physically impossible to keep all MHs in close proximity to one another. This is the basis upon which we are operating. Without considering any routing issues, we may proceed assumng all MHs are in close proximity and within radio range of each other. In real-life scenarios, the level of power

required to establish complete connection can be challenging, to say the least. And that's not even factoring in limitations like battery life or room for additional use. Situations where a small number of MHs are in radio contact with each other are of special interest to us.

The reason behind this is the rarity of such situations. Figure 1.1 shows an additional problem that develops when differentiating between symmetric (bidirectional) and asymmetric (unidirectional) linkages. In what follows, we'll see that symmetric connections with associative radio range are considered by some of the protocols we'll be talking about. In what follows, we'll see this in action. According to Figure 1.1, this means that if MH1 is inside MH3's radio range, then MH3 must also be within MH1's radio range. Basically, the communication linkages between the two sides are balanced with regard to each other.

Routing in asymmetric networks is notoriously difficult, therefore people often make this assumption even if it's not necessarily true [Prakashl999]. Paths that could obstruct asymmetric linkages can be discovered in certain cases. Of course, these things can't always work out. The reason behind this is because these connections are expected to fail in the near future. Throughout this entire book, we shall presume that all MHs have the same abilities and obligations unless otherwise indicated. For the sake of argument, let's pretend that the entire text is filled with symmetric connections.

behaviour and the transfer of certain physical properties of the area around them to a BS or Sink Node that is linked to them by a connection. As soon as these sensors are placed in a certain environment, they remain there. Furthermore, it is expected that power would be the main motivating factor for protocols designed for these networks. Reason being: sensor longevity is usually dictated by battery lifespan. Because of this, this quality exists. One of the most often mentioned scenarios is the battlefield observation of enemy terrain. In this hypothetical situation, an airliner drops a slew of sensors to the ground to monitor and relay any action happening below. Additional possible economic domains include equipment prediction, biosensing, environmental monitoring, and the condition of important bridges and buildings.

1.2 APPLICATIONS OF MANETS

Using ad hoc networks, one may accomplish a lot of different things. Actually, in a setting typical of an ad hoc network, it should be possible to deploy any application that is utilised often, like email and file transfer. This class of applications includes several examples. As an additional option, you can provide web services if any node in the network can act as an external gateway. I can see how this could work.

No special emphasis on the many potential military uses of ad hoc networks is required for the purposes of this presentation. Not only that, but the technology was originally built with the intention of being used in military applications, like in uncharted regions of the battlefield where it would be extremely difficult to build or maintain an infrastructure network.

Ad hoc networks with the ability to self-organize can be useful in situations like these, when traditional technologies are either not applicable or cannot be implemented effectively. More and better features of mobile wireless networks are opening the door for new kinds of apps to be created. The capacity to go across international borders, interact with a variety of network topologies, and access data at rates suitable for multimedia applications are all examples of these capabilities. Popular uses of ad hoc networks include the ones listed below:

- Collaborative Work - The need for collaborative computing may be more important for some business environments that are located outside of the office than it is for those contexts that are located within the office. As a matter of fact, it is frequently the case that individuals are forced to attend events that are hosted by third parties in order to cooperate and share information on a certain project. Applications that are considered to be those that fall under the category of crisis management are those that arise, for example, as a result of natural disasters that cause the whole communications infrastructure to be in a state of disarray.
- It is unequivocally essential that communications be restored as quickly as possible. It is feasible to construct an infrastructure in a matter of hours by employing ad hoc networks, as compared to the days or weeks that are required for wire-line connections.

- Personal Area Networking and Bluetooth — Personal area networks and Bluetooth are two examples of wireless technologies. One type of network that falls under the category of a localised, short-range network is a personal area network, which is also commonly referred to as a PAN. In this type of network, nodes are generally connected with a particular person. It may be possible to attach these nodes to a person's pulse watch, belt, or other objects that are analogous to these accessories. When it comes to these circumstances, mobility is only a crucial aspect to take into consideration when it is required for a large number of PANs to interact with one another.
- Here is an illustration of a scenario in which people come into contact with one another in real life. Bluetooth, which was initially presented by Haarsten in the year 1998, is a technology that eliminates the requirement of wires in order to connect a wide range of electronic devices. These devices include printers, personal digital assistants (PDAs), laptop computers, digital cameras, and many more. The fundamental purpose of this initiative is to make the use of personal area networks (PANs) easier.

1.3 ROUTING IN A MANET

It is now quite obvious that classic routing on physically structured networks and MANET routing are radically different. Topology, router selection, and request beginning points are only a few of the MANET routing features that rely on a certain underlying feature that can serve as a heuristic for efficiently determining the path. A few examples of these factors include the topology, the starting of requests, and the selection of routers. We need to maximise the use of these networks' limited resources because there are only so many of them.

Because of this, finding the best possible routing in ad hoc network design is a top priority. The already severe limitations of routing protocols tailored to these networks are further exacerbated by their extremely dynamic character. The current focus on protocols aiming to provide routing stability is mostly motivated by this need. One of the biggest problems in developing a routing protocol [Jubin 1987] for ad hoc networks is the frequent topological

changes that might occur. This is because, in an ad hoc network, the topology might vary rather often, and, on the one hand, a node has to know the reachability information to its neighbours in order to choose a packet path.

This explains why the structure of a network may shift regularly. Due to the potentially enormous number of nodes in the network, routing control information must be sent frequently and in great quantities in order for the destinations to be chosen. This is due to the fact that there may be a large number of nodes in the network. Because of this, there could be a lot of update traffic, and it might get much worse in cases when nodes are very mobile. Corson (1996) states that high mobility nodes might potentially affect routing techniques' route maintenance overhead to the point that data packet transmission capacity is exhausted. I can see how this could work.

1.4 PROACTIVE AND REACTIVE ROUTING PROTOCOLS

There are mainly two ways that ad hoc routing techniques may be categorised. Proactive, sometimes called table-driven, and reactive, often called on-demand, are two of them. Nodes in a MANET are required by proactive protocols to maintain a complete list of all potential destinations. This means that the route may be quickly and easily employed whenever a packet has to be forwarded. Because the path has already been mapped out. This ensures that the intended destination may be reached trouble-free. In contrast, nodes in reactive protocols wait to discover routes to destinations until asked to do so.

This means that a node can send data packets without a route to a destination unless the destination is going to receive them. Reducing a node's latency when a route is required is a benefit of proactive protocols. One advantage of proactive procedures is this. Reason being, there is no waiting time required when a route is chosen from the routing database. However, proactive protocols aren't always the best choice because they frequently use a lot of network resources to keep the most up-to-date routing information. Because of this, preemptive practices aren't necessarily the way to go.

In contrast, reactive procedures wait until it is absolutely necessary to determine a route to a target before doing so. Why? Because it is the very nature of reactive protocols. Since this is the case, they may triumph over this obstacle. Compared to proactive protocols, the delay to find a route could be substantially larger. Finding a path to a destination before real communication occurs is sometimes a major latency for reactive protocols. Conversely, proactive protocols typically consume far more bandwidth than reactive protocols. We may, in short, conclude that there is no procedure that is suitable for all of the potential situations, even if there have been many suggestions that employ a hybrid method.

1.4.1 Destination-Sequenced Distance-Vector Protocol

In his description of proactive hop-by-hop distance vector routing techniques, Perkins (1994) outlines the destination-sequenced distance-vector (DSDV) protocol. As a result of this protocol, all nodes must regularly broadcast any changes to the routing of the network. In this scenario, each mobile node in the network is tasked with maintaining a routing table that details all the potential destinations inside the network and the number of hops needed to reach each one. Every single item has a unique sequence number that has been sent down from the node that acts as the destination. The mobile nodes are able to differentiate between previously used and newly created routes thanks to the sequence numbers.

This aids in avoiding the process of routing loop development. To ensure that the routing table always has the same information, it is critical to consistently update it across the whole network. When updating a route, you have two options: whole dumps or tiny increment packets. You can swap out one sort of packet for the other. To lessen the possible deluge of traffic caused by network changes, this measure is implemented. A full dump packet may need a significant number of network protocol data units (NPDUs) since it comprises all of the currently available routing information.

During periods of inconsistent movement, these packets are only sent very infrequently. They are only transmitted at this time. In order to transmit just the data that has changed since the

last complete dump, smaller incremental packets are utilised. In order to guarantee the correct transmission of the data, this is done. Because each of these broadcasts should fit inside a standard-sized NPDU, the quantity of traffic should be reduced. The mobile nodes keep a second table open so they may store the data sent in incremental routing information packets. Included in this table is the transferred data.

Along with the destination's address and the number of hops needed to get there, new route broadcasts also include the sequence number of the received information at the destination as well as a new sequence number that is specific to the broadcast. In every case, the route with the most current sequence number is always seen to be the best one. If the sequence numbers of two updates are identical, the one with the smaller metric will be picked for optimisation (to reduce the path). The goal is to make things go more quickly. The goal is to maximise efficiency, therefore that's how it's done.

Also, until the route with the best metric is reached, mobile devices record the settling time of the routes. This is also called the weighted average time that routes to a location might vary. One more thing that mobile gadgets keep an eye on. By avoiding transmissions that would be sent out if a better route could be found soon, mobiles can reduce network strain and enhance routes. A routing update can be postponed during the settling time, allowing for this to happen. This feature reduces the amount of traffic that is transmitted across the network.

The fact that every node broadcasts its own sequence number, which is rising in a regular manner, should be carefully noted. By using an infinite metric and a sequence number that is one more than its sequence number for the broken route, node B will advertise the route to D with an odd sequence number when it finds that its route to D has broken. The result is that the sequence number will be divisible by two. This is what happens when things are done this way. This means that every single node A that uses B as a routing intermediate will have the infinite-metric route stored in their routing database. This will keep happening until node A receives a route to node D with a higher sequence number (SERV).

1.4.2 The Wireless Routing Protocol

The Wireless Routing Protocol (WRP) was introduced by Murthy in the year 1996. It is a table-based protocol that was designed with the intention of preserving routing information across all of the nodes in the network. This protocol was developed with the purpose of resolving the issue of storing routing information, which was a problem that needed to be solved. These four tables are the Distance table, the Routing table, the Link-cost table, and the Message Retransmission List (MRL) table. Each node in the network is responsible for maintaining these four tables.

This task of maintaining these four databases has been assigned to each node in the network. An acknowledgment-required flag vector with one item per neighbour is included in each entry of the MRL. Additionally, the sequence number of the update message is included, as well as a list of updates that were communicated in the update message. In addition, the precise sequence number of the update message is included in each individual item. The fact that the MRL is equipped with a retransmission counter is an extra feature of the device. At the same time as it is the responsibility of the MRL to keep track of the changes that are included inside an update message that needs to be resent, it is also the role of the neighbours to acknowledge the communication that has taken place. It is possible for mobile devices to establish a connection with one another via the use of update messages.

This allows the devices to remain informed of any modifications that may be made to the linkages. An update message is not only delivered between nodes that are located in close proximity to one another, but it also contains a list of answers that designate which mobiles should acknowledge (ACK) the update. In addition, an update message is only sent between nodes that are in close proximity to one another. The destination, the distance to the destination, and the destination that came before the destination are all included in the list of updates that consists of this. When a mobile device has digested updates from other neighbours or discovered a change in a link, it will send an update message to a neighbour.

This occurs when the mobile device sends an update message. This happens once the mobile device has noticed the modification that has occurred. If a link between two nodes is lost, the nodes will utilise update messages to engage with their neighbours in order to keep communication going. This will ensure that communication is maintained. Following the completion of this task, the neighbours will make the appropriate modifications to the entries in their distance table and will seek for alternate pathways that are feasible and that pass via other nodes in a different sequence. Information on any newly detected pathways is sent to the nodes that were first constructed so that they can be able to make the necessary adjustments to their tables.

This is done in order to maintain the integrity of the network. When nodes receive acknowledgments and other signals, they become aware of the presence of their neighbours. This information is sent to them. It is the input that they receive that has brought about this awareness. It is vital for a node to send a welcome message within a specified amount of time in the event that it is not transmitting messages. This is done in order to guarantee that the node will continue to be connected to the network. It is possible that a false alarm will be triggered as a consequence of the failure of the connection in question, which is demonstrated by the lack of signals from the node in addition to the absence of any other symptoms.

When a mobile device gets a hello message from a new node, the routing table of the mobile device is modified to incorporate the message from the new node. At the moment when the user receives the message, this takes place. A copy of the information that is contained inside the mobile device's routing table is also transmitted to the new node. This is in addition to the previous explanation. It is conceivable to attribute a large portion of the originality of WRP to the way in which it makes it possible to break out of loops. This is something that can be determined empirically.

Routing nodes are the nodes in wireless networks that are responsible for transmitting information about the second-to-last hop for each destination, as well as the distance between

the two points. The Wireless Routeing Protocol (WRP) is the entity that is responsible for carrying out this obligation. There is a substantial disadvantage associated with the WRP algorithm, which is a member of the family of algorithms that are used to find routes. It is essential to keep this fact in mind.

The "count-to-infinity" difficulty may be circumvented by requiring that every node do consistency checks on the predecessor information that is provided by all of its neighbours. This allows it to circumvent the predicament. The difficulty can be sidestepped as a result of this. Two results that result from this enhancement are the removal of looping situations and the provision of quicker route convergence in the event that a connection fails. Both of these outcomes are consequences that follow from this improvement. This is not something that happens instantly, which is a crucial point to keep in mind.

1.4.3 The Ad Hoc On-Demand Distance Vector Protocol

Since its inception in 1999 by Perkins, the Ad Hoc On-Demand Distance Vector (AODV) routing system has essentially combined the DSDV and DSR protocols. Data routing via the internet made use of this technique. From DSR, Route Discovery and Route Maintenance draw their basic on-demand mechanism. In addition, it uses DSDV-obtained hop-by-hop routing, sequence numbers, and periodic beacons. You may thank DSR for providing all of these components. By generating routes on demand, the AODV algorithm reduces the amount of broadcasts needed, in contrast to the DSDV algorithm that keeps a complete list of routes.

In turn, this allows AODV to reduce the quantity of transmissions needed. The creators of AODV defined it as an on-demand route acquisition system as nodes that aren't part of a certain path don't keep routing data or take part in routing table exchanges. Their failure to retain routing information is the reason for this. Only symmetric linkages consisting of two distinct phases can be enabled, to the best of its ability:

- Route Discovery, Route Maintenance; and

- Data forwarding.

A source node will start a path discovery operation to find the node that matches the message if it wants to deliver the message but doesn't already have a valid route to the destination. To make sure the message is sent, this is done. Following broadcasting the route request (RREQ) packet to its neighbours, those neighbours will retransmit the request to their neighbours, and the process continues thereafter in the same manner. Until the final destination or an intermediate node with a "fresh enough" path to it is found, the procedure will keep running. This process is carried out again and again till the previously indicated location is found. You can see this in action in Figure 3(a), which displays the distribution of the sent RREQs throughout the network.

In order to guarantee that all routes are up-to-date and error-free, AODV use destination sequence numbers. Make sure there are no loops in any of the paths to achieve this. Nodes are also required to keep track of their own sequence numbers in addition to broadcast IDs. Each RREQ may be uniquely identified when the broadcast ID is combined with the node's IP address. The reason behind this is that the node updates the broadcast ID for every RREQ it begins. In addition to the node's sequence number and broadcast ID, the RREQ also contains the destination's most recent sequence number. The RREQ has this information. Answers to the RREQ can be provided by intermediate nodes if their routes to the destination have destination sequence numbers that are equal to or greater than the ones included in the RREQ.

This is the sole need for their ability to do so. Whenever an intermediary node forwards an RREQ, it adds a note to its route table. The original sender's address of the broadcast packet is included in this record. This establishes a path that connects the two nodes in the inverse direction. If further copies of the same RREQ are received at a later time, the relevant packets might be destroyed. In response to an RREQ, the receiving node will send a route reply (RREP) packet back to the sending node as soon as it reaches the destination or an intermediate node with a recent enough route.

The final or intermediate node can then talk to its neighbour in this way. Nodes along this path will create entries in their route tables that are related with the forward route entry while the RREP is being routed backwards. The RREP's original source node should be mentioned in these entries. There is a depiction of the forward route that is currently in use for each of these entries. There is a route timer in the system that is associated with each route's entry. Once the allotted lifespan has elapsed, this timer will remove the object if it remains unused for that long. Since the RREP is sent along the route specified by the RREQ, AODV can only be used with symmetric networks and not with any other ones.

The following is the procedure for route maintenance. The source node can theoretically identify a new path to the destination by restarting the route discovery protocol if it moves physically. An alternate route to the destination can then be discovered by the source node. The upstream neighbour of a moving node along the route will be the first to know about the change and will notify all of its active upstream neighbours of the connection failure (an RREP with unlimited metric). The route's continued functional operation depends on this. This notification will inform them that the damaged section of the road was recently destroyed. The process will keep going until the nodes reach the source node. Once they do, they will notify their neighbours farther upstream of the connection failure.

At that moment, the source node might choose to begin the route discovery process all over again for that destination if having a route is still desirable. There is an extra part to the protocol that is called welcoming messages. A node transmits periodic local broadcasts in these messages. Each mobile node will be notified of other nodes in its immediate vicinity through these messages. One way to maintain a node's local connection is to send out welcome messages at regular intervals. The usage of welcome messages may not be necessary in all cases, though.

In order to determine if the next hop is still reachable, nodes monitor for the retransmission of data packets. If the subsequent retransmission is still not received, the node can check if the

next hop is within its communication range using a number of methodological strategies, including sending its own welcome messages. And it's not out of the question that the welcome messages may also include a rundown of all the nodes that a mobile node has lately received messages from. This would lead to a better understanding of the mobile nodes' network connectivity.

1.5 ROUTING USING LOCATION INFORMATION

Several ad hoc routing methods that make use of some type of location information in the process of routing will be discussed in the next section of this article.

1.5.1 Location-Aided Routing

The AODV protocol is an example of a system that uses location data to limit the reach of a route request flood. Take the DSR procedure as another illustration. The Location-Aided Routing (LAR) protocol, which was released in 1998, was developed using this information. One way to gather such location-based data is via making use of the Global Positioning System (GPS). When a route is found, a so-called request zone is built using the expected location of the last node. With this expected location in hand, LAR narrows the route search to the request zone.

The Expected Zone and the Request Zone are two ideas that must be understood in order to fully grasp how LAR works. Thus, let's begin by defining exactly what an Expected Zone is. Imagine that node S has the responsibility of finding a route from the network to node D. Assume for the sake of argument that node S knows that node D was at location L at time t0 and that the current time is t1. The "expected zone" of node D is the area that, from node S's perspective at time t1, is thought to encompass node D. For the simple reason that this area is likely to include node D. Since node D was known to be at position L at time t0, node S may use this information to compute the predicted geographic area. Node S is able to make this conclusion with the use of these information.

The expected zone may be the spherical area with a radius of v (t1 - t0), with the centre of the area at point L (see Figure 7(a)), for example, if node S knows that node D moves at an average speed of v. This is due to the fact that the position of the node L determines the location of the region's centre. When the actual speed is greater than the average speed, it's possible that the destination is located outside of the projected zone at time t1. Based on this, the projected zone is just an approximation made by node S to find a region that potentially include D at time t1. Node S cannot correctly determine the expected zone without knowledge of node D's prior location.

The reason behind this is that node S is unaware of where node D is located. This is because it is commonly assumed that the ad hoc network will occupy the whole territory that it is capable of. Given these circumstances, it's feasible to reduce LAR to its most basic flooding algorithm. In a general sense, a smaller predicted zone at the destination might be the outcome of having more knowledge about the mobility of a destination node. Figure 1.2(a) depicts the circular predicted zone; however, in Figure 1.2(b) we see a reduction to a semicircle when S knows that destination D is going northerly. This is because there is less room in the semicircle depiction of the expected zone.

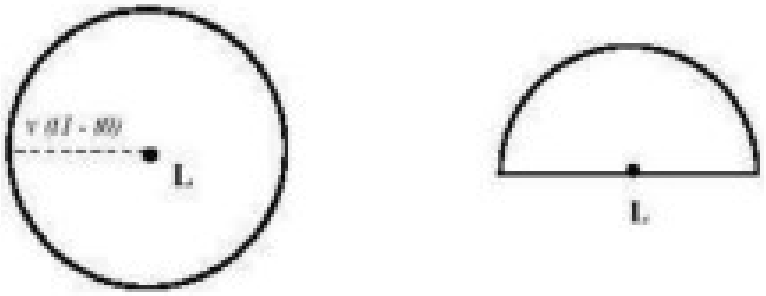

Fig.: 1.2 Examples of expected zone(a) (b)

Source: Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

We can define the request zone based on the expected zone, or we can use a different approach. Consider the case of node S, which has been assigned the task of finding a way to node D. Those LAR algorithms that were proposed use the flooding method with one tweak. Whether done explicitly or implicitly, Node S can build a request zone for the route request. An important difference from the flooding method used by AODV and DSR is that nodes will only transmit route requests if they are members of the request zone. The flooding process is different from this. If you want your route request to go to node D more often, you need make sure that the request zone includes the expected zone, which was discussed in the previous section.

Another potential scenario is that the request zone encompasses other locations that are geographically nearby. With that said, the given information allows source node S to identify the four corners of the predicted zone. Prior to sending out the route request message to initiate the route discovery process, S incorporates these coordinates. Once a node gets a route request, it disregards the request if it's not inside the rectangle that the request contains. The four corners specified in the route request constitute the rectangle. For example, in Figure 1.3, node I will communicate with its neighbours in order to receive route requests. This is because it will detect that it is within the rectangle request zone.

Plus, it'll ask its neighbours for help, so it's certain to happen. Nevertheless, node J fails to respond to the route request as it is outside the request-allocated zone (refer to Figure 8). This is why we have not responded to your request. That approach, LAR scheme 1, was just recently described and goes by that name. The route request packet contains two bits of information that are part of the LAR scheme 2. The original plan was very different from this, so this is a tiny tweak. When node S knows node D's position (Xd; Yd) at time t0, it begins the route discovery process at time t1, where t1 is greater than or equal to t0.

So long as node S knows where node D is, everything will be OK. The distance between Node S and the given location (Xd; Yd) is computed and included in the route request message. This

geographical distance is represented by the symbol DISTS. The route request packet also includes the specifications (Xd, Yd) that were transmitted. If node J is closer to (Xd; Yd) than node I, it will transmit a route request that was originally submitted by node I (from node S). This holds true if the predicted distance from the given node J is within the given range. A portion of the route request includes this data.

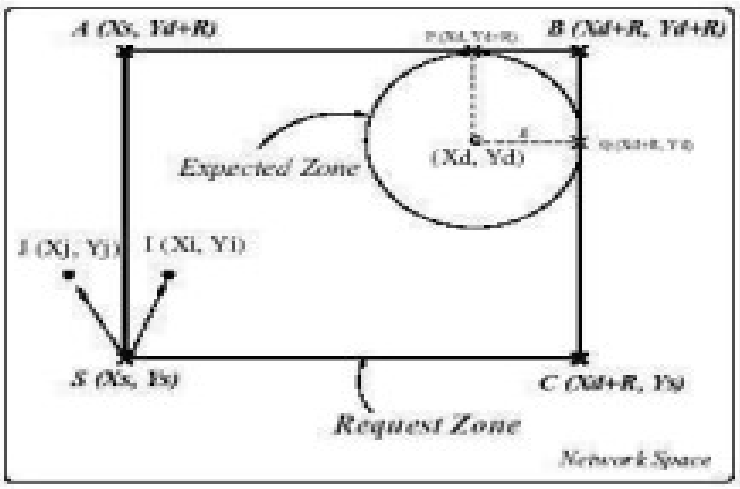

Fig.: 1.3 LAR scheme

Source: Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

1.5.2 Relative Distance Micro-Discovery Ad Hoc Routing

One particularly adaptable, efficient, and scalable routing protocol is the RDMAR (Relative Distance Micro-Discovery Ad Hoc Routing) system. The passage makes this clear. This method works well in settings where topological changes occur at a slower rate, such as big mobile networks. When a connection fails, the protocol's response is often limited to a narrow area close to the affected node. When thinking about the protocol's architecture, this is a crucial idea. This optimal behaviour is achieved via the employment of a unique route-finding technology called Relative Distance Micro-discovery (RDM).

The core idea behind RDM is that the relative distance (RD) between two terminals may be used to pinpoint the exact location of a query flood. The rationale for RDM has always rested on this notion. This primary concept forms the basis of the RDM approach. They estimate their RD using an iterative technique that is applied to each route search between the two destinations. The purpose of this action is to achieve the stated objective. Aside from the time that has passed between the person's last conversation and their past RD, this method also takes into account an average nodal mobility.

Then, the calculated relative distance determines the maximum propagation radius, which is used to constrain the query flood to a certain region of the network centred at the originating node of the route discovery. The area is subsequently pinpointed. The recently decided RD dictates this procedure.

By making use of this capability, which allows the localization of query flooding into a specific area of the network, both the overall congestion and routing overhead may be reduced. Utilising RDMAR allows calls to be routed through the network's stations. Every node in the network maintains its own routing table, which is used to do this.

Each node in this system serves as both a host and a store-and-forward node simultaneously. Every single routing table has a complete inventory of all the possible destinations. Furthermore, for every single destination i, there is supplementary routing data provided. The "Default Router" field estimates the number of hops between the node and i, while the "RD" field shows the current hop node of the current node.

In addition, the "RD" field shows the current hop node of the current node. This encompasses all of these domains. Three fields are present: the "Time_Last_Update" (TLU) field, which indicates the duration since the node last received routing information for i; the "RT_Timeout" column, which keeps track of the duration until the route is deemed invalid; and the "Route Flag" field, which indicates if the route to i is active or not.

1.5.3 RDMAR comprises of two main algorithms:

- If an incoming call arrives at node i for destination node j and there is no route that can be accessed, then I will initiate a phase of route discovery immediately. The occurrence of this occurs when there is no available path. In this scenario, I have two options available to me: either I can flood the network with a route inquiry, in which case the route query packets will be broadcast into the entire network, or I can choose to confine the discovery to a smaller part of the network, provided that some kind of position prediction model for j can be created. Both of these options are available to me. It would appear that the first case is not overly complex.
- The latter situation involves the source of the route discovery, which is symbolised by the letter i, consulting its routing database in order to get information on its previous relative distance with j as well as the length of time that has elapsed since the last time that I was given with routing information for j. During this particular instant, we are going to refer to it as the tmotion. Node i is now able to estimate its new relative distance to destination node j in terms of the real number of hops based on this information and assuming a moderate velocity, Micro Velocity, and an acceptable gearbox range, Micro Range. This has been accomplished by assuming that the number of hops is the actual number of hops. In order to do this, it is appropriate to assume that both the velocity and the gearbox range are reasonable. Node i is responsible for doing the computation of the distance offset of DST (DST_Offset) during tmotion. Subsequently, it "adjusts" the result onto their previous relative distance (RDM_Radius). It is because of this that the node is able to achieve the intended result.
- When a data packet is received by an intermediate node i, the node first performs an evaluation of the routing header, and then it subsequently transmits the packet to the subsequent hop. This type of maintenance is referred to as "route maintenance."

Further, in order to determine whether or not it is feasible to establish a link that is bidirectional with the node that came before it, node i sends a message that is explicit.

- This is done in order to study the possibility of doing so. In light of this, RDMAR does not make any assumptions about the presence of bi-directional linkages. On the other hand, nodes are permitted to investigate the possibility of having such ties. This guarantees that nodes that are responsible for forwarding a data packet will always have the appropriate routing information to transmit the following acknowledgement back to the source regardless of whether or not they are responsible for forwarding the packet. In the event that node i is unable to forward the packet due to the absence of a route that is available or if a forwarding error occurs along the data path as a consequence of a failure in either the link or the node, I have the ability to attempt a number of additional re-transmissions of the same data packet, up to a maximum number of retries. This ability allows me to try a maximum number of times. Additionally, in the case that the failure continues to occur, the node i will initiate a procedure for Route Discovery.

1.6 CHARACTERISTICS OF MANET

Let's have a look at some of the characteristics of MANET:

1. Because nodes are free to move in any direction, the topology of the network is able to alter at any time and is mostly composed of bidirectional links. This has the effect of making the network more adaptable to changing circumstances. There is a possibility that a unidirectional link will manifest itself under circumstances in which the transmission power of two nodes is different from one another.
2. The capacity of wireless links continues to be much lower than that of infrastructure networks. This is due to the fact that bandwidth is limited and the capacity of wireless links might vary.

3. Batteries and other non-renewable sources can be utilised to power a portion or all of the nodes in a MANET as potential sources of power. This type of operation is referred to as energy-constrained operation. When it comes to the optimisation of system design for these nodes or devices, it is probable that the conservation of energy is the most significant criterion to consider.
4. When it comes to attacks on their physical security, MANETs are frequently more vulnerable than wireline networks are to being attacked. Due to the fact that MANETs have little physical protection, this is the case.
5. In light of the heightened risk of eavesdropping, spoofing, and denial of service (DoS) attacks, it is essential to conduct a comprehensive study into the matter. Wireless networks often make use of a broad variety of link security solutions that are currently in existence. This is done with the intention of reducing the number of security concerns with wireless networks.
6. Less Human interaction: They are believed to be dynamically autonomous due to the fact that they require just a little amount of human interaction in order to configure the network.

1.7 ADVANTAGES OF MANETS

1. The fact that any node in the network is capable of performing the functions of both a router and a host is an illustration of the network's autonomous capability.
2. Separation from the central network administration.
3. Has a capacity that is very expandable and is extremely compatible with the installation of new network hubs.
4. Nodes that are capable of self-configuring and self-healing do not require interaction from a person in order to function without human intervention.
5. Since MANETs are decentralised networks, it is not required to have infrastructure in place. This is because MANETs run without a central authority.

6. Because of the multi-hop approach that is used in the process of information transmission for decentralised networks, decentralised networks are frequently more trustworthy than centralised networks. This is because of the fact that decentralised networks employ this method. In the event that a base station in a cellular network fails to function properly, for example, coverage is lost. If, on the other hand, data may travel across several channels, the danger of a single point of failure in a MANET is considerably decreased. This is because of the fact that the MANET is a distributed network.
7. There are a number of advantages that mobile ad hoc networks (MANETs) offer in comparison to fixed-topology networks. These advantages include flexibility (mobile devices can be used to construct an ad hoc network anywhere), scalability (you can simply add additional nodes to the network), and reduced maintenance costs (there is no need to build infrastructure beforehand).

1.8 DISADVANTAGES OF MANETS

- There are no facilities for authorization.
- Noise and interference problems, among others, limit the available resources.
- They are more susceptible to assaults because of insufficient physical protection and have high latency, which means data transfers between two sleeping nodes take a long time.

1.9 APPLICATIONS OF MANETS

Using ad hoc networks, one may accomplish a lot of different things. The reality is that in an ad hoc network setting, it is possible to roll out any commonly used application, including email and file sharing. This is how things really stand. As an additional option, you can provide web services if any node in the network can act as an external gateway. I can see how this could work. No special emphasis on the many potential military uses of ad hoc networks is required for the purposes of this presentation.

One of the initial locations where the technology was built with the goal of being utilised by the military was on a battlefield in a foreign nation, where it is nearly hard to build or maintain an infrastructure network. This does not even take into account the fact that the technology was first created. Ad hoc networks with the ability to self-organize can be useful in situations like these, when traditional technologies are either not applicable or cannot be implemented effectively. More and better features of mobile wireless networks are opening the door for new kinds of apps to be created. The capacity to go across international borders, interact with a variety of network topologies, and access data at rates suitable for multimedia applications are all examples of these capabilities. This is yet another famous instance of an ad hoc network.

Applications are:

- Collaborative Work - The need for collaborative computing may be more important for some business environments that are located outside of the office than it is for those contexts that are located within the office. As a matter of fact, it is frequently the case that individuals are forced to attend events that are hosted by third parties in order to cooperate and share information on a certain project. Applications that are considered to be those that fall under the category of crisis management are those that arise, for example, as a result of natural disasters that cause the whole communications infrastructure to be in a state of disarray. It is unequivocally essential that communications be restored as quickly as possible. It is feasible to construct an infrastructure in a matter of hours by employing ad hoc networks, as compared to the days or weeks that are required for wire-line connections.

- Personal Area Networking and Bluetooth — Personal area networks and Bluetooth are two examples of wireless technologies. In general, a personal area network, sometimes referred to as a PAN, is a localised network that functions over a restricted distance and typically consists of nodes that are linked with a single unique individual. There

is the potential to establish a connection between these nodes and a person's pulse watch, belt, or other such possessions.

- When it comes to these circumstances, mobility is only a crucial aspect to take into consideration when it is required for a large number of PANs to interact with one another. Here is an illustration of a scenario in which people come into contact with one another in real life. Bluetooth, which was initially presented by Haarsten in the year 1998, is a technology that eliminates the requirement of wires in order to connect a wide range of electronic devices. These devices include printers, personal digital assistants (PDAs), laptop computers, digital cameras, and many more. The fundamental purpose of this initiative is to make the use of personal area networks (PANs) easier.

Education via the internet: Educational possibilities are available on the internet or in remote locales due to the practical difficulty of providing pricy last-mile wireline internet connectivity to all people in these areas.

Virtual Navigation: A database situated at a distant location visually represents the physical features of a large metropolitan area, including its buildings, roadways, and other physical components. Not only that, but users may be able to "virtually" examine a building's interior layout—which may include an evacuation plan—or find potential points of interest.

Vehicular area network (VANETs): Ad-hoc network applications are becoming increasingly important, and this one is one of them. Its objective is to give information and emergency assistance. This is something that works just as well in urban as it does in rural settings. In a given scenario, the transmission of knowledge that is critical and necessary.

Limited Bandwidth: Be aware that wireless networks have substantially less bandwidth than their wired counterparts. The capacity of infrastructure communications networks is significantly higher than that of wireless lines. Because the maximum radio transmission rate

is so high in ADHOC networks, fading, numerous accesses, and interference situations have a negligible effect. The high transmission rate of ADHOC networks is the reason behind this.

Dynamic topology: As a consequence of the dynamic topology, the degree of truth that exists between the nodes is reduced. It is also conceivable that the degree of confidence will be brought into question if it is revealed that there is some sort of settlement between the nodes being discussed.

High Routing: As a result of the dynamic topology of ADHOC networks, particular nodes have the ability to change their position, which in turn has an effect on the routing table itself.

Problem of Hidden terminal: The collision of the packets is allowed to continue because of the transmission of packets by those nodes that are not in the direct transmission range of the sender side but are in the range of the receiver side. This is the reason why the collision of the packets is held.

Transmission error and packet loss: As a consequence of an increase in the number of collisions, disguised terminals, interference, and uni-directional connections, as well as those of frequent route disruptions caused by the mobility of nodes, ADHOC networks have seen a greater loss of packets. This has led to a bigger amount of packets being lost.

Mobility: This is due of the dynamic behaviour of the network as well as the changes in the topology that are brought about by the migration of the nodes from one location to another. There is a high probability that ADHOC networks may have path breaks, and the route will also be subject to modifications on a frequent basis.

Security threats: Considering that ad hoc networks are wireless in nature, there are additional security considerations that need to be addressed. The administration of trust between nodes in ad hoc networks or wireless networks is the fundamental reason for the numerous security breaches that take place in these kinds of networks.

1.10 SOME OTHER MAJOR CHALLENGES IN MANET

The following is a quick description of some other issues that the MANET faces:

Dynamic topologies: A Dynamic Topology allows any and all nodes to freely travel in any direction they want. The structure of a network might undergo sudden and unexpected shifts over time. There may be both bidirectional and unidirectional routing setups, and it's likely that this design is to blame. Given that topologies are in a continual state of flux, packet transfer among nodes is a challenging task.

Multicast Routing: The addition of multicast is only one more obstacle that MANET must overcome. One possible explanation for the ever-changing structure of the multicast dynamic network is the random location changes made by the nodes inside it. Not only is it confusing, but there are much more hops than a single hop between any two nodes. If the new device wants the network to perform properly, it has to know which nodes are already there. Due to the presence of nodes, it is crucial to provide dynamic updates to enable fully autonomous route selection.

1.11 VARIABILITY IN CAPACITY LINKS DUE TO BANDWIDTH CONSTRAINT

Being a link of wireless, they continue with low capacity in comparison to the hardwired.

1.11.1 Power-constrained and operation

Within the context of the MANET network, this is also seen as a problem. The MANET network's nodes rely on a depletable energy source, such as batteries, to power its operations. The MANET is a defining feature of this network type. An integral aspect of the system's design is the optimisation of energy conversion, which is the criterion. Using as little electricity as possible is another benefit of using lightweight mobile terminals. Additional considerations that should be given due weight include power saving and the introduction of power-aware routing.

1.11.2 Security and Reliability

The usage of Nasty Neighbour for packet relaying, along with its inherent weaknesses, is another security risk. There is a plethora of approaches to authentication and key management in distributed operations. One more thing about wireless networks is their reliability issues. The fact that wireless communication has its limitations is what causes these complications. The risk of data corruption or loss is inherent in the transfer of packets across wireless media. Despite widespread belief to the contrary, wireless networks are far more vulnerable to intrusion attempts than their wired counterparts. When it comes to security breaches, wireless networks are more vulnerable.

1.11.3 Quality of Service

Due to the ever-changing nature of the environment in a MANET, it will be challenging to maintain consistent quality of service standards. It will be difficult for the person in charge of the network to handle this. It is challenging to provide a reasonable guarantee of service for the device due to the fact that MANET communication quality is unpredictable. This makes it hard to provide a solid service guarantee. By substituting adaptive Quality of Service for more traditional resources, multimodal service provisioning becomes possible.

1.11.4 Inter-networking

In many instances, it is also anticipated that MANET would communicate with fixed communication networks. When it comes to the administration of pleasant mobility, the presence of routing protocols in both networks presents a very challenging situation.

1.12 PROACTIVE AND REACTIVE ROUTING PROTOCOLS

There are mainly two ways that ad hoc routing techniques may be categorised. Proactive, sometimes called table-driven, and reactive, often called on-demand, are two of them. The route may be promptly utilised when a packet has to be sent since proactive protocols require

MANET nodes to maintain a record of all possible destinations. Because the path has already been mapped out. As a result, this ensures that the route may be used immediately whenever necessary.

In contrast, nodes in reactive protocols wait to discover routes to destinations until asked to do so. This means that a node can send data packets without a route to a destination unless the destination is going to receive them. Reducing a node's latency when a route is required is a benefit of proactive protocols. One advantage of proactive procedures is this. Reason being, there is no waiting time required when a route is chosen from the routing database. However, proactive protocols aren't always the best choice because they frequently use a lot of network resources to keep the most up-to-date routing information. Because of this, preemptive practices aren't necessarily the way to go.

In contrast, reactive procedures wait until it is absolutely necessary to determine a route to a target before doing so. Why? Because it is the very nature of reactive protocols. Since this is the case, they may triumph over this obstacle. Compared to proactive protocols, the delay to find a route could be substantially larger. Finding a path to a destination before real communication occurs is sometimes a major latency for reactive protocols. Conversely, proactive protocols typically consume far more bandwidth than reactive protocols. We may, in short, conclude that there is no procedure that is suitable for all of the potential situations, even if there have been many suggestions that employ a hybrid method.

1.13 DESTINATION-SEQUENCED DISTANCE-VECTOR PROTOCOL

In his description of proactive hop-by-hop distance vector routing techniques, Perkins (1994) outlines the destination-sequenced distance-vector (DSDV) protocol. As a result of this protocol, all nodes must regularly broadcast any changes to the routing of the network. In this scenario, each mobile node in the network is tasked with maintaining a routing table that details all the potential destinations inside the network and the number of hops needed to reach each one.

Every single item has a unique sequence number that has been sent down from the node that acts as the destination. The mobile nodes are able to differentiate between previously used and newly created routes thanks to the sequence numbers. This aids in avoiding the process of routing loop development. To ensure that the routing table always has the same information, it is critical to consistently update it across the whole network. When updating a route, you have two options: whole dumps or tiny increment packets. You can swap out one sort of packet for the other. To lessen the possible deluge of traffic caused by network changes, this measure is implemented.

A full dump packet may need a significant number of network protocol data units (NPDUs) since it comprises all of the currently available routing information. During periods of inconsistent movement, these packets are only sent very infrequently. They are only transmitted at this time. In order to transmit just the data that has changed since the last complete dump, smaller incremental packets are utilised. In order to guarantee the correct transmission of the data, this is done. Because each of these broadcasts should fit inside a standard-sized NPDU, the quantity of traffic should be reduced. The mobile nodes keep a second table open so they may store the data sent in incremental routing information packets. Included in this table is the transferred data.

Along with the destination's address and the number of hops needed to get there, new route broadcasts also include the sequence number of the received information at the destination as well as a new sequence number that is specific to the broadcast. In every case, the route with the most current sequence number is always seen to be the best one. If the sequence numbers of two updates are identical, the one with the smaller metric will be picked for optimisation (to reduce the path). The goal is to make things go more quickly. The goal is to maximise efficiency, therefore that's how it's done.

Also, until the route with the best metric is reached, mobile devices record the settling time of the routes. This is also called the weighted average time that routes to a location might vary.

One more thing that mobile gadgets keep an eye on. By avoiding transmissions that would be sent out if a better route could be found soon, mobiles can reduce network strain and enhance routes. A routing update can be postponed during the settling time, allowing for this to happen. This feature reduces the amount of traffic that is transmitted across the network.

The fact that every node broadcasts its own sequence number, which is rising in a regular manner, should be carefully noted. By using an infinite metric and a sequence number that is one more than its sequence number for the broken route, node B will advertise the route to D with an odd sequence number when it finds that its route to D has broken. The result is that the sequence number will be divisible by two. This is what happens when things are done this way. This means that every single node A that uses B as a routing intermediate will have the infinite-metric route stored in their routing database. This will keep happening until node A receives a route to node D with a higher sequence number (SERV).

1.14 THE WIRELESS ROUTING PROTOCOL

Murthy first introduced the Wireless Routing Protocol (WRP) in 1996. It is a table-based protocol that aims to maintain routing information across all network nodes. Distance, Routing, Link-cost, and Message Retransmission List (MRL) are the four tables that each network node is responsible for maintaining. Two of these databases are maintained by each node. Every single item in the MRL has the update message, which contains a list of all the modifications that were sent out. In addition, the update message sequence number, an acknowledgment-required flag vector with one item per neighbour, and a retransmission counter are also included in each entry.

The entry has all of these components. Neighbours are obligated to confirm receipt of the reissued communication as the MRL keeps track of which update message changes need resending. Through the use of messages called update messages, mobile devices may communicate with each other and transmit information regarding changes to connections. Nodes can only communicate with each other via near proximity if they are physically close

by. The location, distance to the destination, and predecessor of the destination are all components of an update message's list of updates.

In addition, each update message includes a set of answers that identify which mobile devices should respond with a "ACK" to the update. Whenever a mobile device detects a change in a link or processes updates received from neighbours, it will immediately send an update message to a neighbour. Either of the two occurrences must have already taken place for this to happen. Nodes will communicate with their neighbours to send update messages in the event that a link between them is broken. This is what will happen if the connection between the nodes is broken. The next step is for the neighbours to update their distance database and look for other pathways that go through different nodes. The originating nodes are notified of any newly discovered pathways so that they can update their databases accordingly.

The tables will always be up-to-date because of this. When nodes receive messages, such as acknowledgments, they can learn about the presence of their neighbours. This is how they get their hands on this data. If a node hasn't sent a message in a while, it has to reconnect to the network by sending a hello message after a certain amount of time has passed. It is up to the network administrator to decide on this set duration. In any other situation, a false alarm might be sent out since the node isn't sending any signals, which would indicate that the link is down. A mobile device will add a new node to its routing table after receiving a hello message from that node. Furthermore, the mobile device will transmit the unknown node a duplicate of the data contained in its routing table.

This happens when the latest node sends a greeting message to the mobile device. The uniqueness of the method is heavily dependent on how WRP can establish independence from loops. The procedure is significantly aided by this. The responsibility of transmitting the distance to each wireless network destination and details about the second-to-last hop along the path lies with the routing nodes when utilising WRP. As a member of the class of path-finding algorithms, the WRP algorithm stands out as a notable outlier.

The "count-to-infinity" problem can be circumvented since each node must perform consistency checks on the predecessor information provided by all of its neighbours. Ultimately, this decreases the occurrence of looping and allows routes to converge faster in the event of a connection failure. Nevertheless, this takes time to happen following the incident.

1.15 LANDMARK ROUTING (LANMAR) FOR MANET WITH GROUP MOBILITY

It was in the year 2000 that Pei first introduced the Landmark Ad Hoc Routing (LANMAR) protocol. This protocol integrates the advantages that are associated with both FSR and Landmark routing into a single package. The most major innovation that this system has to provide is the use of landmarks for every group of nodes that travel together (for example, a group of troops on a battlefield) in order to limit the quantity of information that has to be updated for routing purposes. As is the case with FSR, nodes only transmit their connection state to the neighbours that are closely next to them. This is the case both in and out of the network.

The routes that lead to more distant clusters of nodes are "summarised" by the landmarks that correspond to them, despite the fact that the routes that are included inside the Fisheye view are correct. Furthermore, the Fisheye view contains accurate routes. A packet that is headed to a distant location will first aim for the Landmark as its destination. However, when the packet gets closer to its target, it will finally reroute itself to the more exact path that is provided by Fisheye. The Landmark is the initial target of the packet, which causes something to take place. The preset hierarchical address of each node in the original wired landmark system serves as a representation of the node's location within the hierarchy and offers aid in identifying a path to the node.

This address was designed to be specific to the node. When a hierarchical partition is present, every single node that constitutes the partition is aware of the paths that go to every single other node that is a member of the partition. Furthermore, every node is aware of the paths

that go to the various "landmarks" that are located at the various levels of the hierarchy. These "landmarks" make up the various levels of the hierarchy. It is at higher heights that these "landmarks" are situated. As a packet moves closer to its goal, its path is increasingly refined from the highest level of the hierarchy to lower levels.

This process occurs as the packet moves closer to its destination. The execution of this phase takes place when the packet gets closer to its final destination. Within the framework of the principles, this is carried out in accordance with the landmark hierarchy, which is consistent with packet forwarding. The concept of landmarks, which is today employed by LANMAR in order to keep a record of logical subnets, was first provided by Tsuchiya in the year 1988. Tsuchiya was the one who initially offered the notion. Individuals that are going to travel together as a "group" (for example, troops on the battlefield or students from the same class) are the people who make up subnets. Subnets are made up of people who have a same interest.

These persons are able to communicate with one another more easily thanks to subnets. Subnets are being brought up as examples in each and every one of these situations. When following the conventional approach, it is assumed that each subnet would select a "landmark" node. This system is a modified version of FSR, which serves as the routing system itself. It is the root of the problem. In comparison, the LANMAR routing table only includes the nodes that are within the scope and the landmark nodes. On the other hand, the FSR routing table includes "all" of the nodes that are present in the network.

This is in contrast to the LANMAR routing table, which only includes such nodes. Among the differences that exist between the two, this is the most significant one. This feature, which significantly increases the system's scalability, reduces both the size of the routing table and the amount of information that has to be updated. As a consequence, the system is able to handle increasing amounts of traffic. The address of the destination can be determined in the routing table in the event that a node is required to relay a packet or packets. Furthermore, if the node's neighbour scope contains some of the destinations on the list of destinations, the

packet is then transmitted straight to the destination. If this is not the case, the logical subnet field of the destination is checked, and the packet is then sent to the landmark for the particular logical subnet that is being researched.

This process continues until the packet is delivered to the destination. However, it is not necessary for the package to go via the landmark in order for it to be delivered before it is delivered. The packet is instead sent straight to the destination as soon as it reaches the point when it is within the scope of the destination. This occurs shortly after the packet. There is a substantial degree of overlap between the FSR and the routing update exchange when it comes to the context of LANMAR for routing. For the purpose of exchanging information on the topology, each and every node in the network engages in consistent communication with the nodes that they immediately neighbour.

Inside the fisheye scope of the node, the entries that are included inside it are sent. The occurrence of this action occurs with each and every update. Furthermore, it makes use of a distance vector that has a dimension that is proportional to the number of logical subnets and, consequently, landmark nodes. This is done in order to ensure that the distance vector is accurate. Additionally, this is in addition to the qualities that were discussed before. Should this process of exchange be carried out, the table entries that have sequence numbers that are higher will take the place of those that have sequence numbers that are lower. This will occur in the case that this process of exchange is carried out.

1.16 CHALLENGES

Ad hoc networking, as a subject of research, has grown in stature throughout the last several years. All parts of the network have been thoroughly examined within the parameters of the inquiry. Despite this, not a single issue that has been acknowledged or even discussed has a definitive solution. On the other hand, more people are requesting information. Similar to how ad hoc networks have had several features studied, sensor networks have had numerous aspects studied as well; however, unlike ad hoc networks, there are far more problems that

have not been resolved. The next section provides a detailed analysis of the most pressing issues that require fixing.

The majority of the time, the development opportunities that depend on the protocol are ignored. The emphasis instead falls on the "big picture," here meaning the challenges that will make future peer-to-peer connections unavailable in some areas. Here are the issues that require immediate attention:

- Scalability
- Quality of service;
- Client server model shift;
- Security;
- Interoperation with the Internet;
- Energy conservation;
- Node cooperation;
- Interoperation.

It is our intention to include the technique that is outlined in [Perkins2001, Penttinen2002] into this section, albeit with a few adjustments. Within the context of this discussion, an effort is made to provide a complete analysis of the challenges that ad hoc and sensor networking may encounter in the years to come.

1.16.1 Scalability

Most people who imagine future applications that use ad hoc and sensor networking technologies assume that these applications will be scalable. For apps to be successful, scalability is a must. We might think of the concept of ubiquitous computing as an example, where networks can be of "any size." The question of how these massive networks may ever grow remains open, though. Because of their very design, ad hoc networks inherently have problems with capacity and scalability.

As an example, we may examine a few elementary interference experiments. The throughput per node declines at a rate of 1/"^ in an uncooperative network that uses omni-directional antennas, according to Gupta (2000). When discussing networks, the letter N stands for the total number of nodes. Another way of looking at it is that in a network with 100 nodes, each device only gets around 10% of the data throughput that the network is capable of theoretically. Nobody has yet found a solution to this intractable problem; the only option is to implement physical layer modifications, such the directional antennas examined in Chapter 6.

Both the protocols and the available capacity will establish constraints on the kinds of communications that are really feasible. Procedures like route acquisition, service localization, and encryption key exchange are examples of the kinds that will need a lot of overhead as the network size increases. These are but a few of instances. These networks might never be implemented if the limited resources are squandered on unnecessary control traffic. The reason for this is because there is a lack of resources. Consideration of scalability is a major research hurdle when creating solutions for sensor networks and ad hoc networks. The explanations given above are the main ones.

1.16.2 Quality of Service

As a result of the vast variety of applications that are presently running via the Internet, network designers have been forced to deal with a number of challenges. When they constructed the network, they did so with the goal of delivering the greatest possible quality of service to its customers. Some examples of applications that are highly distinct from one another are the needs for speech, live video, and file transfer. These are only a few examples. To name just a few examples, here are several.

As a means of satisfying the ever-evolving requirements of these applications, solutions that are cognizant of Quality of Service (QoS) are currently being developed. This development is being done with the intention of satisfying the criteria. It is important for the network to

guarantee quality of service (QoS) in order for the network to be able to deliver a certain level of performance for a specific flow or a collection of flows. This ensures that the network is able to give the desired level of performance.

In order to properly evaluate this performance, it is essential to take into consideration quality of service measurements. These measures include, among other things, latency, jitter, bandwidth, and the risk of packet loss while analysing this performance. In the second chapter, we spoke about Quality of Service (QoS) routing, which is an attempt to find routes that are able to meet the performance requirements that have been established and then reserve sufficient capacity for the flow of traffic. In order to find routes that are able to fulfil these requirements, quality of service routing makes an attempt.

Even though there are now research efforts being made in the field of quality of service (QoS), the issue of quality of service in ad hoc and sensor networks is still somewhat opaque. This is despite the fact that there are currently research efforts being made in the field. It is necessary to find solutions to the issues that have been raised about the quality of service (QoS). Quantity of service (QoS) routing strategies, algorithms, and protocols that have a range of priority, including preemptive priorities, are included in these issues.

1.16.3 Client-Server Model Shift

The great majority of the time, a network client on the Internet is set up to utilise a server as its partner in order to carry out network transactions. This is the case since servers are the most common type of network client. Your preferences will determine whether these servers are located automatically or through a static setup. Both options are available. Ad hoc networks, on the other hand, do not let the structure of the network to be determined by the subnets that are created by grouping IP addresses together.

Due to the fact that ad hoc networks are not designed in this fashion, this is the result. Despite the fact that there are no servers that are available for use, there is still a need for essential

services. However, the position that these services hold within the network is unclear and may possibly alter over the course of time. There are a number of services that are required to be extremely fundamental; however, the position that these services occupy now is uncertain. Examples of services that are included in this category include authentication, address allocation, and name resolution. Other examples include name resolution. Another illustration of this would be the location of the service itself.

There is a possibility that a different method of addressing will be necessary in the future because of the infrastructure less nature of these networks and the mobility of the nodes. There is a chance that this will occur. A last point of interest is that it is not yet clear who will be in charge of administering the different network services until more study is carried out. This is something that should be taken into consideration.

Despite the fact that a significant number of research projects have been carried out in this field, the problem of moving away from the conventional client-server paradigm has not yet been successfully addressed. This is due to the fact that the reason for this is that the issue has not yet been adequately addressed. Despite the fact that a significant amount of activity is taking place inside the Zero Configuration (zeroconf) working group of the Internet Engineering Task Force (IETF) and also within the UPnPTM forum [UPnPwww], which is being discussed within the context of the Digital Living Network Alliance [D], there is still a lot of work to be done.

1.16.4 Security

As a result of the characteristics of the networks themselves, ad hoc and sensor networks are especially vulnerable to malicious behaviour. Due to the absence of any centralised network administration or certification authority, these wireless networks, which are always experiencing changes, are extremely susceptible to infiltration, eavesdropping, interference, and other threats of a similar kind. This is because these networks are constantly undergoing changes within themselves.

It is generally agreed upon that the most significant "roadblock" in the process of bringing this technology into commercial usage is the protection of sensitive information. In spite of the fact that a significant amount of progress has been achieved, as will be demonstrated in Chapter 9 later on, security has only gotten a respectable amount of attention up to this point.

In spite of the fact that it is a truth that security is one of the most challenging issues to solve, this is the case. It is not envisaged that the "golden age" of this study issue will begin until the functional difficulties on the underlying levels have been resolved to the satisfaction of all parties concerned. This is because the "golden age" pertains to the "golden age" of research.

1.16.5 Interoperation with the Internet

To make use of the various applications of ad hoc networks that are most frequently used, it is quite probable that a connection to the Internet is necessary in some form or another. This is the case because of the nature of the applications. Despite this, the task of building the interface between the two networks that are substantially dissimilar from one another is not a straightforward one to overcome. Therefore, in the case that one of the nodes in the network is connected to the Internet, then that node is able to interact with the other nodes in the network and provide them with a connection to the Internet.

Despite the fact that the connections are physically maintained over a number of hops, this specific node has the capacity to declare itself as a default router, and the entire network may be viewed as a "single-hop" from the perspective of the Internet on account of this capability. It has been suggested by recent research that was published in [Sun2002] that there is a solution to this problem that is not only effective but also realistic.

Within the framework of this specific circumstance, the objective is to integrate the Mobile Internet Protocol (IP) technology [Agrawal2002] with ad hoc routing in order to make it easier for the gateway node to be regarded as a foreign agent in line with the definition of Mobile IP.

1.16.6 Energy Conservation

The field of ad hoc networking, and sensor networking research in particular, is experiencing a large spike in popularity of energy-efficient networks. This trend is expected to continue. Concerns surrounding the optimisation of energy usage are now being addressed at each and every tier of the protocol stack. This is the current point in time. When it comes to study, the maximization of the lifespan of a single battery and the maximization of the lifespan of the entire network are virtually equivalent to one another. Both of these disciplines are considered to be among the most significant.

The first statement is about commercial applications and concerns regarding node collaboration, whereas the second statement is of more significance. For instance, in military scenarios, where it is anticipated that nodes will interact with one another, the second statement is of greater significance. Despite the fact that the former is more pertinent, the latter is indeed more significant. The aims can be accomplished through the creation of better batteries or through the use of network terminals that are more energy efficient in their operation. Both of these can be accomplished. Both of these choices represent opportunities that may be pursued. In the not-too-distant future, it is anticipated that the first method would result in a forty percent improvement in the battery life (when employing Li-Polymer batteries) [Petrioli2001].

The occurrence of this result is anticipated to take place in the not-too-distant future. The creation of low-power hardware through the utilisation of methods such as variable clock speed central processing units (CPUs), flash memory, and disc spindown is the most crucial part in the process of optimising energy efficiency [Jones2001]. This is due to the fact that the electricity consumption of the gadget is the most important factor in determining the amount of energy that may be saved. Nevertheless, when we evaluate the device from the aspect of networking, our emphasis naturally gravitates towards the network interface of the device, which is often the single most power-consuming component.

It is possible to enhance energy efficiency at the network interface by developing technologies for transmission and reception on the physical layer, as well as by identifying idleness on the application layer. Both of these methods are necessary in order to achieve this goal. When it comes to this particular aspect, however, the utilisation of particular networking techniques is very beneficial. However, the transport and application layers have received a very little amount of attention, despite the fact that a significant amount of research has been conducted at the physical, medium access control (MAC), and routing levels. This is in contrast to the fact that the physical layer has received a great amount of attention. Even taking everything into consideration, there is still a significant amount of work that has to be finished.

1.16.7Node (MH) Cooperation

It has been brought to light that there is a barrier to the commercial adoption of the technology, and this barrier is closely tied to the security concerns that have been drawn attention to. It is the collaboration between nodes that constitutes this barrier. What are the reasons that someone might disseminate the information that belongs to other individuals? The answer to this question is necessary since it is of great significance. The answer, which is an easy one, is to purchase the service that matches to it from other people. This is the solution.

On the other hand, when disparities in the quantity and significance of the data are taken into account, the situation becomes far more challenging than it was before considering these factors. It is inconceivable that a fire alarm box that is crucial to the operation of the building would waste its batteries by transmitting gaming data, and it should not be denied access to other nodes due to the fact that it functions in such a restricted manner. It is impossible to comprehend any of these two things.

It is possible that the implementation of charging, which is analogous to the concept that was proposed for the management of Internet congestion [MacKieMasonl994], might be the result of giving incentives for nodes to work together with one another. It is possible that those members of the network who behave in an appropriate manner may be rewarded, but those

members who are nasty or self-centered may be paid higher fees. There is a possibility that the network may provide rewards to members who act in a positive manner. On the other hand, it is common knowledge that the installation of any form of charging system is considered to be an extremely difficult task. There is still a lack of clarity on the replies that were given to these inquiries [Yoo in 2006].

1.16.8 Interoperation

When two networks that were built independently of one another come into close proximity to one another, the self-organization of ad hoc networks presents a difficulty. This is especially true when the networks are in this vicinity. The circumstance that is the root of the problem is as follows. Not only is this a research subject that has never been explored before, but it also has consequences for the design of the system on every level that you can possibly conceive of. The question of what happens when two autonomous ad hoc networks move into the same place is one that has to be answered, and it is something that needs to be done. There is not a shred of doubt in my mind that they are unable to successfully avoid interfering with one another.

In the event that all went according to plan, the networks would acknowledge the issue and come together to form a new organisation. The challenge of combining two networks, on the other hand, is not a simple one; the networks may use different synchronization, or even different MAC or routing protocols at the same time. This makes the process of merging the networks complicated. Due of this, finding a solution to the problem is challenging. To add insult to injury, the problem of security becomes a factor that is of great importance. In what ways are the networks able to alter their behaviour in response to the existing condition of affairs? Consider the situation of a military force that is moving into a location that is being monitored by a sensor network.

This is an example of a scenario that presents itself as an illustration of such a scenario. The moving unit, on the other hand, would most likely be utilising a different routing protocol that

is able to accommodate location information. This is in contrast to the sensor network, which would utilise a basic static routing protocol. During the course of our conversation on wireless networks in general, we bring up an extra significant issue that comes into play. There are a number of key goals that have been accomplished by the most recent research that has been conducted on all wireless networks all over the world.

One of the most essential of these goals is to enable seamless integration of all different kinds of networks. Furthermore, in light of this challenge, it is of the utmost importance to take into consideration the many ways in which the ad hoc network may be structured in such a way that it is compatible with wireless local area networks (LANs), third-generation (3G) cellular networks, and fourth-generation (4G) cellular networks. In Chapter 7, we delve into this intricate subject matter and provide some insights into the present state of affairs in this particular field of study. In particular, we concentrate on the situations that are occurring in the United States.

CHAPTER 2

ROUTING IN MANET

2.1 INTRODUCTION

If two or more nodes in a data communication network are not directly connected to one another by a communication connection, then it is essential for there to be intermediary nodes in the network in order for those nodes to be able to receive or send messages to one another. This communication connection is what allows the nodes to communicate with one another. This is due to the fact that the network does not have a direct connection to the nodes that are participating in communication with one another. The act of obtaining a route between two nodes in a network in order to permit the transmission of messages between those nodes over the network is referred to as route acquisition.

This process is also commonly referred to as the routing process. The process of routing is another name that may be used to refer to this sort of procedure. Routers are the nodes in a traditional network that are responsible for directing traffic to the right destinations. Routers are also known as router stations. In addition, routers are referred to inside the industry as routers. The activities of switching packets, filtering packets, communicating with the internetwork, and determining pathways are all responsibilities that fall within the purview of a router in a network. Each of these responsibilities is included in the list of responsibilities that a router in a network is responsible for.

This protocol is accountable for two key responsibilities: selecting routes for a broad variety of source-destination combinations and ensuring that messages are delivered to the appropriate recipients. Both of these responsibilities are its principal responsibility. With regard to each of these tasks, the routing protocol is the subject of accountability. With regard to both of these duties, the protocol that is utilised for routing is very necessary. In a broad sense, routing protocols may be categorised into three primary classes, which are as follows

organised according to their classification: In the following order, the categories that correspond to one another are as follows: It is the connection When it comes to connecting state protocols, the Dijkstra Algorithm serves as the foundational component necessary.

This mathematical architecture serves as the foundation upon which state protocols are organised. It is feasible for each node to maintain an up-to-date image or knowledge of the architecture of the network, complete with the costs or metrics that are associated with each connection and route. This is made possible as a result of the fact that this is achievable. Certainly, this is something that is attainable. The full image of the whole routing domain that is presented here makes it feasible for every node to compute and pick the ideal route based on the information that is collected directly from the source. Considering that this picture is typical of the entire routing domain, this opportunity has become available as a result of this.

When this was the case, it was essential for each node to pay attention to what its neighbour considered to be the most optimal path. As a result of the flooding of connection charges by other nodes, every node is required to perform frequent updates of the view of the network topology that it has. This is because of the fact that the network topology is constantly changing. It is because of the fact that other nodes are flooding their connection prices that this flooding is occurring. They begin by identifying the individuals who are located in close proximity to them, and then they proceed to synchronise their topological paths with those that they are already established with.

They then just send out random messages of hello to their neighbours in order to let them know that they are still online and participating in activities. This is done in order to let them know who they are. Link state routing protocols make use of a method that is popularly known as the shortest route algorithm in order to determine the next-hop for each destination as part of the routing process. This is done in order to ensure that the routing process is implemented correctly. On the other hand, it requires more memory and uses more CPU power than the techniques that came before it, despite the fact that it converges more rapidly, requires less

bandwidth for updates, and has more scalability. This is despite the fact that it increases the capability to scale.

Distance vector protocols are concerned with the overall position of the destination, the amount of time and effort required to go there using a specific metric, and the direction (vector) in which a place is put where the destination is expected to be. The Bellman-Ford approach serves as the basis for both distance vector protocols and their implementation. Each node will occasionally provide the nodes that are directly linked with an estimate of the shortest distance between all of the network pathways that it is aware of, including those that are connected as well as those that it has learned. This is in addition to monitoring the cost of its outgoing connections, which is something that each node does.

The sole function that each node is responsible for is this. The execution of this procedure takes place inside the scope of the protocol that is known as the distance vector. As a result of this, the expression "routing by rumour" is occasionally used to refer to specific individuals. The explanation that was given before is the reason behind this. Some of the other benefits that are associated with it include the fact that it is easier to build, that it makes use of less resources from the central processing unit (CPU) and memory, and that it is more efficient in terms of computation. On the other hand, it is plagued by a number of issues, one of which is a performance that is slow.

There are several factors that can lead to convergence problems. Some of these factors include the "counting-to-infinity" problem, insufficient utilisation of the bandwidth that is already available, and the establishment of both temporary and permanent routing loops. To name just a few of the potential reasons of convergence problems, these are only some of them. The difficult conditions are a direct outcome of the difficulties that have been encountered. In this section, we will talk about the places where the routes were initiated in the first place. Whenever this particular method of routing is utilised, the destination of a packet is determined prior to the packet ever being transmitted into the network.

In order for the information that is delivered to arrive at the location that it is intended to reach, it is absolutely necessary for it to have all of the necessary criteria for the route. As a consequence of this, the decision about the routing is made at the source, which is advantageous since it helps to limit the number of routing loops that take place. One of the most important advantages of a source routing architecture is that it eliminates the need for intermediary nodes to maintain their existing routing information in order for them to be able to route the packets that they forward.

This is one of the most significant advantages of a source routing architecture. This explanation is due to the fact that the packets themselves already include all of the routing options that are available. This is the most significant advantage that a source routing design could possibly provide, and it is the reason why it is offered. As a consequence of this, there is a disadvantage associated with it, which is that it requires the payment of a slightly higher overhead cost in order to collect and retain the route information that is utilised. This is a downside that may be associated with it.

When attempting to discern between centralised routing and distributed routing, it is essential to keep in mind that the former is dependent on specialised hardware (in the form of a router) to determine which paths are acceptable and which are ideal. This is the case in order to differentiate between the two types of routing. The distributed routing method, on the other hand, is dependent on the network infrastructure that is already present in the network. However, distributed routing does not rely on hardware of this sort throughout its operation. This is in contrast to the distributed routing model.

Distributed routing, on the other hand, does not need the use of such infrastructure in order to operate in an appropriate manner. Distributed protocols, which are able to function by transferring data back and forth between nodes, make it possible for the choice-making process and the computation of routes to be decentralised over the whole network. Because distributed protocols have certain features, this is something that can be accomplished.

Because of this, the network is able to make use of more flexibility and efficiency than it would have otherwise been able to provide.

The distributed protocol approach is an efficient method that may be utilised for the administration of ad hoc networks, which are networks in which each node functions as both a host and a router. This type of network is sometimes referred to as a "distributed network." Because it is a way that may be utilised for the management of those networks, this is the reason.

Static vs. Adaptive: In particular, this is relevant to how routes adjust to changes in topology and the traffic patterns that utilise them. The connection paths taken by source-destination pairs in static routing are constant. No matter how much traffic is being sent or how the underlying topology changes, this remains true. This is due to the fact that static routing is viewed as a foundational kind of routing. When a component of the system is malfunctioning, it hinders the overall performance of the system since it can't adjust to new circumstances as well as it should.

Maintaining a constant high throughput is not possible with a static routing architecture. Reason being, static routing isn't flexible. You should only use it with simple networks or networks where efficiency is not your top priority when dealing with networks. A reaction is implemented in the route computation to account for or correlate with changes to the traffic input patterns and/or the network design. This is a standard occurrence anytime an update is made. When compared to previous routing methods, adaptive routing is much more interactive. Another thing to think about is that in some parts of the world, it's called Dynamic Routing. Under these conditions, the routing protocol is attempting to modify its routes and reroute traffic by making use of alternative route choices.

The goal is to keep the throughput reasonably high while reducing congestion. This is important for mobile ad hoc networks as it can now handle nodes with a high degree of mobility and can be easily adapted to new network designs. Also, it can now support nodes

with a high degree of mobility. The fact that it performs wonderfully on mobile ad hoc networks is an additional perk.

Reactive vs. Proactive: There is a significant degree of relationship between this category and ad-hoc networks, which are closely related to one another. This link is strong. The use of proactive routing protocols is employed in order to guarantee that the most recent version of the routing information that is immediately accessible is always maintained up to date. For the purpose of ensuring that this is achieved, these protocols do routine evaluations of the routes that are present inside networks.

In the event that a packet needs to be delivered, the route will already be decided, and it will be possible to make use of it without any delay. This is because of the fact that this is the case. It is therefore plausible to argue that reactive protocols only carry out a technique for route determination when it is absolutely essential to do so. This is because of the situation described above. To be more specific, this is because reactive processes are necessary in order to identify the path before moving on with the process.

2.2 DESIRABLE QUALITATIVE ASPECTS OF NETWORK RUNNING PROTOCOLS

It is generally agreed that these characteristics are desirable in relation to ad hoc routing protocols, which are employed for the purpose of traffic routing. A process that is carried out in a manner that is spread systematically The fact that an ad hoc network is primarily composed of a scattered collection of nodes makes it reasonable to anticipate that its routing protocol will also be distributed in a manner that is consistent with the dispersion of the nodes in the network. Furthermore, as a consequence of this, it is essential for MANET routing protocols to be decentralised and capable of functioning independently.

In light of this, it is imperative that they do not rely on a single controlling node that is located within the network. Although nodes can easily join or leave the network, mobility is

something that must be constantly taken into consideration when constructing the network. This is because nodes can join or leave the network at any time. It is still the fact that this is the case regardless of whether or not the network in question is stationary, such as in the case of an ad hoc network. Movement is something that must be taken into mind at all times. This is an absolute need.

Unidirectional Link Support: In the course of developing routing algorithms, it is common practice to make the assumption that the connections that are being utilised are bidirectional. This is a common practice. This is due to the fact that many protocols are unable to work correctly when using links that only go in one way. The explanation behind this is as follows. On the other hand, unidirectional connections are able to and frequently do occur in ad hoc wireless networks; hence, it is anticipated that this characteristic will be incorporated into MANET routing protocols.

Loop-freedom: Within the context of any network protocol, it is generally recommended to avoid route loops wherever it is practicable to do so. The utilisation of unneeded bandwidth and processing resources will be avoided as a result of this, which will result in an increase in overall performance that is assured.

Demand-based operation: It is more efficient for the routing protocol to adapt to the patterns of traffic depending on the demands or needs of the network rather than assuming that every region of the network experiences the same amount of traffic and, as a result, constantly maintaining the same routing between nodes. This is because the routing protocol can adapt to the patterns of traffic more efficiently.

This is due to the fact that the routing protocol is able to better modify itself to meet the patterns of traffic. When the protocol is developed in a sophisticated fashion, it should be able to make more effective use of the power and bandwidth resources that are supplied by the nodes. The protocol must have a reactive nature in order to function well. Nevertheless, this need to be accompanied with an increase in the amount of time it takes to locate the path.

Due to the fact that the nodes in ad hoc networks are often devices or thin clients that are largely powered by batteries, it is essential for these nodes to conserve power by adopting standby modes when they are not in use. This is crucial since these nodes are a substantial source of power consumption. For the purpose of ensuring that there is adequate conservation of energy, this is done. It is of the utmost importance that a routing protocol be able to accommodate and recognise a range of sleep patterns without inflicting an excessive amount of damage. This is because of the fact that this is the case.

There is a chance that these qualities will need the provision of support for link layer protocols through the use of a specific interface. Taking this into consideration, there is a chance that it will occur. It is very necessary to have support for multipath routing in order to achieve the goal of having a large number of routes. Using a variety of routes will result in a more effective reaction or response in the event that there are topological changes and/or congestion. This is because the response or reaction will be more effective. The reason for this is that having a variety of options to choose from enables one to take advantage of extra possibilities for agility. Because of this action, the routing protocol is stopped from launching yet another route discovery operation.

This, in turn, reduces the amount of latency that is experienced as well as the amount of resources that are utilised by the network. All of these factors contribute to a more efficient network. Before a network can be granted authorization to transport a packet stream from its point of origin to its final destination, it must first be able to demonstrate that it meets all of these service characteristics. The packet stream can now be transported by the network as a result of this. The word that is most commonly used to refer to this kind of assistance is Quality of Service assistance, or QoS.

Consumers are expected to be supplied with a guarantee for end-to-end performance characteristics such as latency, bandwidth, the chance of packet loss, delay fluctuation (jitter), and other metrics that are equal to these particular parameters. This guarantee must be offered

to consumers. There are a vast number of instances in which the criteria are established by the needs for the services that are required by the apps that are hosting the end users or the end users themselves. MANETs are distinguished from other types of networks in terms of the quality of the services that they provide by a number of characteristics, one of which is the substantial amount of power that they use. The MANET routing protocol is vulnerable to a broad number of various sorts of attacks due to the fact that it does not have any form of security procedures in place at either the network level or the link layer.

It is therefore susceptible to a broad variety of different sorts of attacks as a result of this. There is no possible way to emphasise the importance of preventative security measures. This is because it is more difficult to maintain the "physical" security of the radio transmission medium, which leaves MANETs open to any and all forms of security threats and assaults. This is the reason why this is the case. The fact that MANETs are vulnerable to this vulnerability is the root cause of this problem to begin with.

The scattered topology of the ad hoc network, on the other hand, presents a challenge that has to be overcome. Both authentication and encryption will be beneficial in this scenario since they will assist in reducing the majority of assaults that are carried out. The challenge of protecting the MANET protocol, which is of the utmost importance, is examined in this paper, and at the same time, some potential solutions are offered.

2.3 MOBILE AD HOC NETWORKS AND PROTOCOLS

Hierarchical Routing: Clusters are formed by bringing together individual nodes to create clusters, or smaller clusters are connected together to build bigger clusters. This step occurs during the process. This stage is also the time when bigger clusters are produced, which is another possibility.

Immediately after this, the clusters that have been created are entrusted with the obligation of carrying out particular responsibilities or tasks. In the context of this scenario, certain nodes

are responsible for carrying out duties, while other nodes continue to wait for those responsibilities to be passed to the subsequent level in the vertical hierarchy (also known as the vertical hierarchy). The network is composed of tiers, and the node that is responsible for controlling a cluster is often a node that is located in the first tier of the network. As a result of the network being logically divided into divisions, this is the case.

Additionally, they are referred to as cluster heads, which is a term that describes a node that is a component of a cluster but also shares a boundary with another cluster. There are many other names for them. In the domain of computer networks, cluster heads are utilised rather frequently. This specific node has been given the responsibility of carrying out certain control responsibilities or other obligations on behalf of its cluster.

This responsibility has been provided to it by the cluster. One may think of a node as being equivalent to the head of a cluster when it comes to the cluster itself. One other significant feature is that it is near to another cluster, which serves as a border between the two collections. This is an additional crucial attribute.

Flat Routing: As the name of this form of networking implies, all of the ad hoc components and routing activities are carried out on the same level. This is the case. It is feasible to reach the conclusion that there is only one layer that comprises all of the nodes together based on this information. Due to the fact that this is the case, the network does not have any tiers or levels that can be differentiated from one another in any particular way either.

Worse still, the nodes in the network do not cluster together very regularly, which makes the situation even more difficult. The occurrence of this kind of circumstance is not unusual. It is believed that flat routing protocols were the ones responsible for the construction of the ad hoc network, which is made up of a number of nodes. Due to the fact that these protocols do not divide the network into subnets, a hierarchical addressing structure is not necessary for them to function. They are not required to have a hierarchical layout as a consequence of this.

2.4 PROACTIVE ROUTING PROTOCOLS

In this form of routing system, which operates in accordance with the same protocols as conventional wired networks, the task of maintaining a database of the many paths that may be taken to reach each node on the network falls on the shoulders of the system. A proactive routing protocol is one that has complete knowledge of the topology and decides the pathways to all destinations in advance. This type of protocol is also known as a fully proactive routing protocol. In contrast, traditional routing is distinguished by the fact that the protocol only has a limited awareness of the topology.

This is one of the defining characteristics of traditional routing. Further, it is possible to precompute routes by maintaining a record of the connection statuses in the routing of the nodes. This allows for the possibility of precomputed routes. It is because of this that the routes are guaranteed to be accurate forever. Proactive routing, on the other hand, takes use of the connection states, in contrast to reactive routing, which does not make use of such information. Proactive routing is using the connection states. During the entirety of the network's operation, the routing information is transmitted to each and every node that makes up the system. This takes place regardless of whether or not a path of this kind is actually required to complete the task that is currently being carried out.

The vast majority of the distinguishing traits that are connected with the "link state" routing protocol are shown by proactive routing as a direct consequence of this fact. This is due to the fact that every node always has comprehensive knowledge on the whole architecture of the network, in addition to the amount of money that is necessary for each link. This is the reason why this is the case. The first group of routing protocols might be referred to as "driven routing protocols," despite the fact that they are of the proactive sort. This is because they are driven by the need to route traffic. It is possible to split it into multiple segments according to the planning, maintenance, and management procedures that are involved in the organisation of the traffic flow.

This is something that may be done. There are a variety of proactive routing protocols that are now being utilised in the industry. Among the protocols that fall under this category are Fisheye State Routing (FSR), Optimised LinkState Routing (OLSR), Fisheye State Routing (FSLS), Wireless Routing Protocol (WRP), Destination Sequenced Distance Vector (DSDV), Global State Routing (GSR), Source Tree Adaptive Routing (STAR), and Backbone Routing (BRF).

2.5 CHARACTERISTICS OF PROACTIVE ROUTING

- Routing information, including new routes, is regularly broadcast through the network between nodes in order to ensure that information is kept current.
- The updates are divided into two categories based on the number of overhead packets that are produced. There are two different kinds of packets, which are referred to as "full dump" and "incremental" packets respectively.
- first convergence takes place when the entire routing and routes (full dump packets) are traded during the process of building a network or setting up the first configuration. The subsequent topological changes on a network, as well as mobility updates, are regularly transmitted via the use of incremental packets that detail the unique network modifications.
- Using flooding, every node will, on a regular basis, broadcast the link prices of its outbound connections to all of the other nodes.
- One or more routing systems store information about the topology's routes, and their histories are kept up to date. This information is also preserved.
- Each route will be numbered according to a sequence that is established by the node that served as the last hop.
- A mobile node is able to detect the difference between routes that have subsequently been defunct and those that are in the process of being constructed thanks to the sequence number.

There is a combination of updates that are frequently planned and modifications that are caused by events that are used to accomplish the design and management of routes. As a component of periodic updates, routing information is transmitted asynchronously between nodes at regular intervals that have been established.

This occurs regardless of the mobility or traffic levels that are present on the network due to the nature of the network itself. Updates that are triggered by events, such as when a connection is made or withdrawn, are instead delivered automatically at intervals that have been specified in advance. This is done in order to make the most efficient use of resources.

2.6 ADVANTAGES OF PROACTIVE ROUTING

- When employing proactive routing, latency is minimized since the route is already accessible and can be swiftly picked from the routing when a source desires to transmit packets. This is because the route is already available.
- To put it another way, as compared to the alternative, proactive routing results in time and cost savings.
- Because the path is known at the moment the packet arrives at the node, proactive protocols often function effectively in networks that have a high number of data sessions taking place inside the network.
- This makes it possible for the packet to be efficiently forwarded from the node. This is due to the fact that many of the pathways are actually used within the network; hence, the expense of ensuring that they are all in good functioning condition is often acceptable.

2.7 DISADVANTAGES OF PROACTIVE ROUTING

- Its drawbacks include the possibility that certain routes may never be utilized, and the fact that the distribution of routing information consumes a significant amount of the limited bandwidth available on the network. This is because the statuses of the

connections and the network architecture can change fast in big networks or networks with high mobility.

- In addition, proactive routing does a thorough search of the routing for each and every packet; thus, it uses more power than reactive routing does since the process requires a greater number of CPU cycles.
- Additionally, entirely proactive routing methods use a significant amount of bandwidth in order to maintain the most recent routing information. Furthermore, due to the rapid movement of nodes, route updates may occur more often than route queries.

2.8 PROTOCOLS FOR REACTIVE ROUTERING

The fact that these protocols start routing based on a "ondemand" basis is what gives rise to their other name, which is reactive protocols. Other names for these protocols are reactive protocols. This is a significant divergence from the proactive character of the more usual protocols, which look for routes between any and all conceivable source-destination pairings, regardless of whether or not these routes are really required. The reactive nature of these protocols is a significant break from the proactive nature of the more conventional protocols. Furthermore, the reactive character of these procedures constitutes a substantial distinction between them.

These protocols are reactive in nature, which marks a significant shift when contrasted with the proactive style of processes that are frequently utilised. In the event that there is no connection between the nodes of a network, reactive protocols will not preserve any routing information or node activity. Other protocols will continue to function normally. The nodes are unable to communicate with one another in any way through any means. When a source node does not have data to transmit to a particular destination, it is unable to select the path that would deliver the most efficient results. It is due to the fact that the source node does not possess the data necessary for communication.

Unlike the traditional methods of Internet routing, reactive routing strategies do not continuously maintain a route between every possible pair of network nodes. This is in contrast to the usual methods. One of the most important distinctions between the two is exactly this.

That this particular routing system is distinct from the other two types of routing systems is the most important distinction between them. Reactive routing systems can be distinguished from traditional internet routing techniques by the fact that the link connection in an ad hoc network is prone to rapid change, which can result in expensive management overhead.

This is one way in which reactive routing systems can be classified. This is one of the properties that sets reactive routing systems apart from other types of routing systems. When there is a strong need, we instead research fresh choices that the market may give. This happens whenever there is a demand. The words "source initiated on-demand routing protocol" and "reactive routing protocol" are interchangeable and can be used interchangeably when discussing reactive routing methods. Both of these concepts are interchangeable.

Before actually delivering a packet in the manner that was intended, a source will first examine its routing table to see whether or not it has a path to the node to which it is intended to deliver the packet. It is the responsibility of this protocol to conduct a route discovery operation inside the network and to create a connection in the case that it does not already exist. Because of this, the packet will be able to be sent out and received whenever it is necessary to do so.

That is, in the event that it does not already know the path that it will travel, it will be able to determine whether or not it is possible for it to build a route for itself. It is common practice for the process of finding routes to start with a flood of packets being discharged into the network in the form of a question. At this point, the procedure has just made its debut. The procedure that is accountable for the purpose of preserving a record of the routes that have been found is referred to as route maintenance.

2.9 REACTIVE ROUTING CHARACTERISTICS

- After a certain amount of time during which the network is not being used, routes to active destinations that have already been traveled and kept at a node will become invalid and disappear.
- It is able to keep standard routing, which specifies the next hop that must be travelled to reach a destination, as well as a route cache, which contains routes that have previously been traveled.
- Routes are only kept between nodes that have a need to connect with one another.

2.10 REACTIVE ROUTING BENEFITS

- Consumes a much lower amount of bandwidth in order to maintain routes at each node, which helps to save the valuable bandwidth of an ad hoc network.

- The decrease in the amount of work that must be done by the routing system was a primary consideration in the development of on-demand protocols. In most cases, a considerable performance effect will be seen on low bandwidth wireless networks if the routing demand is high.

2.11 DISADVANTAGES OF REACTIVE ROUTING

There is a downside associated with these sorts of systems, and that is the introduction of delay as a result of the route acquisition procedures that are utilised by reactive strategies. To put it another way, anytime a source node makes a request for a route while the route is being identified, there is a certain degree of latency that occurs.

- In the event that the topology of networks is in a state of continual change, it will be necessary to generate a substantial quantity of update packets and distribute them across the network. This requirement will use a considerable portion of the bandwidth that is available. It is also possible that mobility will result in an excessive level of route volatility when reactive routing approaches are utilised.

- When compared to more conventional methods of routing, pure reactive routing is not as well suited for real-time traffic since it has a larger latency or a longer setup period.
- The Dynamic Source Routing (DSR) protocol, the Ad hoc On-Demand Distance Vector (AODV) protocol, and the Temporally Ordered Routing (TORA) protocol are a few examples of protocols that are classified as "Reactive Routing Protocols."
- The Ad hoc On-Demand Distance Vector Routing Protocol (AODV) and the Dynamic Source Routing (DSR) will be the primary foci of our investigation of reactive protocols, and we will examine and contrast the similarities and differences between these two methods in great depth.

2.12 ON-DEMAND DISTANCE VECTOR (AODV) FOR ADHOC

One of the most essential qualities of an ad hoc network is the capacity of its mobile nodes to engage in multi-hop routing among themselves. This is one of the most crucial traits there is. The mobile nodes are equipped with the Ad hoc On-Demand Distance Vector (AODV) Routing Protocol, which allows for the successful completion of this task. one of the characteristics that sets the network apart from other networks is the fact that it involves one another. It is able to reduce the amount of broadcasts that take place in mobile Ad hoc networks since it is a reactive routing system.

This allows it to reduce the amount of data that is transmitted. Real-time route discovery is the means by which this objective is fulfilled. Therefore, AODV will only require a route when it is absolutely necessary, and it will not demand that nodes keep paths to destinations that have not been used in communication in the recent past or that are not being used in communication at the present time. AODV will only request a route when it is absolutely required to do so, which is the reason for this statement.

In this method, the distance vector technique is the theoretical foundation upon which this approach is built. In the case of reactive routing protocols, route finding is accomplished through the use of a route discovery cycle, just like it is in the majority of other routing

protocols. A broadcast network search is then followed by a uni-cast reply, which offers the pathways that were found during the search. These two stages are the components that make up this cycle. AODV is a routing system that, like DSDV, depends on sequence numbers in order to locate the most recent route path and reduce the amount of routing loops that occur. Within a network that makes use of AODV routing, the nodes store information in a table that is referred to as a route table.

This table contains information about the subsequent hop in the routing path for the nodes that are the destinations of the network. Throughout the entirety of the routing table, each and every item is associated with a lifetime value that describes its lifespan. The maximum number of times that a route may be utilised before it is deemed invalid and deleted from the routing database is the factor that determines the route's lifespan when it comes to routing. When a route exceeds its expiration date, it is considered to be invalid, and its entry is deleted from the table. Furthermore, the lifespan duration is updated each time the route entry is used, despite the fact that this is the case. The purpose of this is to guarantee that the route will not be removed before it has successfully completed the function for which it was chosen.

2.13 ROUTE DETECTION

A source node will initially check to determine whether it has a route entry for the destination whenever it has data packets that need to be delivered to a destination or whenever it has data packets that it wants to send to a destination. This is done whenever the source node has data packets that it wants to send to a destination. When it sends data packets, it will utilise the route for which there is an entry, assuming that there is an entry for that route. This is only the case if there is an entry for that route. The one that has been predefined will be used in the event that there is no particular route available.

In contrast, in the case that it does not find a route within its routing, it is required for it to commence the process of route discovery in order to search for a route. This is because it is important for it to hunt for a route. A source node is required to first generate a Route Request

Packet, which is sometimes referred to as an RREQ. This is necessary before the source node can begin the process of identifying alternate routes. It is necessary for this to take place before the source node may begin the process of seeking other routes. Each packet not only includes the sequence number that is currently being used and the IP address of the source, but it also includes the IP address of the destination as well as the most recent sequence number that was known to be associated with that destination.

This information is included in the packet. A hop count of zero will be included in the Route Request ID (RREQ), which is also commonly referred to as a broadcast ID. In addition, the RREQ will include a Route Request ID (RREQ ID). Not only will this be included in the router request, but it will also include other information. The unique identifier that is created for each and every node in the network is referred to as the RREQ ID. This is the term that has been given to the identification. This identity, which is also frequently referred to as the broadcast ID, contains a continuously growing counter as one of its components.

This total is continuously increasing since it is increased by one each time a node sends out an RREQ, which implies that the amount is always expanding. This is the reason why this sum is constantly growing. It is feasible to differentiate between RREQs that appear to be similar and to determine which of the RREQs is the most recent when the source IP address of each RREQ is paired with its RREQ ID. This allows for the identification of the RREQ that is the most recent. As a consequence of this, it is not difficult to ascertain which RREQ is being employed at the present time. After the RREQ has been created, the source node will send it over the network to all of the other nodes so that they may process it.

This gives the other nodes the opportunity to process it. As a result, the RREQ will be able to undergo further processing. when receiving the RREQ, an intermediary or nearby node will build a reverse route to the node that initiated the connection. This will take place when the node has been given the RREQ that was sent to it. That this phase will take place after the node has already communicated the RREQ is something that is anticipated to take place. To

do this, it will add a new route record to the network that it employs. When the request was transmitted over the network, this record gives information on the path that the node that initiated the request took in order to reach its destination.

In order to accomplish this, it first determines the node from whence it obtained the RREQ as the next hop, and then it increases the hop count that is included in the RREQ by one. Because of this, it is able to determine the distance that separates it from the node that was the origin of the RREQ by the use of this information. In the event that it is discovered that other copies of the same RREQ were obtained at a later period, it is conceivable that the packets in question will be deleted. This is a consideration that may be taken into account. After that, it performs an inquiry into its internal network in order to determine whether or not it includes a working link that links to the place that is required.

This is done in order to accomplish the aforementioned goal. If it does not already own a route to the destination, it will simply retransmit the RREQ to its neighbours with an increased hop count. This will occur in the event that it does not already possess a route to the destination. The RREQ is given the command to do a thorough search across the network in order to find a path that leads to the location that was specified. This is accomplished by carrying out the procedures described above. The following example, which may be considered an instance, demonstrates how this method should be carried out correctly.

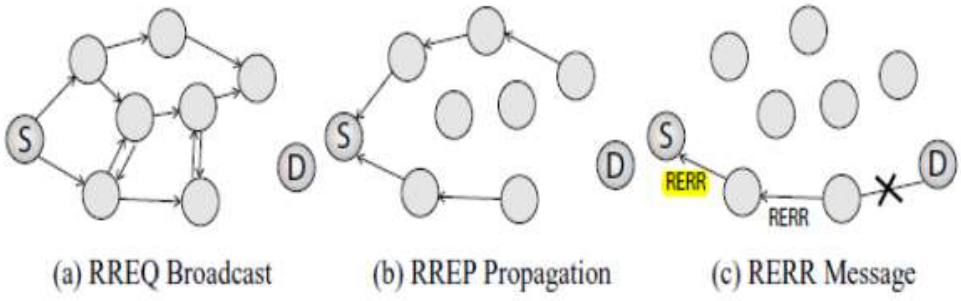

Fig.: 2.1 Adv. Route Discovery and Maintenance

Source: Evaluation of on-demand routing in mobile ad hoc networks and proposal for a secur oposal for a secure routing pr outing protocol data collection and processing through by Soke Mathew Onyemelu kwe (2013)

When a node, on the other hand, is given an RREQ, it is obliged to first assess whether or not it owns a route to the destination that is either still active or has not yet finished its expiry. This is the case regardless of whether or not the route has been terminated. It is important for the node to satisfy a condition before it can transmit a message that is provided in response to a request that provides instructions to the place that is being sought. This message is delivered in response to the request.

It makes no difference whether the node decides that it does in fact possess such a route or not; this scenario is always the same. More than or equal to the sequence number that is included in this node's route entry for the destination, the sequence number that is included in the route request RREQ must be greater than or equal to the sequence number that is there. The sequence number must be the same, with the exception of that circumstance. As a prerequisite, it is of the utmost importance that this specification be satisfied.

The fact that a route entry for the destination is in possession of a route that is at least as up-to-date as the route that has been acknowledged by the source node as being the most recent is an indicator that this is the situation. To put it another way, the information that is included in the entry for the route that leads to the destination is current. It is ensured by this criterion that there are no loops that have been recognised, while at the same time giving priority to the path that has been traversed the most recently. What is referred to as a Route Reply Packet, or RREP for short, is something that may be broadcast by the current node once the conditions that were described before have been completed.

Furthermore, the sequence number for the destination is provided by the node's route entry for the destination. This is in contrast to the previous statement. The RREP is where the IP addresses of both the source node and the destination node are stored. Additionally, the RREP

will change the hop count data in such a manner that it accurately depicts the position of the node in relation to its ultimate destination. This will be done in order to ensure that the data is accurate.

It is possible that the hop count will be equal to zero in the situation that the RREP is being formed at the destination, and the destination itself is the destination. The node will uni-cast the message back to the next hop in the direction of the node that initiated the transmission within a short amount of time following the production of the RREP. This will occur in the direction of the node that received the transmission. When it is sent back to the source node, the RREP will be communicated by the node using the mechanism that is described below.

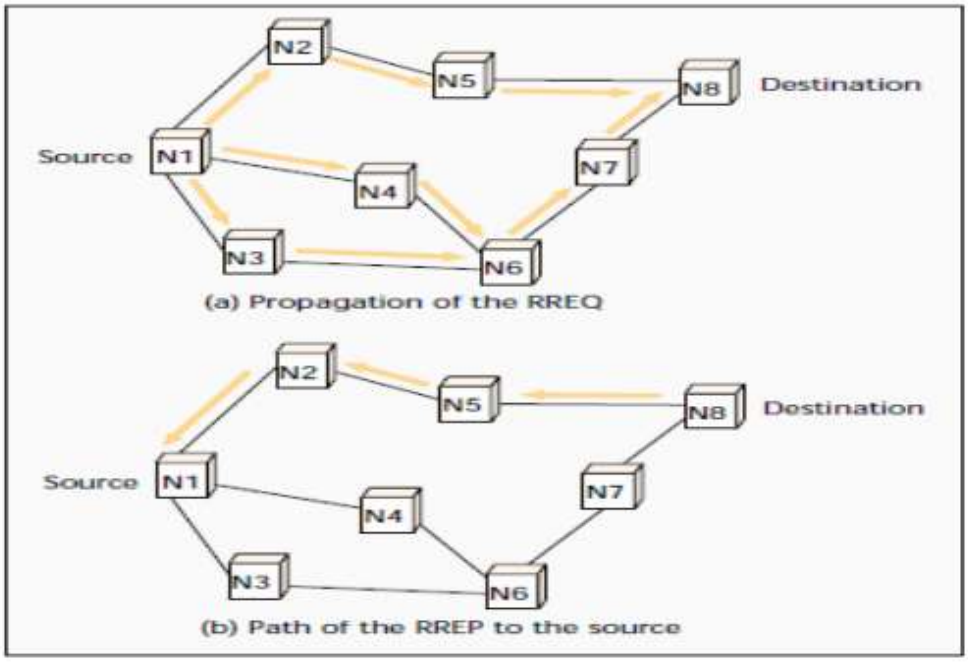

Fig.: 2.2 Adv. Route Discovery

Source: Evaluation of on-demand routing in mobile ad hoc networks and proposal for a secur oposal for a secure routing pr outing protocol data collection and processing through by Soke Mathew Onyemelukwe (2013)

After the intermediate nodes have been told that they have received the RREP, they immediately establish a forward route item in their routing database for the destination node. This is done in order to ensure that the RREP is delivered to the correct node. In the process of travelling to the destination node, this item makes a reference to the node from where the RREP was previously received. This item provides a reference to the root node of the RREP, which corresponds to the point at which the process is initiated. To put it another way, the node from whence it obtained the RREP is now the "next hop" on its journey to the node that it is intended to reach.

The reason for this is that the RREP was retrieved from that particular node. It is the road that is now being used as the path of choice, and it is the road that is signalled by these objects as the route that is being travelled in the forward direction. The fact that this additional hop is factored into the calculation demonstrates that the total number of hops along the route is equivalent to the total number of hops in the RREP plus one. This is the case because the calculation takes into account the additional hop. In the event that a route entry has not been utilised within a certain amount of time after it has been established, the record will be erased from the database. This is because each route entry is connected with a route timer. Each route entry is connected to this timer in some way.

For the purpose of data packet broadcasts to the destination, if the source makes the decision to utilise this specific forward route entry, then the only packets that will be able to reach their destination are the ones that were transmitted from the source via this particular path. Following the establishment of the forward route entry, the RREP will be sent to the node that is acting as a surrogate for the destination that is eventually being transported to. This will take place after. The AODV protocol can only be utilised with symmetric connections.

This is due to the fact that the RREP must be transmitted in a manner that is in accordance with the path that was established by the RREQ. None of the other types of connections are capable of achieving this result. On the basis of this information, it would appear that the

packet that is accountable for transmitting the response to a route request would go in the opposite direction as the packet that initiated the route request. Figure 2.2 provides a graphical representation of the subsequent hop-by-hop transmission of the RREP to the source node. This was done in order to illustrate the process.

To begin the process of using the route in order to carry out data packet transfers, it is the obligation of the source node to commence the process. The beginning of this operation will take place after an arbitrary amount of time has elapsed after the source node was first given the RREP. In the case that more than one RREP is received, the node that is located at the beginning of the network will choose the RREP that has the highest sequence number and the fewest number of intermediary hops. This will be done in order to ensure that the network will function properly.

When more than one RREP is received, this action will be taken in response to the situation. Following the completion of this stage, the routing entry is created and added to the system. It will remain there for as long as it is required and is being employed at the present time. Up to the point that the system no longer requires it, this will continue. During the most recent time frame that has been made available, data packets have been transmitted and received through a route that is currently functioning.

Consequently, a path is deemed to be operational for as long as data packets continue to be transported from their place of origin to their final destination via the channel that is under discussion. This is because of the fact that this is the case. It is the responsibility of each and every node to ensure that their very own routing table is kept up to date.

This table has a single entry for each and every destination. AODV does not store or offer access to a major fraction of the various paths that are theoretically conceivable. This is because of the fact that such a pathway is technically viable. It is a direct consequence of the circumstance that we are in.

2.14 ROUTE MAINTENANCE

An outline of the procedure that is followed when maintaining routes is going to be provided in the following paragraphs. It is possible that the route discovery protocol will be resumed in order to determine an alternative route to the destination in the event that the source node moves to a new location before the destination. This is done in order to guarantee that an individual will arrive at their intended location. If an upstream neighbour of a node along the route discovers that the node has relocated or that a connection between the node and the upstream neighbour has failed, the upstream neighbour will send a link failure notification message (an RREP with an infinite metric) to all of the active upstream neighbours in the area.

This message will be sent to all of the upstream neighbours in the area. A notice like this will be delivered to each and every one of the upstream neighbours in the region. By means of the transmission of this message, the active upstream neighbours will be alerted that the node has relocated or that the link between the node and the upstream neighbour has lost its connection. Both of these events will constitute the transmission of this message. This is what will take place regardless of the conditions; it does not matter whether the relocation was caused by a broken connection or the node itself; it will take place anyway.

When these nodes are alerted that their attempt to establish a connection was failed, they immediately relay this information to their neighbours further upstream, and so on, until the source node is informed of the situation. This process continues until the source node is informed of the situation. Following that, the source node is able to restart the process of route discovery for that destination if it is judged that it is necessary to do so on its own volition. This is the case if it is found that it is necessary to do so. The AODV provides a description of two distinct methods that might be employed in order to ascertain whether or not a connection has been disconnected.

As part of the protocol that is used to maintain the routes, every node will regularly send a "hello" message to the nodes that are immediately next to them. This ensures that the routes

are maintained properly. In the future, this will occur at predetermined intervals. In order to guarantee that it continues to function correctly and to alert all of the mobile nodes in the surrounding area of its presence, it is feasible for a node to send out periodic local broadcasts, which are often commonly known to as "hello" messages. This is done in order to ensure that the node continues to function normally.

Keeping a node's local connection alive is something that may be accomplished through the use of welcome messages. Certainly, this is something that is attainable. Due to the fact that they are able to evaluate the functionality of the connection, they are able to identify any instances of link breakage or node dissociation in a timely manner. This is due of the fact that they are able to analyse the functioning of the connection. In addition, hello messages have the capability of mentioning the other nodes from whom a mobile node has received communication.

One of the most important advantages is that this provides a more complete view of the link between the network and the internet. The second method is detection, which is made feasible by the utilisation of a link signalling mechanism whenever the connection is operating when it is formed. This makes detection a viable option.

2.15 DSR, OR DYNAMIC SOURCE ROUTING

Designed for use in wireless networks that have a large number of hops during transmission A routing system that is both easy to create and extremely successful for ad hoc networks that incorporate mobile nodes is the Dynamic Source Routing protocol, which is also referred to as DSR a few times. By utilising DSR, a network is able to organise and configure itself on its own, eliminating the need for the network administrator to have any kind of pre-existing infrastructure, management, or administration. Instead, the network is able to do it on its own. Regardless of the migration of nodes or any other changes that may take place in the conditions of the network, the DSR protocol offers a highly reactive service in order to aid in the efficient delivery of data packets.

This provides assistance in the effective delivery of data packets. That which differentiates DSR from other routing protocols is the use of source routing, in which the sender is the owner of the whole hop-by-hop path to the destination. Distinguishing oneself from other routing protocols is accomplished through this particular method. This information about active routes is stored in a cache for your convenience. Information that identifies the location of the first point of origin of a data packet is held inside the header of the data packet.

When referring to the manner in which the protocol makes it possible for many pathways to lead to the same destination, the phrase "multipath routing" is generally used. It makes it feasible to disperse the load throughout the network and enhances the network's resilience. This is because it enables individual senders to select and control the channels that are picked when routing their packets. Additionally, it makes it possible to distribute the load. An ad hoc network with a few hundred nodes is the primary target audience for the IETF RFC 4728, which is a document that describes and specifies design guidelines.

To reduce the amount of bandwidth that is consumed by control packets in ad hoc wireless networks, DSR was designed as an on-demand protocol with the goal of reducing the amount of bandwidth that is used up. The dependency that the driven technique (and maybe AODV) had on receiving periodic update signals is eliminated, which allows this to be performed.

2.16 DSR CHARACTERISTICS

- DSR relies on source routing, in which the sender is in possession of comprehensive knowledge of the path used to reach the recipient. Data packets include tight source routes that identify each node along the way to the destination. This means that they are not sent hop by hop but rather contain the routes themselves. Within the header of each data packet is where the source route, which is the whole hop-by-hop path information to a destination, is stored.
- Instead of using a route, it stores routing information in a route cache, which allows for easier maintenance and monitoring of the information. It saves every piece of

information that can be gleaned from the source route that is included in a data packet and puts it all in the route cache. As new routes are learnt, the entries in the route cache are regularly updated to reflect this.

- Because DSR makes such intensive use of source routing and route caching, detecting routing loops does not need the implementation of any specialized detection mechanisms.
- DSR does not need periodic packets of any type at any of the network's layers in order to function properly. Because of this, it does not make use of any periodic routing advertisements, link status sensing packets, or neighbor discovery packets. Additionally, it does not depend on these capabilities being provided by any of the network's underlying protocols in any way.
- It does not make use of beacons and does not call for the broadcast of hello packets, which are typically used by a node to let its neighbors know that it is there.
- It only employs updates that are prompted by events.
- Because it has access to various route information and may support numerous paths, a node that sends a packet using DSR has the ability to pick and control the route that is taken by its own packets.
- When it comes to routing, it uses what's known as a "soft state" approach. Soft state in the sense that the loss of any state will not interfere with the protocol's ability to function as intended. That also means that routing information may be deleted without any prior notice or consultation with the other nodes in the network (as a result of a local choice), yet the network can still function normally. All of the state is found out as it is required, and it is simple and fast to find it again if it is required after a failure without having a substantial effect on the protocol.

2.17 ROUTINE DSR DISCOVERY

Whenever a mobile node is in possession of a packet that has to be delivered, it will initially check the route cache to determine whether or not it already possesses a route to the target or

destination node. The mobile node will proceed to send the packet regardless of whether or not it does. The mobile node will continue to execute the delivery of the packet regardless of whether or not the aforementioned scenario really takes place. In the event that the device is aware of a path that is capable of successfully reaching the destination, it will utilise that path in order to send the packet on its journey. Alternatively, in the case that the nodes do not already possess such a route, a procedure known as route discovery will be carried out in order to dynamically find such a route.

This will be done in order to ensure that the nodes have access to the route. In the event when one node (A) desires to send a packet to another node (D), but the first node does not have an entry for the second node (D) in its route cache, the process of route discovery takes place. As a consequence of this, the nodes that are within the range of wireless transmission of the destination node D will get a Route Request Packet (RREQ), at which time they will add the destination node to their route cache. This specific Route Request (RREQ) includes not only the IP address of the destination but also the address of the source node and a one-of-a-kind identifier that was chosen by node A for this particular round of route discovery.

In this comparison, the node A, which is presumed to be the starting point of the Route Discovery, is contrasted with the node D, which is intended to be the location where it will eventually come to a stop. To assess whether or not there is a path to the destination that is indicated in the RREQ, an intermediate node will check its route cache if it receives an RREQ for which it is not the target. This is done in order to determine whether or not the RREQ specifies a path to the destination. In the event that it does not already possess the destination IP address in its local route cache, it will add it to the route record of the packet before resending it across its outgoing connections as a Route Request (RREQ).

If it does not already have a record of that route saved in its local route cache, then it will not carry out that operation. This route record contains a list of the nodes that have, up to this point in time, forwarded this RREQ. This list is included in addition to the node that

functioned as the route's source or originator. A mobile device will only send a route request to an outbound connection of a node if it has never seen the request before and if its IP address does not already exist in the route record. In other words, the mobile device will only view the request for the first time. This action is taken in order to prevent the outbound connections of a certain node from being overloaded as a result of an excessive number of route requests.

At the final destination, the list of hops (route record) of the RREQ will display the path or series of hops along which this particular RREQ was passed throughout the process of Route Discovery. All of this information will be presented in the sequence in which the hops took place. It is also possible to consider this to be the path that the RREQ travelled in order to get at the node that was intended to be its destination. The RREQ will be retrieved by the node that was scheduled to receive it, and then this will take happening after that. Throughout the course of time, the evolution of the route log may be observed in figure 2.3. The transmission of the route request throughout the network occurs simultaneously with the development of this structure, which takes place simultaneously.

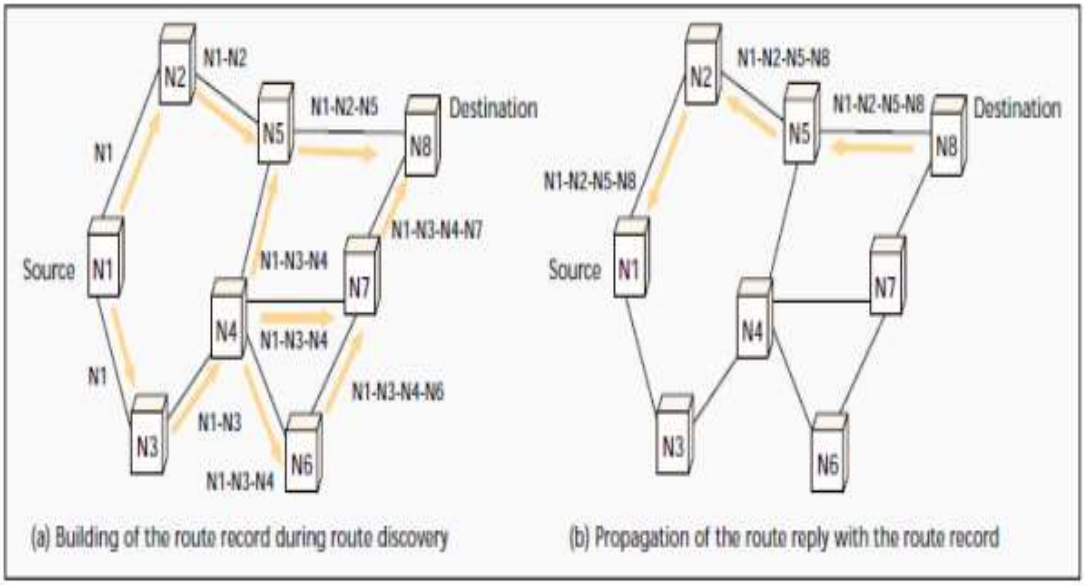

Fig.: 2.3 Making a route record in DSR

Source: Evaluation of on-demand routing in mobile ad hoc networks and proposal for a secur oposal for a secure routing pr outing protocol data collection and processing through by Soke Mathew Onyemelukwe (2013)

In response to a route request, a Route Reply packet is generated once the destination or an intermediate node that possesses an active route to the destination or target has been reached. This occurs after the destination or target has been reached. Now that the package has arrived at its destination, this will take place. There is a possibility that this will take occur when the route request arrives at one of these locations. This node will insert the route record into the header of the packet and then send it back as a unicast Route Reply (RREP) packet if it is the ultimate destination of the packet. There will be an explanation provided in the route record on the journey that the packet took from its origin to its ultimate destination.

In the absence of the node in question being either the destination or the target of the operation, neither of these things will take place. The original path that the Route Request (RREQ) packet pursued in order to arrive at the target node is not connected to the path that the Route Reply (RREP) packet will take in order to arrive at the same destination. To put it another way, this is the meaning of the phrase "routing along any path." Assuming that the MAC protocol that is currently being utilised is capable of enabling the formation of such linkages, the Route Discovery function in DSR makes it feasible to build connections that only go in one direction.

Following that, this RREP is saved in the route cache of the sender node so that it may be utilised for subsequent packets. In the same instant, the source node starts the process of transmitting data along the predetermined path that it had intended to complete, which is to the node that is the destination of the data. If the intermediate node receives a Route Request (RREQ) and already has a record for the destination node in its route cache, then it will send a path Reply (RREP) to the node that is requesting for it, which contains information about the path that leads to the destination. It is only possible for this to take place if the intermediate node is already familiar with the path that leads to the destination node.

As a consequence of this behaviour, a connection is established between the sending node and the intermediary node that is capable of travelling in both directions. It is the responsibility of the intermediate node to update the route record with the route that it has cached after the route reply (RREP) has been established. In the event that a reply makes use of a route that has previously been utilised from its route cache, the newly utilised route is provided to the sender in a way that is significantly more immediate.

Due to the fact that the route was already included in the reply, the overhead of Route Discovery is reduced. Additionally, the RREQ does not need to be rebroadcast because it was already included in the reply. In order for the receiving node to be able to send the route reply, it is necessary for it to have a path that leads back to the sending node, which is also referred to as the source node.

If the node that is the ultimate destination already knows how to go to the node that is the original source, then it might just use the route that it has stored in its memory rather than having to figure out a new one. When the node is set to enable symmetric connections, it is possible for it to change the direction of the route that is specified in the route record. This is a possibility. Therefore, in the event that symmetric connections are not allowed, the node may initiate its own route discovery and "piggyback" the route reply onto the new route request. In the case that symmetric connections are not allowed, this is handled in the appropriate manner.

The route record and the route reply that was associated with it were transmitted back to the origin by piggybacking on the new route request, which is a procedure that is popularly referred to as "riding shotgun." When a node runs its network interface hardware in the discretionary promiscuous receive mode, it is feasible for the node to utilise the source routes and other routing information that it picks up as it passes packets for other nodes in order to update its route cache. This is the case if the node is able to use the information that it picks up.

By utilising this mode, the node is able to receive packets according to its own preferences. Following the collection of this information, the node may make use of it to determine the most effective path for the packets that it transmits to other nodes in the network. You might want to give a couple of the optimisation strategies that were discussed previously in this paragraph a go in order to enhance the effectiveness of the core Route Discovery process.

An excellent illustration of this trend that has been taking place is the fact that the search rings have been growing in size. Setting restrictions on the number of times a Route Request (RREQ) is sent, the distance it travels from its source, and the range over which it is propagated may be accomplished through the use of the Time To Live (TTL) field that is included in the header of an Internet Protocol traffic packet. Among the many applications of this subject is the limitation of the distance that it travels from its origin to other geographic places.

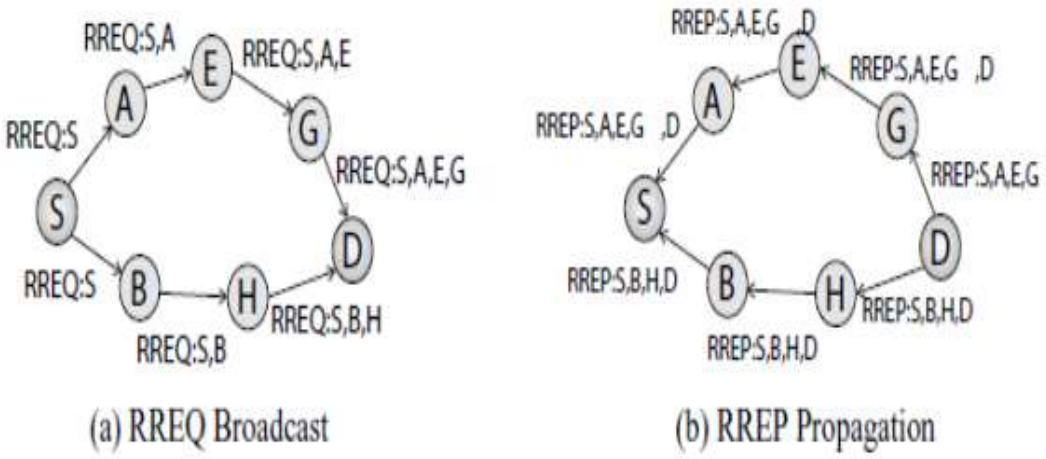

Fig.: 2.4 Dsr route discovery

Source: Evaluation of on-demand routing in mobile ad hoc networks and proposal for a secur oposal for a secure routing pr outing protocol data collection and processing through by Soke Mathew Onyemelukwe (2013)

2.18 ROUTING OVERHEAD

Routing protocols are responsible for the transmission of control packets, which ultimately leads to the production of traffic. The acquisition and maintenance of network information and routes are tasks that need this traffic to be carried out. This traffic may be measured in a few different ways, the most popular of which are the number of packets and the amount of bytes. There are several more ways as well. When it comes to methods of media access that are based on contention, such as wireless, the cost of accessing the media typically takes precedence over the cost of transmitting data per byte.

Taking this into consideration, it is clear that decreasing the total quantity of routing data should be given a greater priority than reducing the number of routing packets that are utilised. In light of this, the term "routing overhead" may be understood as the proportion of data packets to control and routing packets that are present in a certain network. The data-to-control-to-routing ratio is the name given to this particular ratio. To be more explicit, this represents the proportion of data packets that were successfully delivered in comparison to the total number of routing packets that were sent out. Examining the "routing load" statistic of a routing protocol is one approach that may be utilised to evaluate the efficiency of the respective routing mechanism.

2.19 AD HOC MODEL ROUTING PROTOCOL

Reactive (on-demand) routing protocols are the best suitable for the quick shifts and continuous mobility of MANETs because of their on-demand nature. This is because of the nature of the networking protocols themselves. In addition to the mechanics and features of the various routing protocols, evidence of this may be found in the assessment tests and simulations that have been conducted as part of the current study.

This is as a result of the fact that MANETs are made up of a large number of migratory nodes, each of which is free to go wherever it is convenient for them to do so. network up. DSR is an

on-demand routing system that simply responds to requests, in contrast to AODV, which is also an on-demand technology but possesses additional features inside its framework. Because DSR is dependent on source routing, it is extremely well-suited for the mobile and ever-changing nature of MANETs.

This is because both of these characteristics are characteristics of MANETs. It is of utmost significance that the source routing capability of DSR be working. Comparison studies and simulations have shown that DSR is superior in terms of throughput, latency, and routing overhead. These are three of the most important markers of a MANET's performance, and it has been shown that DSR excels in all three of these areas. In addition to the qualities, advantages, and disadvantages of each routing protocol that were discussed in the part that came before this one, there is one more feature that should be taken into consideration.

CHAPTER 3

SECURITY

3.1 INTRODUCTION

It is hard to overstate the relevance of network security in a multiple access network (MANET) when essential network operations such as packet forwarding and routing are taken into consideration. In the case that preventative measures are not incorporated into the structure of the system at the very beginning of the design process, there is a possibility that the security of the network may be compromised. Therefore, this is due to the fact that the framework of the system serves as the foundation upon which the system is constructed. Without the requirement for specialist nodes, ad hoc networks are able to carry out important support functions on their own.

These operations include packet forwarding, routing, and network administration. On the other hand, conventional networks, which are dependent on these nodes in order to function properly, do not have this need. Ad hoc networks are able to carry out these functions without the need for specialist nodes to be present. In addition, in order for the item to be regarded finished, it must go along a path that is widely available to the general public. As a consequence of this, it is of the utmost importance to take measures to safeguard the data while it is being transferred via wireless networks during the entirety of this procedure.

The construction of secure wireless networks presents a distinct set of obstacles that are not present in the case of wired networks. This is in contrast to the collection of issues that are presented by wired networks. A few examples of these sorts of problems are unclear topology, wireless shared media, fluctuating resources, and restricted availability.

Another example is restricted availability. These are only a handful of the difficulties that have been experienced. Due to the fact that there are various layers involved, the problem of

establishing adequate security for an ad hoc network is not limited to a single layer but rather involves numerous levels. This is because there are multiple layers involved. The challenges that are connected to the security of MANETs may be classified into two distinct groups. These categories can be used to classify the obstacles. Both the identification of secure pathways and the transmission of secure data inside MANETs fall under the first category. The second category is the identification of secure pathways.

3.2 CONTROVERSIES WITH SECURITY IN AD HOC NETWORKS

The open peer-to-peer design of MANETs is one of the most significant problems associated with these types of networks. On the other hand, this might result in concerns with the security of ad hoc networks.

Vulnerability of Channels: The operation of an ad hoc network is fundamentally identical to that of any other wireless network. Because the media is either wireless or based on radio spectrum, it does not possess any type of physical security. This is because of the nature of technology. Because of this, ad hoc networks typically begin at a disadvantage due to the fact that their capacity to protect the physical layer is extremely poor or maybe nonexistent. This is because to the combination of the aforementioned factors. Because of this, the wireless channel is accessible not just to users but also to those who are attempting to attack it.

When wireless connections are utilised, an ad hoc network becomes vulnerable to a variety of connection threats, including active impersonation, communication replay, message distortion, and passive eavesdropping, amongst others. An adversary may easily compromise the availability, integrity, authentication, and non-repudiation security objectives of a network by eavesdropping, deleting communications, and inserting fake messages. These are all straightforward ways for an adversary to do so. It is not even necessary for the attacker to have physical access to the components of the network in order to effectively carry out these assaults. Because of this, there is a chance that the network's security may be breached. This is a possibility.

Vulnerability of Nodes: In contrast to the nodes that are physically constrained to protected areas in conventional wire-line networks, the nodes that make up an ad hoc network are frequently mobile and may be moved around from place to place. Nodes are exposed to a substantial danger of having their integrity compromised or being taken over by an adversary due to the fact that they have a poor level of physical protection. As a result of this, we should not only take into account destructive attacks that originate from outside the network, but we should also give substantial weight to the possibility that attacks are launched from within the network by nodes that have been infiltrated.

In order to attain high levels of both survivability and availability, ad hoc networks need to have a dispersed architecture that does not include any central organisations. Because the entire network is rendered susceptible in the event that the centralised node is attacked and exploited, the inclusion of any central entity into a security system may result in a significant increase in risk. This is because the network as a whole is rendered exposed.

Absence of Infrastructure: Ad hoc networks are meant to operate independently of any permanent infrastructure, and they do not require any pre-existing network architecture in order to function successfully. As a result of this, the traditional and standard security solutions are not entirely appropriate since they need to be adapted to the dynamic nature of the network and the absence of infrastructure that it possesses. In addition, because there is no support infrastructure, it is possible that it will be difficult to apply standard methods for the goal of reaching a critical agreement.

Dynamically Changing Topology: In order to accommodate the mobility that is intended for ad hoc networks, there is a continuous change in topology, which necessitates the implementation of advanced routing protocols. Securing the protocols, which are already of a technical nature, offers an extra challenge. The fact that it is difficult to discriminate between the two possible sources of incorrect routing information is a key difficulty that has to be solved when it comes to routing information.

Erroneous routing information may be generated either as a result of specific alterations to the topology or by nodes that have been hacked without authorization. Additionally, trust relationships between nodes are subject to regular shifts as a consequence of the dynamic nature of the network, which indicates that nodes are continuously joining and leaving the network. In order for the trust connections to be genuine and helpful, it is possible that this occurs too frequently. As a result, it is preferable for the security methods used here to be able to adjust on the fly to these modifications. There is no absolute guarantee that the service will always be accessible since the topology is continuously changing. This is the last point, but it is an important one.

Scalability: The number of mobile nodes that comprise an ad hoc network might be ranging from a few hundred to several thousand. This is because the network is not centralised. Scalability is a highly significant problem that has a large effect on security services, despite the fact that it does not have a direct consequence on security. Scalability plays a significant role in the provision of security services. In order to address the challenges posed by such a large network, the security methods that are implemented need to be scalable.

Additionally, the limited resources that are accessible to the nodes in ad hoc networks place limitations on the cryptographic protections that may be applied on those nodes. It is possible that the attacker will be able to compromise the newly joined node in the network in the case that this does not take place. This vulnerability might then be used to gain unauthorised access to the entire system.

3.3 REQUIRED MANET SECURITY SERVICES OR MEASURES

As a unified or end-to-end security solution, there is no such thing as an ultimate solution or therapy that can guard against all active and passive assaults. This is because both types of attacks are possible. Individuals are responsible for addressing the vast majority of security breaches and threats. In order to ensure the safety of a MANET, it is necessary to make use of a number of different security services.

The functionality that is required to provide a safe and secure environment for networking is contained in the security services that are provided. In order to be able to solve the open problems that are displayed by MANETs, the security models that are capable of doing so must be able to do so while adhering to the stringent resource restrictions that are imposed in terms of the capability of computing, memory, communication capacity, and energy supply. We take into consideration the following services in order to assure the safety of an ad hoc network: availability, confidentiality, integrity, authentication, and nonrepudiation.

3.4 ASSESSMENTS IN MANETS

Mobile ad hoc networks are very dependent on the cooperative efforts of all of the nodes in order to successfully construct and run the network. In a configuration like this, the most fundamental assumption is that all of the nodes are reliable and behave appropriately. However, because of the dynamic and dispersed nature of MANETs, which lack centralized infrastructure, and the absence of centralized authority, ad hoc nodes are susceptible to being hacked and are accessible to a wide range of different types of assaults.

The following are the three primary categories that may be used to classify an attacker's behavior: Insider vs outsider against internal versus external between malicious versus rational versus passive versus active There are two different types of assaults that may be made against MANETs. Attacks against the fundamental capabilities of the MANET, such as routing and information while it is in transit.

3.5 VULNERABILITY OF EXISTING PROTOCOLS

Within MANETs, the most important operations that are performed at the network layer are ad hoc routing and data packet forwarding. These two processes are responsible for the capability of conveying data packets from their place of origin to their final destination. They interact with one another and are together accountable for this capability. In order to reach their destination, data packets are transported by intermediary nodes following a

predetermined path, and the routing states are responsible for determining the direction of this movement.

When it comes to MANETs, each and every one of the routing protocols is heavily reliant on the active involvement of the nodes in order to properly create and operate the network, as well as to offer routing between the nodes. because to the fact that they are the cornerstone of any network, attackers concentrate their attention on them the most. Additionally, they are extremely vulnerable because to the challenges that are given by ad hoc networks. The malicious nodes that have a self-interested agenda are the ones that are responsible for attacks on the physical layer, the link layer, the network layer, and the application layer. By launching both active and passive assaults against the routing protocols that are currently in place, it is feasible to achieve the desired results.

The attacker does not engage in any kind of contact with the victim; rather, they maintain silence and merely watch the communication channel during the attack. As the name suggests, passive assaults are those that are carried out in a manner that does not cause any disruption. The information that they are looking for, on the other hand, is both urgent and sensitive. When an adversary who is not actively participating in the assault listens to the channel, it is conceivable that packets that include sensitive information (including, among other things, an IP address, data, or the position of nodes) will be taken advantage of. A violation of confidentiality has occurred here.

Since passive attacks do not produce any new traffic in the network and have a little impact on any of the traffic that is already present, it is extremely challenging to identify them in wireless networks for this reason. It is possible for self-centered nodes to carry out passive attacks with the purpose of conserving energy for themselves by not actively participating in the transmission of messages. "Passive attacks" In spite of this, it is possible that the networks may become fragmented, which would result in a decrease in their level of performance. The nodes are the ones who carry out the passive assaults.

On the other hand, active assaults are those that are carried out by malicious nodes and involve actions that are both damaging and capable of invasive behaviour. Active attacks tend to be carried out by hostile nodes. An active attacker will violate the network's availability, integrity, authentication, and non-repudiation precepts by, among other things, injecting packets into the network with wrong destinations, deleting packets, changing the contents of packets, and impersonating other nodes. This will allow the attacker to get access to the network. On the other hand, authentic nodes in an ad hoc network could be able to recognise active attacks and, in the long run, figure out a means to navigate around them. An assault that is being carried out in secret cannot be identified or stopped since there is no method to do so.

3.6 ACTIVE ATTACKS:

Denial of Service: It is intended to cause full havoc with the routing function, and as a result, with the functioning of the Ad hoc network as a whole. The attacker overwhelms the nodes with continuous ads or broadcasts, which stops the nodes from functioning normally and prohibits them from participating in the scheme. It will seem as if the flooded node is inaccessible from the other legal nodes. The routing overflow attack and the sleep deprivation assault are two examples of specific kinds of denial-of-service attacks that may occur.

Black Hole Attack: In this form of attack, the hostile node responds to route requests it receives by sending fake route responses (RREP). Because of this, the bad node will advertise that it can reach the target node more quickly than any other node, which will allow it to intercept more packets. It aims to collect packets from a certain node, which is called the target node. One conceivable goal in creating these false replies is to direct network traffic to a malicious node so that it can spy on other users or launch a denial-of-service attack by rejecting all packets that arrive at the malicious node.

These false responses might be utilised for eavesdropping or to direct all traffic to the malicious node. Furthermore, if an adversary has the best or nearest path, they can persuade the node's neighbours to send packets via them based on their best metric. Because of this, the

packets would end up going via the enemy. It occurs when the assailant declares a metric of zero for every target they plan to attack. Instead of continuing their attack, the attacker will stop and discard the packets in this case.

Furthermore, a black hole may launch an attack on a node if it makes an arrogant presentation. When a node takes use of the services provided by other nodes and the resources, they possess in order to protect its own resources, it is being selfish. The node's selfishness means it won't contribute to the MANET's functioning by forwarding packets; instead, it will just discard all packets that pass through it, which might compromise the network. Because the network could be compromised, this poses a risk to the network. A black hole attack is the name given to this kind of attack.

Gray Hole: This is the situation in which a node in an established MANET routing architecture loses packets selectively with a specific probability, generating a distraction on the network. It has the ability to discard some ones while continuing to send all of the packets on to other nodes. It's also possible that it may act maliciously for a period of time by dropping packets, but then it will revert to its usual behavior afterwards. There is also the possibility that a gray hole may display behavior that is a hybrid of the two described behaviors above.

Byzantine Attack: When authentication and packet integrity are compromised, this attack occurs at the network layer. Through packet rejection, improper path forwarding, or the generation of routing loops, these attacks impair routing services and are carried out by groups of intermediary nodes inside a network. They achieve this by manipulating the network to suit their purposes.

Partition: A network may be partitioned into two distinct sets by severing the connection between two distinct groups of nodes. In this kind of cyberattack, the malicious node or group of nodes seeks to divide the network in order to stop one group of nodes from communicating with the other group. This is accomplished by inserting faulty routing packets and keeping the route busy until the partitioning process is finished.

Node Isolation Attack: The OLSR protocol may be the target of such an assault. The objective of this attack is to isolate the targeted node by cutting off all communication with other nodes in the network. Among the many methods at an attacker's disposal, one is to prevent the propagation of a node's or group of nodes' connection information throughout the network. In order to build a route to target nodes and transmit data to them, other nodes must have access to their connection information. If these other nodes can't access the information, the data will never reach its destination.

Wormhole Attack: In order to pull this off, the attacking nodes must work together. This form of assault is also known as a tunnelling attack. A tunnelling assault occurs when many nodes collaborate to encapsulate and communicate over already established data channels. One or more nodes in the network can exploit this vulnerability to bypass the usual network traffic flow; if this happens, two or more malicious actors can take control of the network.

To simplify, the evil nodes in the network create a tunnel or other form of communication shortcut so that they may send packets to each other. Wormholes allow packets to seemingly go over legitimate routes, while in reality they are being tunnelled to the malicious partner's node. Verifying the existence of these tunnels is an arduous task.

Session Hijacking: This is an assault on the transport layer. The TCP protocol is the primary emphasis, and the frequency of the TCP handshake is used to full effect. In MANETs, TCP authentication is only performed at the beginning of a session. Because of this, an attacker may take advantage of the lack of authentication while a session is in progress by hijacking the connection in order to get unauthorized access to private information.

Malicious Code: An assault against the application layer has been launched. Injecting harmful software such as viruses, spyware, or worms into a network in order to accomplish purposes such as hurting other nodes or gaining access to secret information is included. The network will eventually get damaged as a result of this.

Jellyfish Attack: The rogue node sneaks its way into the network's forwarding group and then unfairly slows down the transmission of data packets by delaying them for a certain length of time before sending them on. Real-time application performance is negatively impacted as a direct consequence of the greatly increased end-to-end latency and delay jitter that it causes.

Spoofing: When a rogue node does this, it assumes the identity of another node. It makes it more difficult to see the topology of the network.

Sybil Attack: The attacker makes it seem as if they have several identities or nodes. Either through impersonating other nodes in the network or by simply asserting fake identities, a single node may take on the behavior of a large number of other nodes. As a result, sending communications having a variety of source identities that were manufactured.

Replay Attack: An attacker that is carrying out a replay attack will inject traffic that they have previously recorded into the network in order to reroute it. This attack often focuses on the newness of routes; however, it may also be used to identify security mechanisms that have been inadequately constructed.

Blackmail / Black list Attack: Importantly, this attack is spreading to routing systems that employ methods for detecting malicious nodes and that keep track of suspected harmful nodes on a list (a black list). It is common practice for nodes to keep details regarding other nodes that are deemed malicious in a blacklist. In this case, an attacker might intentionally mislead other nodes in the network into thinking a certain node is malicious, leading to the blacklisting of that node and the subsequent isolation of legitimate nodes. This is where the non-repudiation security feature, which associates a node with the communications it has generated, might come in handy.

3.7 ATTACKS TARGETING DSR ROUTING PROTOCOL

We are focusing on problems with the ad hoc routing protocols' specifications rather than those with the IEEE 802.11 standard, which means that the routing methods now used for

mobile Ad hoc networks are susceptible to a wide variety of attacks. The same kinds of attacks can compromise wired networks, but the design of wired networks makes them more resilient to such attacks.

It is not necessary for the routing protocol to be unstable or weak for basic denial-of-service attacks based on non-cooperation and interception to succeed; such attacks are possible in any ad hoc routing system. Ad hoc routing systems are susceptible to assaults that fall into one of three broad categories: modification, impersonation, or invention.

3.8 ASSAULTS WHO USE MODIFICATION

A denial of service and traffic redirection can be caused by malicious nodes by altering control message fields or sending routing messages with fake values. This may occur during the forwarding of control messages. The accompanying graphic depicts a network where a malicious node M can divert traffic away from the advertised route to X by suggesting a faster alternative.

Fig.: 3.1 The Basic Ad Hoc Network

Source: Evaluation of on-demand routing in mobile ad hoc networks and proposal for a secur oposal for a secure routing pr outing protocol data collection and processing through by Soke Mathew Onyemelukwe (2013)

Redirection with modified hop counts: Modifying the hop count field in route discovery messages makes it feasible for an attacker to carry out this attack. The hop count field is the statistic that is used by DSR to decide which route is the shortest. During the process of route

discovery in DSR, hostile nodes have the ability to tamper with and manipulate the hop count field of the RREQ. Because DSR makes use of source routing and keeps a record of the nodes that it passes through, a malicious node that is traversed by DSR has the potential to alter the RREQ header by adding or deleting nodes in order to achieve a diversion and routing via another route.

Denial of Service with modified source routes: One simple way to target DSR with a denial-of-service attack is to alter the source paths listed in the packet headers. These first paths clearly show the paths that have been or will be taken. The absence of integrity check methods throughout the source pathways of DSR is to blame for this. Figure 3.2 indicates that a hostile node M will execute a denial-of-service assault if the shortest trip from S to X passes via M. The reason behind this is that M is now following the quickest route.

Before attempting to communicate with X, S will check its route cache for a current path to X. If so, it will include the source route in the packet's header and transmit data packets to X. Malicious node M may alter the packet's source path upon receipt by adding or removing nodes such as node D from its header. C will not be able to find a next hop node on the source route given in the packet header when it gets the modified packet and tries to transfer it to X. Since C is compelled to reject the packet due to this, the transmission will not succeed.

Fig.: 3.2 More examples of ad hoc networks

Source: Evaluation of on-demand routing in mobile ad hoc networks and proposal for a secur oposal for a secure routing pr outing protocol data collection and processing through by Soke Mathew Onyemelukwe (2013)

In the event that the forwarding node does not get confirmation that the packet has been received by the subsequent node along the route, the packet will be reissued an infinite number of times, up to the maximum number of times that are authorised. It is the responsibility of the node that is forwarding the packet to guarantee that it has been successfully delivered to the destination that it was meant for, despite the fact that DSR does provide a way for route maintenance. was obtained.

In the event that the packet is not acknowledged as having been received, it is strongly suggested that it be resent until the maximum number of attempts has been achieved. This node is the one that is responsible for communicating an error message to the sender in the event that the node in front of it has not validated that it has received the message.

As a consequence of this, if C were to send a route error message to S, S would receive it; but, given that M is the first hop on the RERR message's journey back to the source node S, it is possible for M to dismiss the message and proceed with its denial-of-service attack. This is because C is only aware of one possible route to X along which the denial-of-service attack may be completely successful, and that route is the erroneous route. This is the sole reason why this is the case.

Considering that DSR makes use of route salvage, which is a maintenance approach for recovering from damaged connections along a path, this assertion is founded on the fact that DSR uses route salvage. The premises upon which this statement is based are provided by this. It is the responsibility of the upstream node to execute a lookup on the route cache in order to ascertain whether or not there is an alternate path to the destination. If you make any changes to the source route in DSR, there is a possibility that the path that has been supplied will become a loop.

Tunneling: As was previously said, A tunneling assault is carried out when numerous nodes cooperate together to transmit and receive messages silently across existent networks in an effort to circumvent security measures. It's possible that a cyberattack may be started using

this way. Malicious nodes M1 and M2 are working together in the situation represented in Figure 3.3 to carry out a tunneling attack.

They do this by delivering tunneled route request packets, which are referred to as RREQ in DSR source routing. These packets fraudulently inflate the lengths of all potential pathways. The thicker colored lines denote the tunnel, whereas the solid black lines denote the real connections that exist between the nodes. The route that M1 and M2 incorrectly presume is between them is represented by the dashed lines.

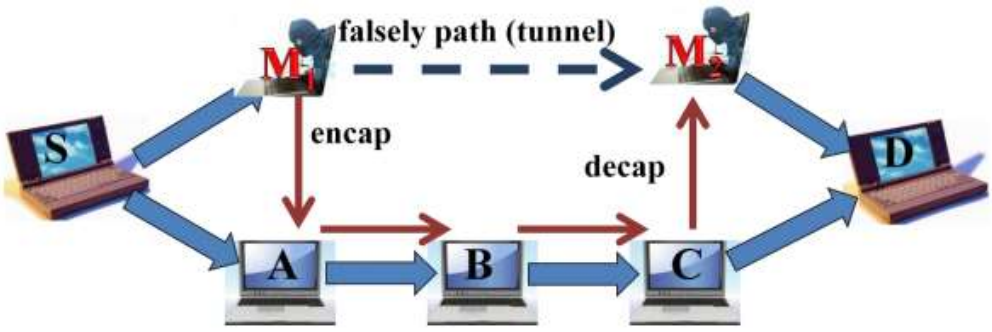

Fig.: 3.3 Tunneling spoofs path lengths

Source: Evaluation of on-demand routing in mobile ad hoc networks and proposal for a secur oposal for a secure routing pr outing protocol data collection and processing through by Soke Mathew Onyemelukwe (2013)

In this particular situation, the process of route discovery is initiated by a node S that has the intention of transmitting or connecting with a node D located at the destination. RREQs are transmitted from the source node S to the nodes that are directly next to it through a broadcasting transmission. In the case that S provides M1 with an RREQ, M1 will encapsulate the RREQ and tunnel it to M2 by utilising a data channel that has previously been created. The data path used in this particular case is It is passed on to D as if it had only travelled via this route, which is marked by the notation S-M1-M2-D, when the encapsulated RREQ is delivered to M2.

This is because the route is denoted by the notation. There will be no modification to the packet header by either M1 or M2 to reflect the fact that the RREQ was also sent over the path 'A-B-C'. Due to the fact that M1 and M2 do not have access to the packet header, this is the result. There appear to be two routes from the source node S to the destination node D, both of which have unequal hop lengths. These routes are referred to as "S-A-B-C-D" and "S-M1-M2-D." After route discovery, it appears that there are two routes. Therefore, S would make the erroneous assumption that the route to D that goes through M1 is a better alternative (in terms of hop counts) than the one that goes through A. This would bring about the inaccurate assumption.

3.9 ATTACKS THAT USE SPOOFING OR IMPERSONATION

This kind of attack takes place when a node in the network gives false information about its identity. This may be accomplished by changing the MAC or IP address of the device in the egress packets, and it is straightforward to combine this tactic with modification attacks.

Routing Loops by Spoofing: Using figure 3.4 as a guide, let's assume that connectivity exists not just between the five nodes shown there and a distant destination, X, but also between the nodes themselves, as indicated. In this example, person A is able to hear people B and D, person B is able to hear people A and C, person D is able to hear people A and C, and person C is able to hear people B, D, and E. While M is able to hear A, B, C, and D, E is only able to hear C and the following hop along the path leading to X.

Because this architecture in DSR has been optimized to allow for promiscuous listening, it can be discovered by an adversarial attacker, M. The RREQ/RREP interactions that take place while M is in the process of route discovery might provide it with information regarding this topology. In order for M to carry out a looping attack, it is necessary for it to first move out of range of node A while simultaneously moving closer to node B, and then it is necessary for it to alter its MAC address such that it is identical to node A's. After then, it will respond to the RREP sent by node B with a metric/hop count of zero, which is a value that is lower than

the one that was provided by C. This will take place immediately after the one before it has finished its course.

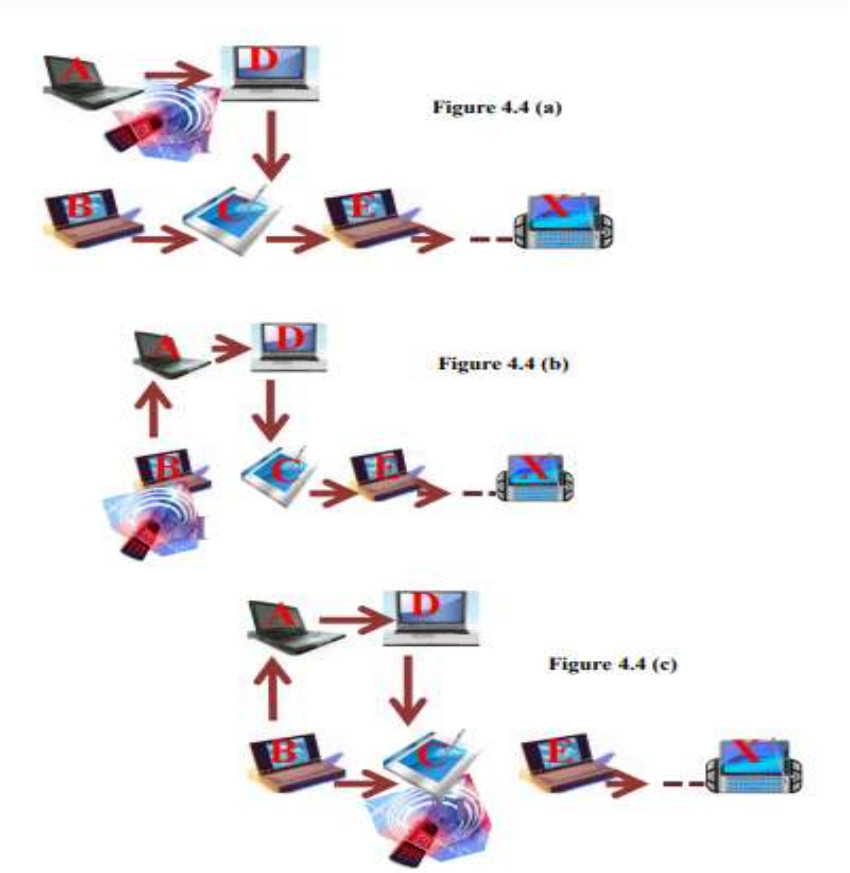

Fig.: 3.4 A series of activities that include packet spoofing to create loops

Source: Evaluation of on-demand routing in mobile ad hoc networks and proposal for a secur oposal for a secure routing pr outing protocol data collection and processing through by Soke Mathew Onyemelukwe (2013)

B is going to make the required adjustments. its path to the destination, X, to travel via A since it has found a route that has a lower hop count. This is depicted in the following diagram. After M has accomplished this goal, it will modify its MAC address such that it is identical to B's while simultaneously moving out of B's range and closer to C. After that, it will transmit

to C an RREP that has a hop count that is X less than what E advertised it to have. Following that, C travels to X by way of B, as seen in figure 3.4. After this point, a loop has been created, and X can no longer be reached from any of the four nodes.

Attacking a partition via spoofing: Spoofing is used to do this in precisely the same manner as described in the routing loops. Because to an oversight, the network is accidentally segmented into partitions, as seen in.

3.10 ATTACKS USING FABRICATION

It is possible to launch attacks using MANETs by generating and spreading bogus routing packets. These kinds of attacks may be difficult to verify and are sometimes difficult to separate from legitimate routing signals. This is particularly plausible in the case of manufactured route error messages RERR that suggest there was a breakdown in contact with a neighbor.

Falsifying DSR Route Errors: With the help of path maintenance and fixes, DSR may restore broken routes when MANET nodes relocate. Given that the node serving as the source was The first step in rerouting a device is to create and send route request RREQ messages to both the device that moved and the one that still needs the route. We do this because we still need to tread this route. Meanwhile, if the node at the end of an active path or one of its intermediates moves, the node upstream of the break will notify its active upstream neighbours of the link break with a route error message called RERR.

After that, it will remove the destination's route from its route cache. When a link is severed, something occurs. This paves the way for the transmission of bogus route error signals through a hole in the MANET's routing technology. Since there is no safeguard in place, an attacker might potentially exploit the system.

The route from node S to node X may be seen in Figure 3.5; it passes through nodes A, B, C, and D. Any sequence is acceptable for travelling this course. By sending route error signals

to B, a malevolent node M can block service to a naive node X. To achieve this, send a deluge of route error signals to B. These signals suggest that the connection between nodes C and X has been broken. Here, an adversarial node called M masquerading as node C is the key player.

After that, Node B will get the message, but it will incorrectly assume that Node C was the source. The truth is that Node C was the true sender of the message. After that, node B will notify node A of the route fault and remove its item from the routing cache related to X. This allows M to spoof and broadcast fake RERR packets, thereby disrupting S and X's connections.

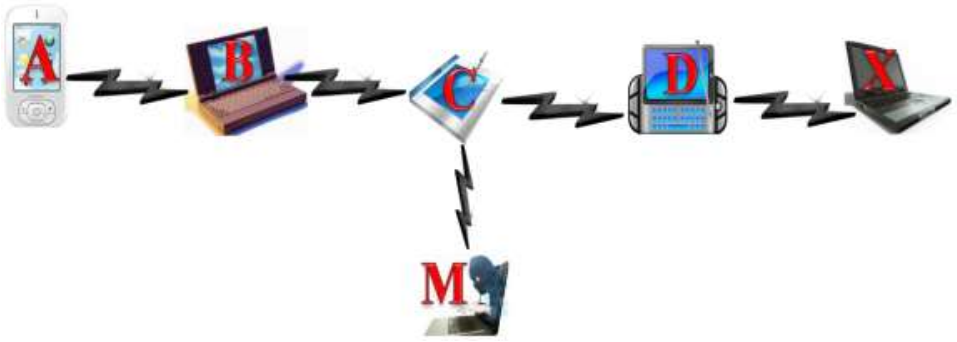

Fig.: 3.5 Network Ad-Hoc - Fabrication

Source: Evaluation of on-demand routing in mobile ad hoc networks and proposal for a secur oposal for a secure routing pr outing protocol data collection and processing through by Soke Mathew Onyemelukwe (2013)

DSR Route Cache Poisoning: An example of a subtle assault on the routing system's security is poisoning route caches. The corruption of routing information due to poisoning route caches is an example of an indirect attack. The deletion, modification, or injection of incorrect data into the nodes' route caches might cause this to happen. It is possible that these three outcomes will occur. This is a real risk with wired networks, but typically it's easy to protect against thanks to well-established designs and router-level security mechanisms. This benefit is not available with wireless networks.

One way to find routes in DSR is to look at the packet headers as they are processed by nodes along the path. Another way is to listen promiscuously. It is also possible to perform this in addition to figuring out the routes from the packets. Think of a network where a route from S to X passes through A, B, C, and D as an example. If a different node happens to overhear a packet on route from S to X and decides to save the path in its route cache, it might be because it is now travelling between S and X.

The attacker can swiftly contaminate route caches by taking advantage of route learning's promiscuous nature. One example is when a malicious node M pretends to be node X but really sends out packets that really came from node M. One possible way to poison traffic to another node X is this. The intended destination for these packets is X. A neighboring node that is listening promiscuously and overhears the packet exchange can save the route in its internal database if it already knows it. An attack of this security hole may significantly degrade a MANET's state and routing architecture.

Wirelessly connected mobile computer devices (nodes) constitute mobile ad hoc networks, which are often called wireless mesh networks of mobile nodes or just mobile ad hoc networks. These networks are also known as MANETs. Unlike cellular and wireless local area networks, this network design does not rely on a central hub or any type of access point. Since nodes in a wireless network can move in any direction and arrange themselves anyway they choose, the network's topology might change unexpectedly and suddenly. The Internet, the largest network available at the moment, may be accessed through these networks, or they can function independently.

Although traditional mobile wireless networks rely on a central coordinator to ensure smooth operation, MANETs are able to self-organize and continue functioning. Wireless communication between mobile nodes is possible when they are in radio range of each other. Interactions between mobile nodes are possible. But for this kind of communication to happen, there has to be supplementary nodes that mediate between mobile nodes that are

geographically farther away. In a mobile ad hoc network, each node doubles as both a host and a router all at once.

While hosts may send and receive data, routers are in charge of relaying that data to other nodes in the network. Among the many terms used to describe these types of networks is "multi-hop wireless ad hoc networks." Figure 3.6 shows the mobile ad hoc network and the associated communication technologies. Ad hoc networks can consist of a wide variety of devices, including PCs, PDAs, mobile phones, and more, as shown in. At full functionality, each node in the network may communicate directly with any other node within its range, independent of whether they are on the same network or not. In order to communicate with devices beyond of this range, an intermediate device must be used to hop-by-hop transmit the messages.

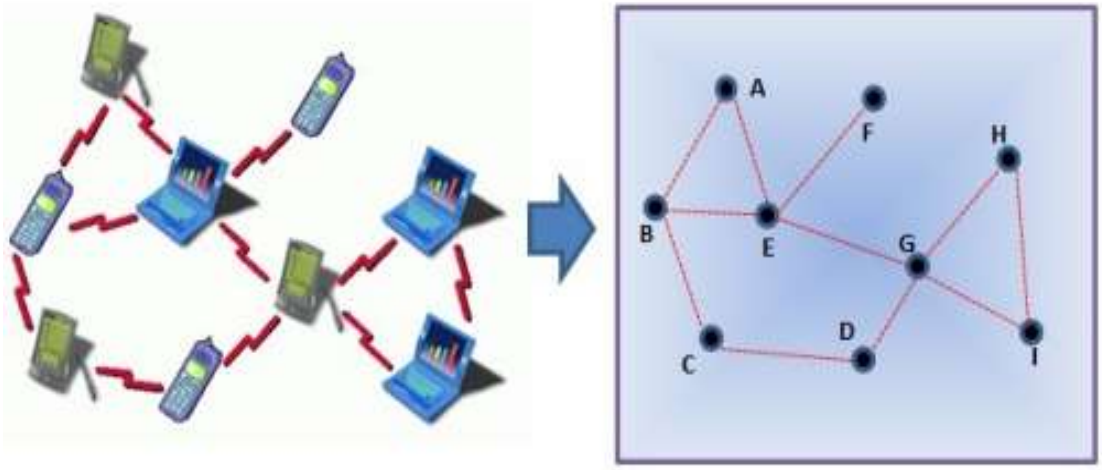

Fig.: 3.6 A Mobile Ad-Hoc Network Example

Source: Evaluation of on-demand routing in mobile ad hoc networks and proposal for a secur oposal for a secure routing pr outing protocol data collection and processing through by Soke Mathew Onyemelukwe (2013)

3.11 CHARACTERISTICS, COMPLEXITIES AND DESIGN CONSTRAINTS

The constraint of putting up infrastructure is eliminated by mobile ad hoc networks, which also enable devices to establish and join networks while they are on the go, at any location, at any time, and for nearly any purpose. On the other hand, these nuances of flexibility and convenience do come with a price tag attached to them. Not only are mobile ad hoc networks susceptible to the common problems that are associated with wireless networking in general, but they are also vulnerable to the limitations that are specific to ad hoc routing. A summary of some of the most critical features, challenges, and design restrictions of MANETs is provided in the following paragraphs.

Dynamic and changing network topology: As a consequence of the fact that nodes in mobile ad hoc networks are free to move anywhere they like, the topology of the network, which is often multi-hop, is subject to frequent and unpredictable shifts. This may lead to route alterations, frequent network splits, and even possible packet losses.

Wireless medium: Nodes in an ad hoc network connect with one another via wireless methods and share the same medium (such as radio, infrared, and so on). The wireless medium does not have any absolute bounds or boundaries that can easily be seen, and stations are unable to receive network frames if they are outside of these boundaries. Because of this, the channel is not shielded from signals coming from the outside, making it substantially less dependable than media that is connected.

Limited availability of resources: The quantity of different services and applications that a mobile node is capable of providing is limited by the amount of computing power that it possesses. This is due to the fact that the batteries that are included within each mobile device only hold a limited amount of energy. Because each node in a MANET serves as both an end system and a router, the transmission of data packets in a MANET consumes more power. This is far more challenging than it would be in a standard network.

Autonomous and infrastructure less: The MANET technology can function without the need for a preexisting framework or a centralized management. Each node in a distributed peer-to-peer system functions as a router on its own and produces data independently of the other nodes. When the administration of the network needs to be divided among several nodes, both the identification of faults and their control become significantly more difficult.

3.12 PROBLEMS WITH SECURITY IN MOBILE AD HOC NETWORKS

Mobile ad hoc networks are susceptible to a wide range of kinds of attacks, both active and passive, which can be conducted against them. In comparison to other systems, it is significantly more vulnerable due to the fact that it does not possess a centralised authority and its resources are restricted. Based on the location of the malicious node that is responsible for the attack, attacks are divided into two distinct groups: internal attacks and external assaults. These categories are segregated according to the location of the malicious node. In addition, it is possible to separate it into two distinct types, namely aggressive attacks and passive attacks, based on the method in which it is carried out.

In the context of wireless networks, mobile ad hoc networks, sometimes commonly referred to as Manets, are a sort of network in which information may be transferred between mobile nodes without the help of a predetermined network. An architecture for communications that is based on peer-to-peer interaction is utilised in these networks, which are also referred to as spontaneous networks. Because of this, the nodes in the network are able to communicate with one another in a direct manner.

Due to the absence of an underlying infrastructure that can provide support for the network, the routing services are established through a collaborative process. Additionally, every node that is a part of the network can function as a possible router for various other nodes. Consequently, in the case that one node desires to communicate with another node that is not within the range of its link, that node will send its packets to a neighboring node that is situated in a location that is closer to the node that it needs to communicate with.

After then, the packet will be sent to the target node via the neighboring node on its way. As a result, Manets are multi-hop mobile networks that make use of collaborative routing to ensure that nodes in the network are connected to one another. The mobile nodes that make up a Manet are the most important part of the system. Each of these mobile nodes is outfitted with a wireless local area network (LAN) interface or several interfaces. It is expected that wired connections would continue to perform better in terms of capacity than wireless ones in the great majority of situations.

Not only do wireless networks face challenges that are specific to their transmission method, such as multiple-access effects, fading, noise, and interference from electromagnetic sources outside the system, etc., but there are also differences and limitations in terms of the nominal throughput of an interface (the maximum transfer rate of the radio link is generally lower than the nominal rate of wired links). Wireless networks are a relatively new technology. methods of transmission, such as multiple-access effects, fading, noise, and interference from electromagnetic sources that are external to the system, among other things. On account of this, the actual data transfer rate of a radio link is frequently lower than the data transfer rate that is advertised for a cable link.

This is a direct result of the fact that this is the case. Due to the fact that wired connections often have a greater maximum transmission rate than wireless connections do on average, this is the reason why this difference exists. Furthermore, mobile nodes require a portable power supply, which often takes the form of batteries that will eventually run out of power. This is a fundamental requirement for mobile nodes. To ensure that the resources and services that have been developed expressly for Manet are utilised to their full potential, it is essential to make the most of the available bandwidth and power.

Inside a Manet, the nodes of the network have the ability to move around constantly and at any time inside the network, as well as to emerge and disappear. The nodes of the Manet are constructed in a manner that is dynamic as a direct consequence of this, and the topology of

the network is prone to frequent and unforeseen changes as a result of this. Because of this characteristic, which is tied to the mobility of the nodes, as well as the limited trust and bandwidth of wireless connections, it is difficult to ensure that a certain node will always be available. This is because of the fact that. As a consequence of this, the services that are offered inside a Manet are not capable of being consolidated into centralised entities.

On the other hand, and in the same way that routing services are provided, the services in a Manet need to be provided in a manner that is distributed and self-organizing, through communication and collaboration amongst the nodes of the network. It is common practice for this form of collaboration to make use of the inherent redundancies that are the result of the communication paradigm. The lack of assurance regarding the availability of individual nodes is somewhat compensated for by these redundancies, which serve to compensate for it to some degree. In order to establish these networks, the Manet that was demonstrated before is differentiated by two key services: routing and autoconfiguration. These services are necessary in order to create any network.

There is an inextricable connection between the multi-hop design of Manets and the routing function that it offers. The routing protocol needs to be created in a manner that enables it to adapt to the constant variations in the network architecture that are brought about by the mobility of the nodes. This is because of the fact that the mobility of the nodes is a significant factor. There is also the possibility of the nodes being automatically connected to the network through the utilisation of the autoconfiguration service, which enables rapid deployment with minimal intervention from end users. The purpose of this study is to provide a unique security model in order to solve the one-of-a-kind difficulties that occur in environments that are suitable to the utilisation of ad hoc networks.

Through the course of this project, a collection of distributed and interoperable security services will be developed and put into operation. These services will be able to be provided by the nodes of a Manet working together. This will be the objective of the project. As a

consequence of this, it will be possible to provide the services in a manner that facilitates their distribution. In addition, this set of services must be flexible enough to offer varying degrees of security that may be customised in accordance with the particular requirements of each and every distinct use case for the Manet application.

The architecture that was recommended is immediately put into effect and worked upon in order to ensure that the essential functions that are provided by a Manet remain uncompromised. There are several features that are incorporated, but two of the most crucial ones are routing and auto-installation.

Despite the large number of recent studies that have been written on the topic, the problem of security in ad hoc networks is still considered to be a relatively new topic in the professional technical literature. The vast majority of these efforts are conceived of as independent methods that are intended to solve certain types of security challenges.

The development of alternative security techniques that are capable of being tailored to the environment of a particular application or protocol, such as a routing protocol, is a key focus of attention. When compared to other projects, this one stands out as being particularly remarkable owing to the fact that it provides a security solution that is not restricted to just one ad hoc setting but is applicable to all of them. This makes it a very noteworthy endeavour. This is done in order to give security levels that are adjustable enough to meet the requirements of the Manet application and to make it feasible for the application to be utilised in settings that comply to a diverse set of security rules.

3.13 APPLICATIONS FOR MANET

A diverse range of requirements must be satisfied by both the existing and forthcoming technology for ad hoc networks. The functioning of Mobile IP2 is currently receiving a lot of attention, which means that the developing field of mobile and nomadic computing will soon require network technology that is exceptionally adaptable. These techniques need to be able

to exert control over ad hoc networks that are made up of a great number of hops and either function independently or are connected to the larger web. The utilization of Manet technologies is specifically related to the rise in the number of impromptu connections made across networks.

In point of fact, ad hoc networks are the result of the notion of self-organization, and they offer a flexible alternative for the development of networks. Mobile network setup may be accomplished in a snap and with little effort with the assistance of ad hoc networks. to construct equipment in advance. Within this framework, there are numerous potential uses for Manets in a variety of settings, including commercial, industrial, academic, governmental, or military applications, such as the following:

- Collaboration and cross-group communication are popular practices in many different industries, including business, education, and the corporate world. These methods are used to achieve common goals.
- Peer-to-peer networking is used in PANs, also known as personal area networks, to permit communication in environments in which a more comprehensive network infrastructure would be difficult or even impossible to implement.
- The following are examples of survival scenarios that call for quick communication via changing networks: operating in locations with either no infrastructure or infrastructure that has been completely destroyed. Instances such as accidents, sabotage, fires, collapses, and remote maintenance are examples of the kinds of things that fit within this category.
- Sensor networks are the networking of several sensors, some of which may be mobile, for the purpose of exchanging and processing information pertaining to the measurements that are being produced.
- Moving networks are networks that are composed of systems that are in motion, such as airplanes, automobiles, or soldiers moving across a battlefield.

The Manet technology has other uses as well, including ubiquitous communication and the construction of networks that can be accessed from any location. Because of this, link-based

mobile ad hoc networks have the potential to be an effective alternative to conventional cellular mobile networks or a useful addition to these networks.

3.14 VULNERABILITIES OF AD HOC NETWORKS

A significant number of the security flaws that are typical of traditional network topologies are also present in Manets. In the meanwhile, some of the unique qualities of Manets highlight these vulnerabilities because they provide new methods in which they may be exploited. This is the case because these traits offer new ways in which they can be abused. In addition to this, Manets are susceptible to their very unique one-of-a-kind vulnerabilities, which do not apply to other network topologies. The following are some of the most notable features of Manets, all of which highlight existing flaws in conventional networks or include new vulnerabilities that are unique to the ad hoc setting:

- This is as a result of the following factors: the mobile nature of the network topology;
- The decentralized peer-to-peer communication model;
- The dependence of the nodes on one another to establish and maintain network connectivity; the collaborative communication model;

Because of these qualities, manets are more susceptible to a wider variety of assaults than wired networks are. Some examples of these attacks include passive listening, spoofing (which is when one entity takes the identity of another), and denial of service. An adversary may take use of these traits to: continuously pay attention to broadcasts coming from adjacent nodes.

- Move in order to collect information on the activity of other, more distant nodes or to avoid being monitored by nearby nodes;
- Communicate directly with any node that is within its range of transmission;
- Provoke unnecessary activity in order to discharge the power sources of other, more heavily used nodes more quickly;

Traditional networks also entrust tasks like routing and autoconfiguration to entities designed to be secure, such as servers that handle autoconfiguration and routing. The safety of the network is the responsibility of these organisations. Due to their specialised role and distinct placement within the network architecture, these entities are better able to withstand external attacks. Because they don't have generic functions, can disable features they don't need, and can activate protection based on their position in the network's architecture (usually at points of concentration or centralization within controlled parts of the network), these entities have a reduced set of vulnerabilities. There is a lower set of vulnerabilities because of all of these things.

There will be fewer exploitable vulnerabilities as a result of this. In contrast, all of the network nodes in Manets are given the chance to take part in the decentralised delivery of the essential services and other network services. Computer hardware with generic software and hardware commonly implements these nodes. Consequently, the hardware housing these nodes is open to a slew of security flaws related to the OS, bugs in the software, backdoors, viruses, and the like. Furthermore, a Manet node can be taken over if its physical security is inadequate.

Because of this, it is common for parts of the network to be broken or compromised. An incorrect entity might be a node that is assaulting the Manet and decides to move to another part of the network or hide from its neighbours, depending on the situation. It is feasible to have both of these outcomes. This feature makes it difficult to spot attacks and distinguish between legitimate nodes in the network and those that are malicious.

3.15 ADHOC NETWORKS' REQUIREMENTS FOR SECURITY SOLUTIONS

To protect Manets's other network services, the recommended security solution comprises creating a unified suite of security services. As part of our research, we are looking at this solution. Two distinct types of criteria are considered in this case. In this first section, we will outline the general requirements that all of the services running on a Manet's network must meet. This includes the prerequisites for establishing security services.

After that, we'll provide the actual security requirements, which will let us figure out and build all the security services that our model will need. In order to design a service that works with this type of network, we need to establish certain baseline requirements. One way to achieve this is to look at what makes Manets special. Following this, we will review the key points of Manets and the subsequent requirements for network services:

- There can be no concentration points, and there is no assurance that individual nodes will be available. A dispersed strategy is what is required for the Manet services.
- Capacity constraints in terms of both bandwidth and power supply: the services must not produce an excessive amount of overhead in the network. This will allow the services to be delivered locally whenever it is feasible, hence avoiding the need for relaying and retransmission of messages.

When it comes to the creation of security services in general, it is necessary to take into consideration the requirements that were originally specified. It is important to keep in mind that the bulk of the security methods and safeguards that are used with ad hoc networks are not advised. The only exception to this rule is certain security services, which can only operate correctly when they are isolated on the local host. The services of access control, authentication, authorization, monitoring, and security management are frequently coupled with endpoints that are explicitly defined in standard architectural layouts.

Additionally, this is true for other services that are associated with security, such as monitoring and the management of data storage. Just two examples of this form of infrastructure are firewalls and authentication servers. Other examples include other types of infrastructure. Manet's art is characterised by these characteristics. There is no exception to the rule that components cannot exist as independent devices of any type. As a consequence of this, the security services that are run inside these networks are required to implement a decentralised approach that is founded on the principles of collaboration and independent organisation. Additionally, this cooperation must be totally local if it is at all possible to do so.

This is done to ensure that the communication and processing overheads are kept to the region immediately surrounding the nodes that are participating in the activity. The purpose of this section of Manets is to describe a variety of approaches to determining the requirements for security. Within the scope of this study, we explore the integration of two key requirements: the identification of trustworthy and untrusted Manet nodes, as well as the identification of hacked or misbehaving nodes and the subsequent isolation of such nodes (afterward). Nodes are differentiated from one another by the construction and deployment of a trust model, which describes the requirements that must be completed before a node can become a member of the network.

This distinction is made possible by the fact that the trust model provides the requirements. It is necessary for nodes to become part of the network and develop what is referred to as "mutual trust" among themselves in order for them to be able to accomplish their function as the initial line of defence for shared services. Due to the fact that cooperation can only take place between nodes that are logically connected to one another, it is necessary for the nodes to have been members of the network in the beginning. When it comes to this hypothetical scenario, nodes will only share control information and relay packets among themselves when they have demonstrated that they are trustworthy.

Due to the fact that wireless communications are inherently promiscuous, there is no requirement to expressly join the network in advance while using these types of communications. There has been an increase in the requirement for explicit network engagement. This is due to the fact that every device that is equipped with a wireless interface has the capability to connect with other nodes that are part of a network. As a result of the unpredictability of the manet environment, the mobility and flexibility that wireless networks provide are of even greater significance.

A node is expected to be able to tell the other nodes of its engagement in a network after it has become a member of that network. Additionally, it must provide those other nodes with

the ability to independently verify its network membership status. Another key requirement for a Manet is the presence of entities inside the network that have been broken or hacked in some way.

This is a precursor condition. Due to the fact that the existence of such entities cannot be disregarded, the security services need to be built in such a way that they continue to operate properly even when there are nodes present that have been compromised or that are behaving in an improper manner.

In this sense, we are only able to let the performance deterioration that is brought about by the presence of nodes that are incorrectly integrated with the network to be temporary. Before the reliability of the service is put in jeopardy, it is necessary to identify and remove the nodes that have been erroneously integrated from the cooperative services.

As was said before, there are many different contexts in which manets might be utilised. This is the last but not the least point. It can be said with absolute certainty that the required level of safety would change based on the specifics of the situation. The levels of security that are required for a Manet that is set up to facilitate collaborative work in a classroom are therefore different from those that are required for a Manet that is set up to offer communication and information services for a rescue effort in an area that has been affected by a catastrophe. This is because the former Manet is intended to facilitate collaborative work in a classroom setting. In a similar fashion, the levels of security at a Manet site that is located between troops that are manoeuvring on a battlefield would be far stricter.

In general, these demands may be articulated into the form of a security policy, which describes the varying degrees of protection that are essential for each unique case. As a consequence of this, the purpose of this research is to ensure that security services are capable of being promptly adapted to the security policy that is given for each and every application environment.

3.16 AN AD HOC MOBILE NETWORK SECURITY MODEL

Regardless of whether the vulnerabilities that are present in a Manet are shared by other types of networks or are unique to the Manet context, the objective of this study is to develop a security model that is capable of reducing or eliminating the vulnerabilities that are present in a Manet. In order to achieve this objective, the proposed security model defines a set of integrated security services that are provided in accordance with the conditions that are required by the Manet architecture. These prerequisites were discussed in the part that came before this one.

The first contribution that this body of work has produced is a recommendation for a cooperation model that is compatible with peer-to-peer architecture. This is the consequence of the work that has been contributed. The distributed self-organization would continue to be one of the fundamental parts of the design and development of services inside Manets if this model were to be implemented. Therefore, all of the security services that have been discussed are produced in line with this paradigm, and there is absolutely no need whatsoever for centralised organisations, even during the period of bootstrapping the network.

In light of the fact that the Manet task force of the Internet Engineering Task Force (IETF) has only recently completed the defining phase for the experimental standards for Manet routing protocols over the Internet, this is of the utmost importance. Taking into consideration the fact that the security aspects of these previous versions of the protocol were not thoroughly explored, it is plainly clear that this stage marked the final step in the process of establishing the protocol.

A number of different businesses situated in different parts of the world work together to provide the services that are referred to as L-Cert (local certification) and L-IDS (local intrusion detection). Both of these services are provided in a collaborative methodology. every Manet node in existence. Communication between the nodes is all that is required; it is not

essential for there to be collaboration between the nodes; all that is required is communication between them.

This capacity opens the door to the possibility of self-organization, which is a direct outcome of this ability. The ability to begin immediate collaboration at any point and with any node presents the opportunity for self-organization. In a nutshell, in reverse order When a new node is added to the network (through the certification service) or when an accusation against a compromised node triggers a response (through the intrusion detection system), a certain (threshold) number of nodes must be in agreement (through the concept of security policy) and cooperate (through the concept of coordinated communication) in order to maintain a secure solution. This is necessary in order to ensure that the network remains secure.

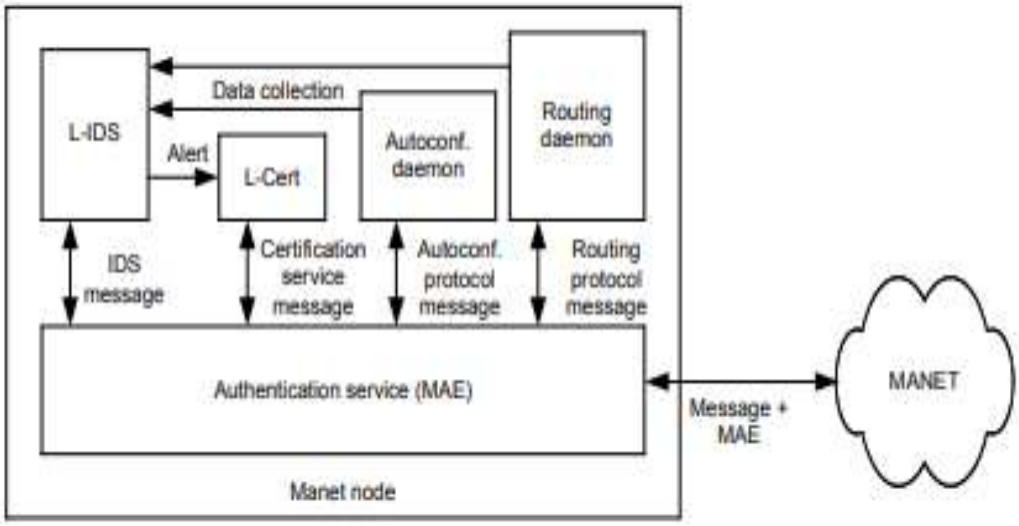

Fig.: 3.7 Using a security paradigm, routing and autoconfiguration services offer protection.

Source: University of brasilia faculty of technology department of electrical engineering data collection and processing through by Dr rafael timóteo de sousa (2004)

Before a new node may join the network, it is necessary for both of these conditions to be taken into consideration and met. By designing and analysing the interaction between these

security services (in this case, the distributed certification and authentication service as preventive mechanisms and the distributed intrusion detection system as corrective mechanisms), this work makes a contribution to the field of securing the routing and autoconfiguration protocols.

This is accomplished through the design and analysis of the interaction. With the intention of facilitating communication between the distributed certification and authentication service and the distributed intrusion detection system, this interaction is intended to take place. The distributed certification and authentication service and the distributed intrusion detection system are two examples of two types of security services that fall under the category of proactive and reactive security services. Both of these are examples of security services that are handled by many parties. The supply of both of these services in a more general sense

As far as the structure of the certification service is concerned, the responsibilities of certification, which are customarily carried out by certification authorities (CAs) in more conventional architectural configurations, are distributed among the individuals who are a part of a Manet. It is necessary for a specified minimum (threshold) number of the nodes to cooperate with one another in order to properly deliver collaborative certification services. The threshold cryptography that was first proposed is the method that is being utilised in the construction of these services. At first, this approach was utilised in order to bring about the establishment of a distributed certification system that was adapted to the Manet environment. Additionally, this plan was developed further in the future.

3.17 SECURITY FOR MOBILE AD HOC NETWORKS AT THE STATE OF THE ART

Due to the fact that both the environment and the challenges are relatively new, there are a great deal of concerns that remain unresolved about the safety of manets. As a result, this subject has been thoroughly explored in the most current specialised literature. The published research and ongoing efforts to build security solutions for these networks have resulted in the

establishment of two separate groups, which may be thought of as rival schools of thought. These groups have produced a number of different ideas.

The first set of academics focuses into the idea of trust and how it may be utilised to discern which nodes in a network are trustworthy and which ones are hostile. The second subcategory investigates the safety of the protocols that are utilised in the process of delivering the fundamental services that are associated with this type of network.

Throughout the entirety of this examination, a considerable amount of emphasis is focused on the security of routing protocols. On the other hand, despite the fact that a few research on this major topic have emerged in a relatively short period of time, there have been very few publications to this point on corrective security techniques.

A few of these solutions consist of intrusion detection systems that have been developed specifically for Manet specifically. During the course of this chapter, we are going to talk about the most significant findings that have been presented in the study that has been carried out on the subject of malware security. In this section, we will discuss topics such as the design of an intrusion detection system, the establishment of a trust model definition, and the development of routing and autoconfiguration security protocols, all of which are necessary for networks of this nature.

The purpose of this chapter is to offer a high-level review of the present state of the art in mobile ad hoc networks. Additionally, the chapter will position the contributions of this study and provide context for those contributions. within the context of other works that are really comparable.

3.18 SECURITY OF ROUTING PROTOCOLS

The importance of routing and autoconfiguration services was emphasized in the prior chapter, so it should come as no surprise that they are crucial to the architecture of the Manet

technology. In this, we will discuss the most important research that have been done on the subject of the safety of routing and autoconfiguration protocols.

3.18.1 Routing protocols

The routing that is utilized in wired networks and the routing that is used in ad hoc networks are somewhat different. When it comes to identifying the most efficient or quickest way to transport data, routing in ad hoc networks is dependent on a wide variety of parameters, such as topology, router selection, and unique features, some of which may be heuristic in nature. The following is a summary of the primary features that are unique to Manets and that may have a direct influence on the design of routing protocols:

- A limited supply of resources, such as available bandwidth and electricity. It is necessary for the routing algorithms to make effective use of the available bandwidth while also allowing for the conservation of energy wherever this is feasible.
- Links that are both symmetrical and asymmetrical. while two nodes are located inside one another's transmission region and have the same routing characteristics while traveling in either direction, we refer to a connection as being symmetrical. When this is not the case, we refer to the connection as being asymmetrical, and it makes the process of routing more challenging. The vast majority of routing methods used in ad hoc networks are based on symmetrical connections since it is best to avoid using asymmetrical links.
- Modes of transportation. While some nodes are able to move very quickly, others may be stuck in place or move very slowly.

3.19 ROUTING PROTOCOL SECURITY

There are still many unresolved security issues with the routing protocols, and the effort to standardise them is in its infancy. When put into practice, not a single one of these protocols offers a satisfactory solution to security challenges. In contrast, protecting routing protocols

has been the primary focus of the studies conducted on Manet security. In the references, we may get an analysis of the potential vulnerabilities that the different AODV protections might exploit. In this paper, we examine the DSR protocol's security measures in detail. Finally, we recommend using the Secure Routing Protocol (SPR)—an enhanced variant of the DSR and ZRP protocols—directly in this reference. The effectiveness of DSDV and other proactive distance-vector routing techniques is examined in this study.

A stated authentication extension for the routing protocol is the foundation of most of the proposed security measures. Danhill and colleagues provide A variant of the AODV protocol called Authenticated Routing for Ad hoc Networks (ARAN). Any communication sent over the routing protocol must first pass authentication. Digital signatures that have already been produced are utilised by the ARAN protocol. Authentication may take place because every message delivered via the protocol has a digital signature.

In order to verify the digital signatures in the messages, the certificates are given so that they may link a node's IP address to the public data required for authentication. The trust of all Manet nodes is placed in a single server, which is responsible for providing them with certificates. Only the sender node is authorised to sign protocol messages because to the sensitive nature of the information they contain, which might be altered during transmission. Conversely, signatures are also needed of every node that transmits messages containing updated information, such as route discovery and route reply messages.

Consequently, this method makes heavy use of the available computer resources and causes message sizes to significantly increase at each hop. One such protocol, SAODV (Secure AODV), was created by M. Zapata and N. Asokan. Every single AODV communication has a security extension called SAODV attached to it. There has been no change to the original specification of the AODV messages. The SAODV protocol differs from the ARAN protocol in that it requires the sender to be the sole signatory. To sum up, hash chains are a way to secure fields that may be changed, like "hop count."

The anticipated study delves into the likely characteristics of the incremented monotonically altering fields. Also provided is a brief summary of how the security extension may be used to secure DSR and other routing protocols used by Manet. Both approaches depend on certification services, which are either implicit in the network and node bootstrapping or specified briefly. Symmetrical cryptography primitives can be used after security links have been established between nodes. In contrast to the other mentioned efforts, this one does not make use of asymmetric cryptography.

Both mobility and node synchronisation can lead to the acquisition of these associations, which can then supply local security associations. Even while these systems use symmetrical cryptography, they also use message authentication extensions. With an emphasis on reactive routing protocols such as DSR and IERP, Papadimitratos and Z. Haas present the SRP. The reactive routing protocols were intended to be protected by the SRP.

The SRP requires that every route's origin and destination establish a security connection (e.g., by exchanging a secret key) before the route may be located, albeit this is not always the case. Nevertheless, assaults that aim to exploit this weakness can use the fact that SRP does not offer any form of protection for route error messages.

Two techniques developed by Y. Hu and colleagues are SEAD (Secure Efficient Ad hoc Distance vector) and ARIADNE. The two protocols in question both make use of authentication keys acquired using the TESLA mechanism, a broadcast authentication approach.

However, certain degree of clock synchronisation across the ad hoc network nodes is required for this protocol to operate correctly. network, the likelihood of which is extremely low for Manet. Since ARIADNE was created to guarantee the security of reactive routing protocols, it primarily focuses on DSR and IERP.

The SEAD group has proposed security measures to be used in distance-vector type routing protocols, with a focus on the DSDV protocol, by combining symmetric cryptographic

authentication with hashing mutable fields that are incremented monotonically (here, "hop count" and "sequence number"). A mix of hash and symmetric cryptographic authentication allows us to do this.

A mix of hash and symmetric cryptographic authentication allows us to do this. An in-depth examination of the DSDV protocol appears to accompany these security measures. Y. Hu and colleagues provide a more generic overview of the security mechanisms employed in the development of the ARIADNE and SEAD protocols in their. H. Yang and colleagues offer a different approach in their research.

The developed protocol is an adaptation of the original AODV technique and is referred to as AODV-S. This protocol differs from others in that it floods the network with RREQ messages that include the word "next hop" rather than sending them unicast to a single node. Other protocols, on the other hand, broadcast RREP messages to a large number of nodes in a single packet. No authentication procedure is followed by transmissions utilising AODV-S.

Another choice is for tokens to be updated and given to all participating nodes on a continuous basis. The method of identifying compromised or malicious nodes involves the use of these tokens. of the messages exchanged inside the routing protocol. The broadcast nature of the wireless communication channel necessitates promiscuous protocol message monitoring by all AODV-S nodes.

3.20 SECURITY OF AUTOCONFIGURATION PROTOCOLS

Even though a significant amount of work has been put on establishing and standardizing the Manet routing protocols, the design of autoconfiguration protocols is still in its infant stages. As a direct consequence of this, ideas to enhance the level of security offered by Manet routing protocols are coming at a quick rate. On the other hand, the amount of written material about secure protocols for Manet autoconfiguration is still rather limited. In this, we will provide some suggestions on how the problem of Manet autoconfiguration may be solved.

3.20.1 protocols for autoconfiguration

Distributed host address translation (DHCP) allows TCP/IP networks to dynamically assign addresses. Recent efforts by the Internet Engineering Task Force's (IETF) zeroconf working group have promoted autoconfiguration using random address allocation. You may think of each of these approaches as viable substitutes. While using DHCP, however, a central server is required to provide network-related details like IP addresses, network masks, standard gateways, and more. We demonstrated that using centralised servers in ad hoc networks is problematic. The zeroconf working group's protocols are also in their early stages of development, which is really descriptive.

Accordingly, the conditions offered by ad hoc environments are incompatible with the methods utilised in conventional networks. The upshot of this is the emergence of several new proposals for autoconfiguration solutions developed with Manets' needs in mind. In addition to all other network configurations, the autoconfiguration protocol must automatically assign IP addresses (16 in total), including those of the DNS servers.

The following requirements were identified as critical for the development of an autoconfiguration protocol suitable for the many application scenarios supported by Manet: Come up with a bunch of metrics that can be utilised to see how effectively an ad hoc network autoconfiguration protocol performs. We did this to ensure that our autoconfiguration approach would work for all of the possible uses of Manet. Autoconfiguration protocols may be grouped into two types. The first one is associated with autoconfiguration, and the second one with mechanisms for detecting copies.

3.20.2 Allocation with duplicate-address detection

Perkins and colleagues, who wrote the paper, offer a method based on the idea of trial and error. An AREQ is a message that a randomly selected network node sends out to all of the other nodes in the network in order to obtain an IP address. It will look for IP addresses that

are already in use. when that, when a specific period of time has passed, the requester will get an Address Reply message (AREP) confirming that the requested address has been allocated. For the duration of this request and response operation, the node making the request uses a temporary address. This particular address was selected from a limited pool of addresses reserved for the autoconfiguration procedure.

Because of this, the reply message can be delivered directly to the requester via unicast. There is no requirement to handle duplicate addresses for this temporary address because its assignment is time-limited. This is the sole temporary usage for the address. This protocol uses a flooding mechanism to get the OK from every node in the network when choosing an address; it doesn't let networks merge or divide. The establishment of new networks is also not supported by this protocol. This method could cause autoconfiguration delays or an excessive load on the network; it is also not easily scalable.

3.20.3 Security of auto configuration protocols

The problem of securing the autoconfiguration process in ad hoc networks is not one that is discussed frequently, and up until quite recently, it was not even discussed in the technical literature. There is an introduction to the subject matter that is presented in the first section of this work, and the subject matter will also be discussed in subsequent sections of this work. The trust model should be implemented as soon as possible following the addition of a new node to the network, according to the strategy's recommendation.

In order for a node to achieve this objective, it must first win the confidence of the network (that is, by receiving a certificate) through the use of the distributed certification services that are provided by the network. There will be a delay in the beginning of the autoconfiguration process on the node until after this step has been completed. In order to ensure the authenticity of each and every one of the autoconfiguration service messages, authentication must be performed using the Manet Authentication Extension (MAE). The only communication that takes occur, including the automatic setup of addresses, is between neighbours who are only

a single hop away from one another. The protocol that underpins this communication does not function effectively, which explains the inadequacies of the protocol as well as the protection model that is applied to it.

Additionally, the protocol does not adequately safeguard the information being transmitted. On the other hand, due to the fact that the method is sufficiently broad, it may be utilised with a wide variety of different autoconfiguration procedures. This is made possible by the use of autoconfiguration, which has the capability of validating newly added nodes before they are placed. In the case of DCDP, the only thing that is necessary is a digital signature, but only the messages that are part of the autoconfiguration protocol need to have an MAE attached to them that contains the authentication information that is pertinent to the message.

Due to the fact that the messages do not contain any fields that may be altered). Additionally, Orset is presenting another body of work that is, in some respects, akin to the one that is being discussed here. On the other hand, the authors of that proposal restrict themselves to creating an authentication extension for the messages that are transmitted over the autoconfiguration protocol. Despite the fact that they do so on the presumption that certificates have already been distributed in advance, they do not provide any details about the manner in which this is accomplished.

CHAPTER 4

WI-FI LANS (WLAN)

4.1 INTRODUCTION

When it comes to recent developments in the realm of communication networks, the Internet has clearly become the driving force behind the vast majority of these innovations. There has been a marked disparity between the growth of telephone traffic and packet data traffic in recent years. The area of wireless technology has also grown substantially over this period. There are now three distinct generations of cellular communication technology available. Because of the efficient mobile connectivity they provide, these systems have been well-received by consumers. Wireless technology has also become an integral part of the networking infrastructure that data transmissions rely on.

Modern networking paradigms and technologies, such as WLANs (like IEEE 802.11), WPANs (like Bluetooth) and WMANs (like IEEE 802.16), WWANs (like IEEE 802.22), and WRANs (like IEEE 802.22) have enabled this revolution. Wireless local area networks (WLANs) in particular are seeing explosive growth in their indoor usage. This is mostly because to their greater design flexibility, reduced installation and maintenance costs, and improved mobility compared to their conventional cable counterparts. The popularity of wireless networks and the growth of the Internet suggest that the demand for applications accessible over the Internet will continue to rise in the future. Wireless local area networks (WLANs) and wireless personal area networks (WPANs) offer the most popular ad hoc and mesh mode, also called infrastructure less mode, although the ad hoc protocols discussed in earlier chapters can be used on almost any kind of network.

Due to the importance of these two new paradigms in local wireless ad hoc communications, we must investigate WLANs and WPANs in conjunction with ad hoc networking. One of the most recognised types of WLANs is the 802.11 standard from IEEE and its many variations

[IEEE802.il 1997online]. An industry standard, Bluetooth is the best example of a short-range wireless personal area network (WPAN). Next chapter will cover the activities taking place in IEEE 802.15, but the IEEE 802 committee has also formed the IEEE 802.15 Working Group for WPANs [IEEE802.15www] to standardise protocols and interfaces because it recognises the importance of short-range wireless networking.

This chapter will go over the IEEE standard 802.11 for WLANs, the design hurdles that must be overcome, and how it may be used to provide ad hoc networking. Also included are the many research developments in WLAN, as well as the HIPERLAN/2 standard established by the European Telecommunications Standards Institute (ETSI). Next up, we'll dive into the world of Bluetooth and the IEEE 802.15 standards. We must stress that our focus is on these technologies' ad hoc style of functioning.

4.2 Why Wireless LANs

Since the early 1970s, when Xerox's Palo Alto Research Centre successfully implemented Ethernet and similar communication protocols, the foundational technology needed to build public and private sector LANs has been available. Virtually every computer now has access to digital networking thanks to standard LAN protocols like Ethernet, which run at very high speeds and employ extremely affordable connecting hardware. Thanks to modern communication networks, businesses of all sizes may easily share and access data. On top of that, the potential of distributed computing and networking is within reach. However, up until recently, LANs could only connect to the actual, hardwired infrastructure of a building.

Although dial-up connections are available, the only way to access network nodes is through wired telephone connections. Many network users find that wireless local area networks (LANs) offer a number of benefits, especially mobile users in many sectors, medical fields, institutions, and businesses [Goldberg, 1999]. Wireless local area networks (LANs) allow users more flexibility and mobility, which is one of their most significant benefits. In contrast to more conventional connected connections, users of wireless LANs are essentially free to

move around as they wish without losing their connection. The only thing limiting wireless networks' practical use is people's imaginations.

Without relying on mountains of paper charts, medical practitioners may obtain real-time vital signs and other reference data in addition to patient information at the bedside. Without the need to wire connections, which may be annoying and time-consuming, factory floor workers can access process and part specifications.

Even in the most unforgiving of production environments, a remote engineer can diagnose and maintain the health of manufacturing equipment through wireless links to any real-time sensor system. Faster and more accurate warehouse inventory counts may be achieved with the use of wireless scanners linked to the main inventory database. With the use of wireless "smart" price tags that include liquid crystal display (LCD) readouts, stores may virtually do away with discrepancies between the stock-point prices and the prices scanned at the checkout.

A seemingly endless array of choices is at play here. In addition to the mobility benefits, wireless LANs (local area networks) also provide more customisation options. The only thing restricting is, once again, one's imagination. Imagine a conference where employees discuss and share ideas for future products and designs utilising small computers and wireless connections. Anyone can envision this type of get-together. Whether it's in the middle of a conference room or halfway across the globe, this ad hoc network can be quickly put up and dismantled as needed. In an effort to streamline the check-in process, certain car rental agencies are now using wireless networks.

Trading on Wall Street is made possible by traders using wireless terminals. A rising number of college students are accessing course materials, such as lecture notes, on the go using their mobile devices. Wireless LANs, or local area networks, could sometimes be more economical. For instance, compared to the expense of installing a wireless local area network solution, the cost of removing or cleaning up asbestos from older buildings is far greater. Many

environments, like a factory floor, may not lend themselves to the use of a traditional wired local area network.

4.3 Transmission Techniques

Here we provide you a rundown of all the different wireless network standards and devices, as well as the transmission techniques that have been developed for them. Because understanding wireless transmission technologies requires an understanding of wired transmission methods, we shall start by presenting them. Since the underlying design issues are essentially the same in practically every situation, these solutions should work for both wired and wireless modems.

The ideal scenario would be to minimise the transmitter's and receiver's complexity, channel bandwidth, and signal power consumption while transmitting data at the highest possible pace. Nevertheless, the application's needs and the communication channel dictate the relative importance of these goals. Additionally, distinct characteristics are present depending on the application and the transmission medium. Lastly, these design objectives aren't always in sync with one another; the trade-offs dictate the relative importance of the various components.

4.3.1 Wired

There are very simple protocols that all data applications, including LANs, employ to send data via wired networks like twisted pair, coaxial cable, or optical fibre. Line code is utilised to encode data received from higher levels; an example of this would be Manchester code on Ethernet. During transmission, voltages or optical signals are applied directly to the medium. It is common to call these transmission methods "baseband transmission schemes" when discussing them. Modulation of the transmitted signal over a carrier is used in applications like coaxial cable models, Digital Subscriber Line (DSL), and voice-band modems.

One or more of the three parameters—amplitude, frequency, or phase—can be used to convey data. Amplitude shift keying (ASK), frequency shift keying (FSK), phase shift keying (PHK),

and quadrature amplitude modulation (QAM) are many acronyms for digital modulation systems. For voiceband modems with a telephone channel passband ranging from 300 to 3,300 Hz, a carrier frequency of around 1,800 Hz is chosen. In the centre of the passband lies this frequency. In order to make room for DSL services, the spectrum needs to be relocated from the lower frequencies used for voice applications. When transmitting data, Digital Subscriber Line (DSL) networks employ Discrete Multitone Transmission, a kind of OFDM.

To improve the bandwidth efficiency of the channel and enable bigger data rates, modulation is used in cable modems to shift the signal's spectrum to a certain frequency channel. Broadband modems are another name for cable modems in the data networking industry; this is because they provide a far higher data rate (broader band) than voice-band modems. Some of the specific problems that can be seen on telephone lines are amplitude and delay distortion, phase jitter, frequency offset, and the effects of nonlinearity. It is precisely because of these limitations that wired modems have evolved to include so many useful design methods.

4.3.2 Wireless

There are three unique types of digital wireless transmission techniques that are the most frequent. These techniques may be classed according to the applications that they are utilised for. First and foremost, there is the category of pulse transmission methods. Infrared (IR) technology is the primary application for these methods, which are used in the majority of applications. Additionally, in more recent times, they have been employed in the transmission of ultrawideband (UWB) or impulse radio [link]. The second group consists of the many ways of fundamental modulation. These techniques are employed to a significant degree in Time Division Multiple Access (TDMA) cellular networks, in addition to a wide range of mobile data networks. In the third category, we have spread spectrum systems.

These systems are utilised in Code Division Multiple Access (CDMA) and wireless local area networks (LANs) that function in the unlicensed Industrial-Scientific-Medical (ISM) frequency ranges. Also included in this category are spread spectrum systems. It is now being

planned and developed via continuing efforts that new transmission technologies that are capable of generating higher data rates are being conceived and developed. In the year 1985, the United States of America started making the ISM frequency bands accessible to the general population. It is not essential to get a licence from the Federal Communications Commission (FCC) in order to operate inside these bands, which are 902-928 MHz, 2.4-2.4835 GHz, and 5.725-5.85 GHz.

These bands are located in the frequency range mentioned above. The technologies that are associated with these are illustrated in Figure 4.1 along with the technologies themselves. Currently, the vast majority of wireless local area network (LAN) equipment is running inside ISM bands. This is because the spectrum is unlicensed with no restrictions. However, the Federal Communications Commission (FCC) does control the ISM bands in a certain manner inside a set framework. The implementation of spread spectrum technology in radio frequency (RF) networks in the United States is mandated by the government.

Moreover, radio frequency (RF) systems are limited to a power level of one watt and are obliged to confine the spectrum that is emitted to a certain band. This restriction is in place to maximise efficiency. Microwave systems must operate at a power level of 500 mill watts or less in order to be classified as very low power systems. There is no further requirement for this classification. Infrared, microwave, and radio frequency transmissions are the three basic techniques of propagation that are utilised in the context of wireless local area networks (LANs). The following is an explanation of each of these methods.

4.3.2.1 Infrared (IR)

Infrared technology is utilised by a variety of popular electronic devices, including remote controllers for televisions, videocassette recorders, DVD players, and CD players. These are just some of the examples of common electronic devices. There is a sort of wireless technology known as infrared transmission, which is classified as line-of-sight (LOS) technology. In order to efficiently establish a communication link, it is essential that the

workstations and digital appliances be in a straight line of sight of the transmitter. This is because of the reason stated above.

An infrared-based network is an option that should be considered in situations when all of the digital devices that need to be connected to the network are in close proximity to one another. We expect the release of these products in the very near future. Despite this, there are new diffused infrared technologies that are capable of working without line of sight (LOS) inside of a room. These technologies are coming soon. However, the signals may be degraded by elements such as people walking or moisture in the air, despite the fact that it is feasible to establish infrared networks in a fair length of time. The promotion of infrared technologies that may be utilised in the house is the responsibility of an international network of firms that is known as the Infrared Data network (IrDA).

The development of infrared systems is not a tough task, and the overall cost of these systems is not very high. The signal frequencies that are employed by them are identical to those that are utilised by fibre optic networks respectively. There is a considerable reduction in interference as a consequence of the fact that infrared devices just detect the amplitude of the signal. As a consequence of the fact that these systems do not have any limitations placed on their bandwidth, they are able to achieve transmission speeds that are superior to those of the other systems. In order to work, infrared transmission does not require a licence from the Federal Communications Commission because it is located within the light spectrum. There are two different approaches that may be taken in order to set up a conventional IR local area network.

Taking into account the fact that infrared emission may be directed, the range has the potential to increase to a couple of kilometres, and it is also suited for use outside. In addition, it offers the highest possible speed and bandwidth compared to any other alternative. There is also the possibility of transmitting in an omnidirectional way and bouncing the signals off of anything in every direction. On the other hand, this would result in a coverage area that is just thirty to

sixty feet in size. Infrared technology quickly gained popularity after it was originally developed because of its capacity to give high data rates at a relatively cheaper cost.

This was the primary reason for its appeal. One of the most major drawbacks of an infrared (IR) system is that its transmission spectrum is similar to that of the sun and other objects, such as fluorescent lights. This disadvantage is the most significant disadvantage of such a system. In the event that there is significant interference from external sources, the local area network (LAN) may become useless. It is impossible for infrared signals to penetrate through opaque objects because of the necessity that they have a line of sight across them.

There is a possibility that the signal will be hindered by all of these items, including walls, dividers, curtains, and even fog. Additional examples of systems that are based on infrared radiation include the IEEE 802.11 standard, which defines a physical layer for high-speed diffused infrared radiation and makes use of pulse-position-modulation (PPM). An additional example of such a system is the IEEE 802.11 standard. This physical layer utilises a wavelength that falls anywhere between 850 and 950 nanometers, and it is capable of transmitting data at rates of between 1 and 2 megabits per second.

4.3.2.2 Microwave

In order to comply with the regulations set out by the Federal Communications Commission (FCC), microwave (MW) systems are required to function at a power level that is lower than 500 mill amps. The market is flooded with megawatt (MW) systems, which are only a small fraction of the total. The majority of them are installed in the 5.8 GHz range, and they make use of narrow-band transmission with single frequency modulation. Since MW systems do not have the overhead that is associated with spread spectrum systems, they have the advantage of having a higher throughput than spread spectrum systems. This is because spread spectrum systems have a higher overhead. Radio LAN, which can be accessed at RadioLAN.com, is an example of a system that makes use of microwave technology. These systems may be found on the internet.

4.3.2.3 Radio Frequency

Radio frequency technology, sometimes known as RF technology, is an additional significant form of microwave technology. Users are able to connect equipment that is located in various parts of the home thanks to the adaptability of this technology, which allows for greater flexibility. There are two categories that may be used to categorise radio frequency (RF): narrowband and broad spectrum. One of the most important aspects of narrowband technology is the transmission of microwaves, which are radio waves with a high frequency. The transmissions of these broadcasts have the potential to travel for a distance of up to fifty miles.

Microwave technology is not suited for use in local networks; nevertheless, it might be used to connect networks that are situated in separate buildings. Microwaves are a type of microwave technology. One of the technologies that is utilised in wireless networks the most frequently is the spread spectrum technology, which is also commonly referred to as SST. It was during World War II that the SST was developed with the intention of enhancing the level of security that was provided for applications that were utilised by the military. Due to the fact that spread spectrum technology entails distributing the signal across a number of different frequencies, it makes it more difficult to intercept the transmission.

Traditional radio modems have a bandwidth that is of the same order as the information signal at the baseband. This means that the transmitted signal fills the same bandwidth. On the other hand, with spread spectrum transmission (SST), the signal that is being transferred takes up a far broader bandwidth than it does in conventional radio modem equipment. The fundamental difference between the two technologies is that they are not identical. When compared to that of UWB, the bandwidth that is used by spread spectrum, on the other hand, is still sufficiently constrained.

This indicates that spread spectrum radios are able to share the medium with other spread spectrum radios as well as traditional radios in a way that is characterised by frequency division multiplexing [Pahlavan2001]. Direct sequence spread spectrum (DSSS) and

frequency hopping spread spectrum (FHSS) are the two primary approaches that are utilised in the process of deploying SST. Both of these approaches are referred to as "direct sequence spread spectrum."

4.3.2.3.1 Frequency Hopping Spread Spectrum

Through the utilisation of this technique, the band is partitioned into a number of smaller subchannels, such as one megahertz respectively. The signal then goes from one sub channel to another, where it delivers small bursts of data on each channel for a predefined period of time, which is referred to as the dwell time. This occurs after the signal has moved from one sub channel to another. A further requirement is that the hopping sequence must be synchronized at both the transmitter and the receiver; if this is not done, the information will be lost.

To be in compliance with the requirements set forth by the Federal Communications Commission (FCC), the band must be subdivided into a minimum of seventy-five subchannels, and the dwell length must not be more than four metres. Because of the constant fluctuation of the frequency, frequency hopping is less likely to be impacted by interference. This is because the frequency is always changing. As a consequence of this, frequency hopping systems are extremely difficult to intercept, which causes them to have a high level of security. In order to generate interference making use of a frequency hopping system, it is essential to jam the whole band.

Having these attributes is especially enticing to organisations that are affiliated with law enforcement or the military because of the potential benefits they provide. In the event that an orthogonal hopping sequence is employed, it is feasible to co-locate a significant number of FHSS local area networks (LANs). Due to the fact that the sub channels in FHSS systems are smaller than those in DSSS systems, it is possible to have a higher number of co-located local area networks (LANs) using FHSS systems.

4.3.2.3.2 Direct Sequence Spread Spectrum

When employing DSSS, the transmission signal is spread out throughout a section of the spectrum that is allowed to be used. It is possible to think of DSSS as a two-stage procedure when discussing modulation techniques related to modulation. In order to modulate the signal that is being broadcast, the first state makes use of a random binary string that is known as the spreading code. This string is used in order to control the transmission of the signal. An arrangement of "chips" is utilised in order to accomplish the task of mapping, or spreading out, the data bits. In order to finish the transmission, the chips are put through a typical digital modulator in the second stage of the process. After being demodulated at the receiver, the chips are subsequently routed via a correlator in order to map (dispread) them back into data bits at the destination.

This process is repeated until the chips are mapped back into data bits. In the context of computer systems, the word "spreading ratio" refers to the number of different chips that each represent a single bit. The resistance of the signal to interference rises in proportion to the spreading ratio, and this resistance grows as the ratio increases. It is observed that the amount of bandwidth that is made available to the user grows in proportion to the decreasing spreading ratio. However, the typical spreading ratio for commodities is less than twenty, despite the fact that the Federal Communications Commission (FCC) requires that the spreading ratio be more than ten. For instance, the physical layer of the IEEE 802.11 standard, which employs DSSS, requires a spreading ratio of eleven.

This is an illustration of the requirement. In order to work correctly, it is necessary for both the transmitter and the receiver to be in sync with the same spreading code. When orthogonal spreading codes are utilised, it is feasible for a number of local area networks (LANs) to share the same band. On the other hand, because DSSS systems make use of big sub channels, the number of co-located local area networks (LANs) is limited by the size of those sub modes. This is because of the fact that DSSS systems include huge sub channels.

DSSS systems are able to disseminate the signal across a wider area, which results in a considerable reduction in the amount of time required for recovery. The length of time that the pulse or symbol is being broadcast or received is inversely linked to the bandwidth of any digital system, which is a fact that is widely known and widely accepted. Because the chips that are sent are substantially narrower than the data bits, the bandwidth of the DSSS signal that is conveyed is significantly larger than that of systems that do not spread. This is because the chips are transported. When compared to the transmission bandwidth of FHSS, which is a narrowband system that hops over a variety of frequencies in a wide spectrum, the transmission bandwidth of DSSS is consistently big.

This is in contrast to the transmission bandwidth of FHSS, which is continually small. The DSSS systems, which also have a larger coverage area than the FHSS systems, are able to deliver a signal that is reliable. On the other hand, the FHSS may be implemented with substantially slower sampling rates, which results in cost savings for the implementation process as well as a reduction in the amount of power that the mobile units require. This is a considerable advantage.

These distinctions have been the driving force behind the implementation of these systems in a variety of technologies for wireless local area networks (WLANs) and wireless personal area networks (WPANs). For instance, the IEEE 802.11b standard, which may be found in both DSSS and FHSS, is an example of this type of configuration. FHSS, on the other hand, is the only protocol that Bluetooth utilises since it meets the requirements for low power consumption and low cost entirely.

4.4 Medium Access Control Protocol Issues

Both the commercial sector and the academic community have shown a great level of interest in MAC protocols over the course of the past several years. There are a number of considerations that need to be addressed in order to construct an efficient MAC protocol that can be utilised in an environment that is characterised by wireless ad hoc and wireless

networks. Bluetooth and HIPERLAN are two examples of MAC protocols that may be employed for ad hoc networking.

Both of these technologies are examples of MAC protocols. When building MAC protocols for any wireless network, there are a number of fundamental considerations that need to be taken into consideration. In this section, we will discuss these difficulties. One thing that should be brought to your attention, however, is that the bulk of these issues are connected to single channel MAC protocols, such as IEEE 802.11, which will be discussed in further depth in the next section.

4.4.1 Hidden Terminal Problem

In the Carrier Sense Multiple Access (CSMA) protocol [Agrawal2002], each station (we will use the terms node, mobile station, and mobile terminal interchangeably throughout this chapter) detects the existence of a carrier prior to transmitting, and the transmission is postponed if a carrier is identified. This is done in order to ensure that the transmission is not interrupted. The process of evaluating the signal intensity in the local vicinity of the transmitter is what carrier sense does in order to make an effort to avoid collisions. On the other hand, collisions take happen at the receiver, not the transmitter; in other words, the existence of one or more interference signals at the receiver is what can possibly result in a collision with the transmitter.

Carrier sense does not provide the essential information for collision avoidance since the transmitter and the receiver are not often positioned in the same area. This is important for collision avoidance. In order to offer a more comprehensive representation of this subject, an illustration is provided. Note that the configuration depicted in Figure 4.2 should be taken into consideration. Station A is able to hear station B, while station C is unable to hear station A. Station C, on the other hand, is able to hear station B, but not station A. According to the concept of symmetry, we are also aware that station B is able to hear both station A and station C.

This is something that we are knowledgeable of. Let's pretend for a second that A is sending a transmission to B. It is possible that when C is ready to broadcast (perhaps to B or maybe to some other station), it does not detect carrier and so begins transmission; this results in a collision at B. This might happen on either side of the spectrum. Station C was unable to offer the necessary information because it was "hidden" from the carrier sense of station A. This prevented station A from providing the information that was necessary. It is given here that a well-known example of a "hidden terminal" event took place.

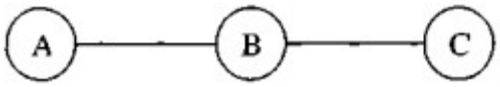

Fig.: 4.2 A and C are unable to hear one another, but Station B is able to pick up on both of them.

Source: Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

It is a terminal situation that is regarded to be "exposed" when we make the assumption that B is transmitting to A rather than A sending to B. This is because B is doing the transmitting. Following this, when C is ready to transmit a transmission, it will execute the detection of the carrier, which will result in a delay in the transmission. Despite this, there is no need to delay transmission to any station other than B because station A is beyond of the range of station C. Instead, there is no reason to delay transmission to any other station. Due to the fact that it was exposed to station B, the carrier sense of station C did not provide the necessary information.

Despite the fact that station C would not collide with station B or interfere with its transmission, this was the situation that occurred. It is essential to bear in mind that carrier sense is responsible for transmitting information about potential collisions to the transmitter, but it does not convey this information to the receiver. It is possible that this information will

turn out to be misleading if the arrangement is scattered in such a way that not all of the stations are within range of each other. There is a solution to the issue of concealed terminals that has been offered in the Medium Access with Collision Avoidance (MACA) protocol [Kami990]. This method has been presented.

To be more specific, it entails the transfer of packets between nodes that are interested in transmitting data. These packets are known as Request-to-Send (RTS) and Clear-to-Send (CTS). The length of the data transmission that is being carried out by the parties who are speaking is conveyed by both the RTS packets and the CTS packets. Stations in the area that are not participating in the transmission but are able to overhear either the RTS or the CTS should maintain their silence for the whole of the transfer. To continue with our instance in Figure 4.2, when node A wants to send a packet to node B, it first sends an RTS message to B. This serves as the first step in the transmission process. It is node A that is responsible for this. The response that node B delivers in response to receiving the RTS packet is a CTS packet.

This is the case under the assumption that node A is able to receive the message. As a result of this, when node C overhears the CTS that is being broadcast by node B, it does not speak for the duration of the time that the CTS packet includes the transfer. This is because the CTS packet contains the transfer. As for the exposed terminal problem, although there is almost no scheme to deal with it in the IEEE 802.11 MAC layer, the Medium Access with Collision Avoidance for Wireless (MACAW) protocol [Bharghavanl994] (based on MAC A) solves this problem by having the source transmit a data sending control packet to alert exposed nodes of the impending arrival of an ACK packet. This procedure is based on MAC A. It was decided to build this protocol.

4.4.2 Reliability

Wireless connections are more likely to experience errors than wired ones. The error rates of packets that are conveyed over wireless channels are much higher than the error rates of

packets that are delivered using materials that are wired. The performance of some protocols, which were first intended to work in a wired environment, is significantly impacted when they are utilised in a wireless setting. This is because of the fact that the wired context was the context in which they were initially developed. Because it uses the expiration of the transmission timer as a warning that the network is suffering congestion, the Transmission Control Protocol (TCP), which was created and optimised for wired networks, is a well-known example of this problem.

TCP was designed to provide optimal performance for wired networks. As a consequence of this occurrence, the execution of TCP congestion control mechanisms is initiated, which ultimately leads to a decrease in the transmission rate. This is done with the intention of lowering the level of congestion that is currently present on the network if it is successful. This is often the case in wired scenarios, which are characterised by the fact that the media are typically extremely reliable. Generally speaking, this is something that takes place. On the other hand, this is not always the case in wireless situations since packet loss can occasionally occur due to a number of reasons, such as multipath fading, interference, shadowing, the distance between the transmitter and the receiver, and so on.

In other words, this is not always the case. Because of this, if a packet is lost during a TCP conversation, the loss is wrongly considered to be the result of congestion, and the mechanisms that control congestion are engaged. This is because of the assumption that congestion is the cause of the loss. Regarding the behaviour of TCP in wireless and mobile ad hoc networks, there have been a few ideas made [Cordeiro2002a, Liu2001]. These suggestions have been made in order to cope with the situation. Chapter 7 devotes a significant amount of space to discussing Transmission Control Protocol (TCP) in relation to ad hoc networks.

In the same way that the Media Access Control (MAC) protocol is a well-known approach, the implementation of acknowledgment (ACK) packets is a common method that is used to reduce the rates of packet loss that are experienced by upper layers. To back to the example

that we showed earlier, Figure 4.2, whenever node B gets a packet from node A, node B will send an ACK message to node A within the same time frame. This will occur whenever node B receives a packet from node A.

In the case that node A is unable to acquire the acknowledgment from node B, it will transmit the packet once more with the intention of submitting it. The procedure that is being explained here is employed in a number of different regimens. To illustrate, the IEEE 802.11 Distributed Coordination Function (DCF) makes use of RTS-CTS in order to effectively sidestep the hidden terminal problem and ACK in order to achieve dependability. This is done in order to achieve the goal of achieving dependability.

4.4.3 Collision Avoidance

They are of the half-duplex kind, and the radios that are used for communication purposes in the wireless and mobile nodes are of that sort. Consequently, it is not possible to detect collisions with these radios since they are unable to concurrently transmit and receive signals. This makes it impossible to detect collisions. This indicates that there is no possibility of doing collision detection. It is common practice for some wireless media access control (MAC) protocols, such as CSMA with Collision Avoidance (CSMA/CA), to make use of collision avoidance strategies in combination with a carrier sensing system, which may be either physical or virtual. This is done in order to cut down on the amount of collisions that take place between vehicles.

The implementation of collision avoidance is performed by mandating that, in the case that the channel is found to be idle, the node must wait for a length of time that is selected at random before engaging in transmission. This occurs in the event that the channel is recognised to be unavailable. Because of this strategy, the possibility of more than one node attempting to transmit at the same time is considerably decreased, which helps to avoid collisions from occurring more frequently. This method also improves the reliability of the network.

The fact that there will be situations in which more than one node will begin transmission at the same moment is not something that should should come as a surprise to anyone. When something like this takes place, the transmissions become jumbled, and the nodes that are associated with them make an effort to retrieve them at a later time.

4.4.4 Congestion Avoidance

It is necessary for wireless media access control solutions to include the prevention of congestion as one of its components. A backoff interval between the values [0, CW] is chosen by a node in the IEEE 802.11 DCF protocol when it arrives at the conclusion that the medium is not being utilised now. The contention window, which normally consists of a minimum value (CW_min) and a maximum value (CW_max), is referred to as the "contention window" (CW) in the industry. The backoff interval will be determined by the node through the use of a countdown, and once the countdown reaches zero, the node will be allowed to transmit the RTS without any further delay.

When the medium becomes busy while the node is still counting down before the backoff interval, the process of counting down the backoff period is paused. This occurs when the backoff interval is still being counted down. Please have a look at the example that is presented in Figure 4.3 in order to acquire a deeper comprehension of the operation of DCF. BOi and B02 are the symbols that best illustrate the backoff intervals of nodes 1 and 2, respectively, in this picture. To simplify things for the purpose of this example, we will assume that CW is equal to 31. The information that is shown in Figure 4.3 makes it very clear that node 1 and node 2 have chosen a backoff interval of twenty-five and twenty, respectively.

There is no question that node 2 will arrive at zero five units of time earlier than node 1, making it the undisputed victor in this competition. Node 1 will become aware that the medium has grown busy and will freeze its backoff interval, which is now set at 5. This will take place in the case that this occurs. Node 1 will continue its backoff countdown and start sending its data as soon as the backoff interval gets closer and closer to zero. This event is

going to take place as soon as the medium is once again able to function normally. Similarly, when node 1 transmits a transmission, node 2 will immediately suspend its backoff transmission until the transmission is completed.

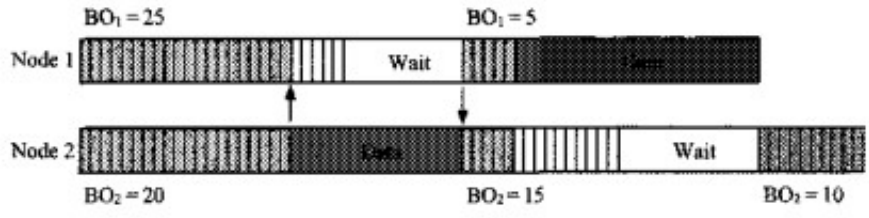

Fig.: 4.3 A demonstration of the DCF mechanism for the back off off

Source: Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

It is imperative that you immediately resume the countdown operation in the case that node 1 finishes its broadcast. Through the use of this method, it is possible to lower the chance of accidents occurring to a certain degree. The selection of a large CW leads to the formation of lengthy backoff intervals, which may also contribute to an increase in overhead. This is because the countdown technique is required to be carried out by the nodes. On the other side, choosing a small CW leads to a higher number of collisions, and as a consequence, it is more likely that two nodes would count down to zero at the same time. This is because the number of collisions becomes more frequent.

4.4.5 Congestion Control

Previously, it was said that there is a chance that the number of nodes that are attempting to broadcast simultaneously would change over the course of further time. As a result, there is a need for a system of some type to control the amount of congestion. The dynamic selection of the contention window and contention window (CW) is what allows IEEE 802.11 DCF to achieve its goal of congestion control.

In the event that a node does not get CTS in response to its RTS, it will extend its contention window up to CW_max. This is based on the assumption that congestion has became more severe. This is due to the fact that the node has made the assumption that congestion has increased. When a node is able to successfully complete its transmission, it will reset its contention window to the lowest possible value that is available. This method, which is used to dynamically regulate the contention window, is referred to by its name, Binary Exponential Backoff. The reason for this is because the contention window expands at an exponential rate with each congestion management system that fails to successfully control congestion.

4.4.6 Energy Efficiency

The fact that many mobile hosts are powered by batteries has led to an increase in the number of people who are interested in numerous access control mechanisms that have the ability to conserve energy. According to the concepts that are now being studied in this area, it is frequently recommended that the radio be turned off when it is not necessary.

A Power Saving (PS) mode is present in IEEE 802.11, which enables the Access Point (AP) to send out a beacon at regular intervals. This mode is included in IEEE 802.101. With the help of this beacon, you may determine which nodes are now awaiting the arrival of packets. Every PS node wakes up at predetermined times in order to have the opportunity to receive the beacon that is sent by the AP.

After a backoff interval in the range [0, CW_min] has been completed, a node will send a PS-POLL packet to the access point (AP) in the event that it has a packet that is waiting for it. This occurs in the event that the node has a packet that is waiting for it. Immediately following the receipt of the PSPOLL packet by the access point (AP), the data will be sent to the node that has made the request for it. In the event that this procedure is followed, it is possible to extend the amount of time that mobile nodes are able to work with their batteries for a longer period of time. We shall discuss further strategies that may be utilised to conserve energy in

a later portion of this chapter. Energy conservation is an important topic. Techniques such as transmit power control are included in these technologies.

4.4.7 Other MAC Issues

It is important to note that the explanation of MAC protocol difficulties that has been provided here is by no means exhaustive. In addition, there are a great many other issues that need to be taken into consideration, such as fairness. One of the many ways that fairness may be perceived is to indicate that stations should be given with equal bandwidth. This is only one of the many ways that fairness can be understood. This type of fairness cannot be provided by the IEEE 802.11 MAC because it is impossible to supply it. This is because unfairness will eventually occur when one node backs off much more than some other node in the same neighbourhood.

An approach that has been developed by MACAW to address this problem is one that requires attaching the contention window value (CW) to the packets that a node sends out into the network. This guarantees that any node that receives that CW will make use of it for their following broadcasts once it is sent out. As a result, MACAW recommends that a CW be kept in a distinct location for each receiver. This is because CW is an indication of the degree of congestion that is present in the neighbourhood of a certain receiver node. This is the reason why this is the case. Additionally, there are additional proposals that are being taken into consideration, such as the Distributed Fair Scheduling technique and the Balanced MAC.

In light of the receiver-related challenges that are inherent to wireless MAC protocols, it is necessary to incorporate a closing remark. All of the protocols that have been discussed up until this point are all examples of sender-initiated protocols. To put it another way, the person who initiates the process of sending a packet to a destination is always referred to as the sender. While it is feasible that the receiver may play a more active role in the process, it is also possible that the receiver will provide aid to the transmitter with specific obstacles. These challenges may include collision avoidance and some form of adaptive rate regulation.

4.5 The IEEE 802.11 Standard for Wireless LANs

When compared to other wireless data technologies, such as cellular or point-to-multipoint distribution systems, wireless local area networks (WLANs) provide an efficient usage model for high-bandwidth customers. Additionally, WLANs are particularly desired owing to the low cost of their infrastructure and the high data rates they offer. For consumers that have a high bandwidth need, wireless local area networks (WLANs) are also great. The 802.11 standard, which is also frequently referred to as Wi-Fi, which stands for Wireless Fidelity, was ratified by the IEEE in June 1997 for use in wireless local area networks (WLANs). There are many other names for this standard.

In July of 1997, the IEEE 802.11 standard was officially acknowledged as a standard by the International Organisation for Standardisation (ISO at the global level). There are three distinct potential implementations of the physical (PHY) layer that are included in the standard. The specification allows for data transmission speeds of either 1 Mb/s or 2 Mb/s. In addition to it, there is a single MAC layer that is shared by everybody. A FHSS system that uses 2 or 4 Gaussian frequency-shift keying (GFSK) modulation, a direct sequence spread spectrum (DSSS) system that uses differential binary phase-shift keying (DBPSK) or differential quadrature phase-shift keying (DQPSK) baseband modulation, and an IR physical layer are the alternatives that were considered alternatives for the PHY layer in the original standard.

In the later part of 1999, the IEEE 802.11b working group came to the conclusion that it would be more beneficial to shift away from the FHSS and instead utilise the DSSS. The inclusion of the IEEE 802.1 lb standard was something that was done in order to broaden the scope of the IEEE 802.11 standard. Furthermore, in order to implement the Orthogonal Frequency Division Multiplexing (OFDM) strategy, the IEEE 802.11a working group made significant adjustments to the physical layer (PHY). These modifications were done in order to replace the Spread Spectrum methods that were utilised in the IEEE 802.11 in order to meet the

requirements of the OFDM approach. Techniques that use multiple carriers, multiple symbols, and multiple rates are all effectively integrated into this framework.

Within the context of this particular situation, the IEEE 802. llg amendment is still another adjustment that ought to be highlighted. The IEEE 802.1 lg standard, which is an extension of the IEEE 802.11 PHY standard, has been receiving a lot of attention from companies who manufacture equipment for wireless local area networks (WLAN). The full certification of this standard was completed in June of 2003. In addition to enabling backwards compatibility with 802.11b equipment, the IEEE 802.1 lg standard delivers the same maximum speed as the 802.11a standard. This is made possible by operating in the 2.4 GHz ISM band. For the purpose of achieving higher data rates, devices that are compliant with the 802.llg standard make use of the OFDM modulation technique.

CCK modulation is a form of transmission that may be automatically switched to by these devices in order to simplify communication with slower 802.11b and 802.11 compatible equipment. This mode of transmission is known as cross-band modulation. As a result, the PHY layer modulation of 802.1 lg may be seen as the combination of the PHY layer modulations of both 802.11a and 802.11b. For the purposes of this chapter, we will be putting more of a focus on the physical layer requirements that are included in the IEEE 802.1 la/b standards. This is occurring as a result of the fact that the later is now being employed to a significant degree, whilst the former is getting an increasing amount of acceptance. We are going to undertake a consistent examination of the IEEE 802.1 lg PHY layer while we are in the midst of characterising the different physical layer interfaces (PHYs).

4.5.1 Network Architecture

In the context of wired local area networks (LANs), wireless local area networks (WLANs) can serve either as an alternative to wired LANs or as an extension of the architecture of wired LANs. An illustration of the core topology of an 802.11 network may be seen in Figure 4.5(a), as can be seen right now. A basic service set, often referred to as a BSS, is comprised of two

or more wireless nodes, also referred to as stations, that have identified one another and then proceeded to establish communication with one another. One of the most fundamental versions of the system comprises stations connecting directly with one another through the use of a peer-to-peer mode, while at the same time sharing a certain cell coverage area.

A network that is also known as an Independent Basic Service Set (IBSS) is referred to as an ad hoc network, which is one of the most common names for this type of network. The construction of this form of network often takes place on a short-term and instantaneous basis. As a result of the fact that the bulk of the protocols that are described in this book are adapted expressly for this sort of scenario, the primary emphasis of this book is placed on this style of operation. The infrastructure mode, which is sometimes referred to as the client/server mode, is the other way of operation, as can be seen in Figure 4.5(b). Within this mode, an Access Point (AP) is utilised to facilitate the operation of the system.

In order to facilitate communication between wired and wireless local area networks (LANs), the primary function of an access point is to serve as a bridge. Every base station (BSS) often has an access point (AP), which functions in a manner that is analogous to that of a base station (BS) that is utilised in cellular phone networks. Peer-to-peer communication between stations is not possible when an access point (AP) is present since stations cannot communicate with one another. All communications are directed through the access point (AP), regardless of whether they are between stations or between a station and a wired network client. Access points, also known as APs, are fixed in place and do not move around as part of the design of the network configuration.

Stations, on the other hand, are frequently mobile and have the capacity to move between access points (APs), which means that they require help in order to get continuous coverage. This configuration of a BSS is referred to as operating in the infrastructure mode, and it is the word that is used to define the configuration. There is a collection of overlapping BSSs that make up the Extended Service Set (ESS), as shown in Figure 4.5(b). Each of these BSSs has

an access point (AP), and they are connected to one another via the use of a Distribution System (DS) that is able

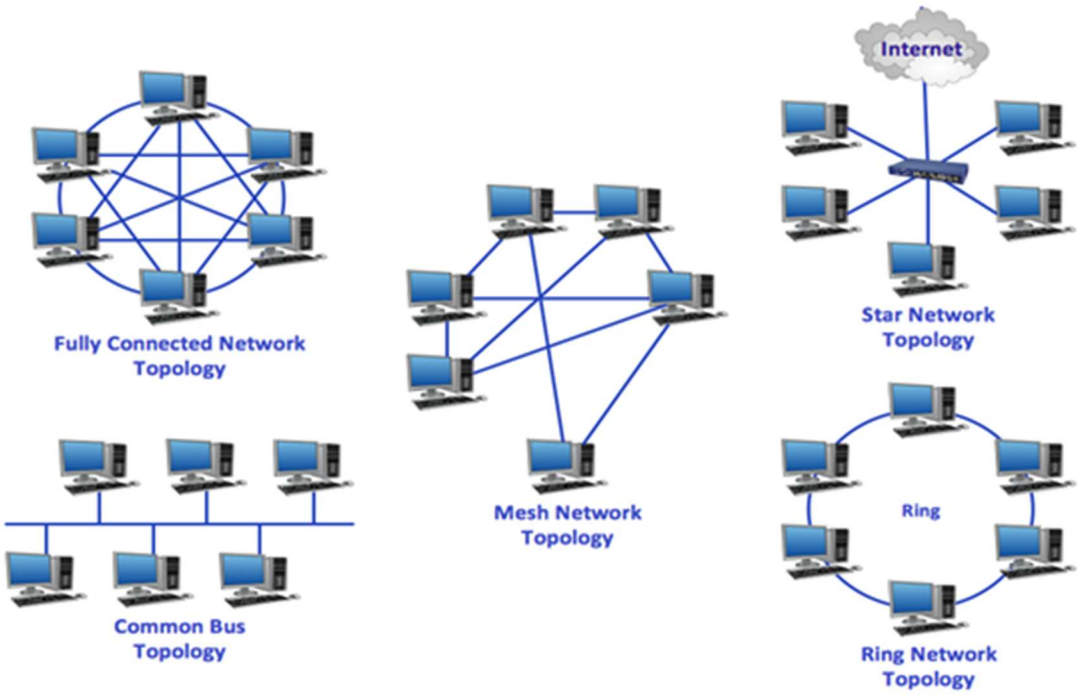

Fig.: 4.5 The many topologies of the network

Source: Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

It is possible that the network is of any sort. In most cases, the DS is a local area network (LAN) that makes use of Ethernet networks. Wireless mesh networks, on the other hand, have lately seen a significant surge in popularity as a distributed system [Akyildiz2005]. When it comes to wireless mesh networks, it is not required for access points (APs) to have wired connections with one another. The alternative is that access points are able to connect with one another wirelessly in a hierarchical arrangement, which eliminates the demand for any cable infrastructure that may have been present in the area. The working group of IEEE

802.11s is responsible for standardising wireless mesh networks, which are specifically designed for wireless local area networks (WLANs).

4.5.2 The Physical Layer

It is the responsibility of the Physical Layer (PHY) to act as the interface between the Media Access Control (MAC) and wireless media, as seen in Figure 4.6. This component is accountable for the transmission and reception of data frames via a wireless medium that is shared. Within the realm of functionality, the PHY offers three distinct levels of functioning. To begin, the sublayer known as the physical layer convergence procedure (PLCP) is accountable for the regulation of the frame exchange that occurs between the media access control (MAC) layer and the physical layer (PHY) layer. It is the responsibility of the physical medium dependent (PMD) sublayer, which is the second layer, to ensure that data frames are sent via the medium for the physical layer (PHY).

Utilising signal carrier modulation and spread spectrum modulation are the means by which this objective is realised. The physical layer (PHY) is responsible for sending a carrier sense indication back to the media access controller (MAC) in order to confirm the activity that is taking place on the media. The performance of high-speed neural networks is hindered by the quick fading that appears as a consequence of multipath propagation. This is the factor that is responsible for this limitation. For example, air scattering, reflection, refraction, or diffraction of the signal between the transmitter and the receiver can all contribute to the phenomenon of fading, as stated by Agrawal (2002).

These occurrences cause the signal to arrive at the receiver with different delays and interfere with itself, which ultimately results in inter-symbol interference, also known as ISI. An illustration of multipath propagation is shown in Figure 4.7. This figure gives a visual depiction of. This particular type of fading takes place when the symbol time becomes much smaller than the channel delay spread. This is the exact situation that causes it to take place. The transmission data rate increases, which causes this specific sort of fading to become more

prominent. In this section, we are going to talk about a number of different strategies that are used in IEEE 802.11 in order to defend against the impact of fading.

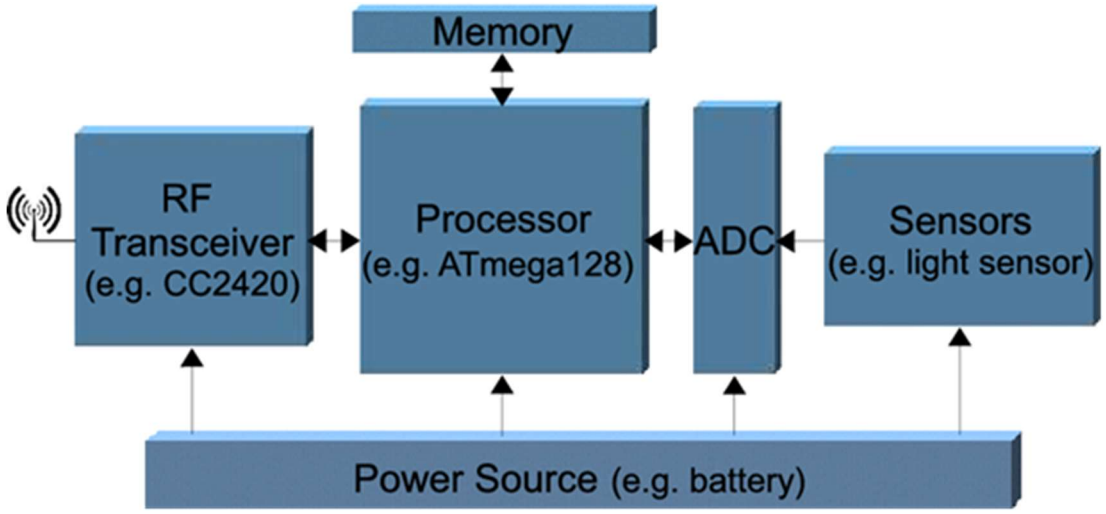

Fig.: 4.6 When it comes to the PHY, the sublayers

Source: Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

Spread Spectrum, often referred to as FHSS or DSSS, and Orthogonal Frequency Division Multiplexing, generally known as OFDM, are two techniques that are widely utilised in order to combat frequency selective fading. As we have seen in the past, the signal is processed using Spread Spectrum in order to occupy a substantially greater bandwidth. This is done before the signal is transmitted.

The purpose of this action is to lessen the impact of frequency selective fading, which will only have an impact on a limited percentage of the signal bandwidth. For the aim of mitigating frequency selective fading, orthogonal frequency division multiplexing (OFDM) entails the data stream being divided into a particular number of substreams, each of which has a bandwidth that is smaller than the coherence bandwidth of the channel. This is done in order to achieve the desired effect. Understanding the definitions of some of the terminologies that

are used at the physical layer is very required in order to have a complete comprehension of the complexity that are involved in IEEE 802.11:

- Gaussian Fourier transform (GFSK) is a modulation system in which the data are first filtered using a Gaussian filter in the baseband, and then modulated using a comparatively straightforward frequency modulation. In the context of data symbols, the numbers "2" and "4" denote the number of frequency offsets that are utilised to represent one and two bits, respectively;

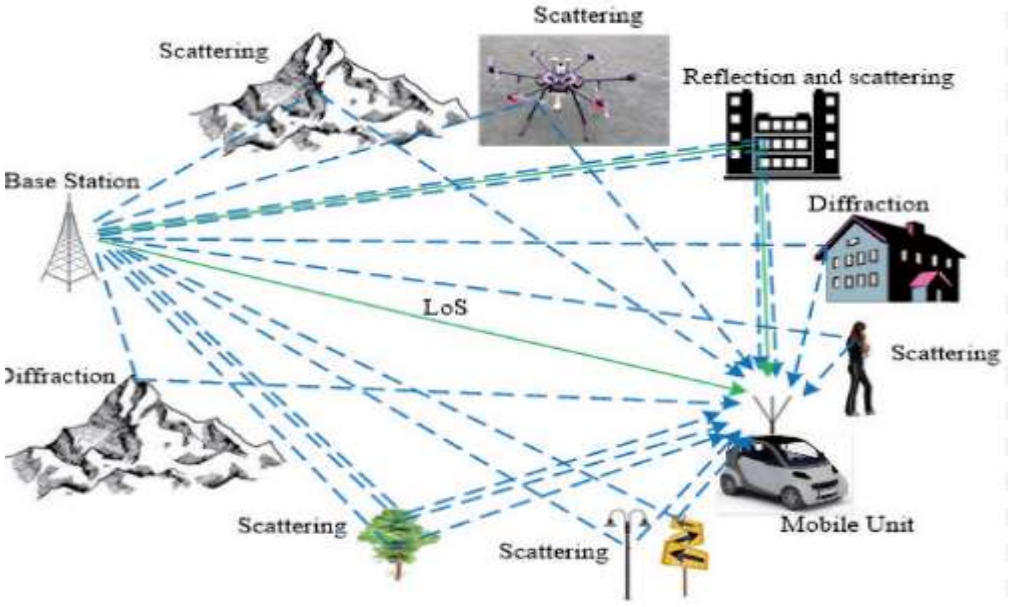

Fig.: 4.7 Some of the factors that contribute to multipara propagation

Source: Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

- DQPSK is a sort of phase modulation that uses two pairs of unique carrier phases, in quadrature, to indicate two bits per symbol.
- DBPSK is a phase modulation system that uses two distinct carrier phases for data signalling, meaning that it provides one bit for each symbol. It is the differential feature

of the modulation schemes that denotes the utilisation of the difference in phase from the most recent change or symbol in order to ascertain the value of the present symbol, as opposed to any absolute measurements of the phase change.

Both the FHSS and DSSS modes are specified for operation in the 2.4 GHz ISM band, which has been jokingly referred to as the "interference suppression is mandatory" band due to the fact that it is often employed by a variety of electronic devices. The ISM band is the frequency at which both modes are defined for operation. Another option is a third physical layer, which is an infrared system that use near-visible light in the range of 850 nm to 950 nm as the transmission medium. This system is an alternative to the first two physical layers. The utilisation of this method is not at all widespread.

The IEEE 802.11 standard has been expanded to include three new additions: 802.11a, 802.11b, and 802.1 lg. In addition, there is a standard published by ETSI that is referred to as HIPERLAN/2. The changes that have been made are at the forefront of the new wireless local area network (WLAN) alternatives that would allow for much higher data transfer rates. In terms of their physical layer characteristics, 802.11a and HIPERLAN/2 are equivalent; both of these technologies operate in the 5 GHz range and make use of the OFDM modulation pattern.

But the multimedia access control (MAC) layers of these two networks are significantly different from one another. MAC stands for multimedia access control. On the other hand, the objective of this section is to provide a description of the physical layer characteristics of the IEEE standards 802.11a and 802.11b and to compare those characteristics. This is because HIPERLAN/2 has a number of the same physical characteristics as 802.11a, and 802.1 lg PHY may be regarded as a combination of 802.1 la/b PHYs. This is the reason why this is the case.

4.5.2.1 DSSS

The 2.4 GHz frequency band is utilised by the DSSS for radio frequency communication. The DSSS PLCP sublayer provides instructions to the DSSS PMD sublayer, which is then

responsible for guiding data transmission via the medium. To facilitate transmission via wireless media, the DSSS PMD may convert the binary bits of data received from the PLCP protocol data unit (PPDU) into RF signals.

The utilisation of DSSS and carrier modulation allows for this to be achieved. The IEEE 802.11 standard incorporates DSSS as a safeguard against frequency-selective fading. In 1999, the IEEE certified the 802.11b standard, which could provide enhanced payload data rates of 5.5 and 11 Mb/s, adding to the 1 and 2 Mb/s rates that the original 802.11 standard could handle.

This is on top of the original speeds that the IEEE 802.11 standard supported. In addition, the 2.4 GHz ISM range (2.4 GHz to 2.4835 GHz) is a highly populated frequency where IEEE 802.11b operates. Even with just 83 MHz of spectrum, this band can handle a wide range of goods. Items such as cordless phones, microwave ovens, and a variety of WLANs and WPANs (such as Bluetooth) are examples of such items. Being sensitive to interference is one of the most critical challenges that needs addressing.

There is a voluntary frequency hopping mode specified by the 802.11b standard. However, this mode may also be used with six overlapping channels that are 10 MHz apart, or with three non-overlapping channels. Reducing interference effects is the intended purpose of this mode. In order for the transmitted signal to have a consistent pattern of chips, DSSS converts each bit from the original signal. The implementation of this mapping is achieved by use of a pseudo-noise (PN) sequence. The arrangement of the chips remains constant during the transmission of the signal.

This process not only increases the signal's resilience to frequency selective fading, but it also greatly expands the usable bandwidth. One definition of a PN sequence is a deterministic binary sequence that appears to be random at first glance but which, upon further examination, reveals that it is really repeating itself. The fact that PN sequences are self-repetitive makes this definition possible. There is one symbol in the PN sequence, and it is called a "chip" here.

4.5.2.1.1 Modulation

DBPSK is utilised by the DSSS PMD in order to transmit the PLCP preamble and PLCP header at a rate of 1 Mbps. Depending on the information included in the signal field of the PLCP header, the MAC protocol data unit (MPDU) is sent at either 1 Mbps DBPSK or 2 Mbps DQPSK.

4.5.2.1.2 Operating Channels and Power Requirements

Every single DSSS PHY channel has a bandwidth of 22 MHz, and the spectral form of the channel is a representation of a filtered SinX/X function. Within the framework of IEEE 802.11, the DS channel transmit mask stipulates that spectral products must be filtered to a level of -30dBr from the centre frequency, while all other products must be filtered to a level of -50dBr instead. As a result, this makes it possible to have three channels in the 2.4 GHz ISM frequency range that do not interfere with one another and are separated by 25 MHz. Illustration of this DSSS channel architecture may be seen in Figure 4.8, along with the channel nominations that correspond to it.

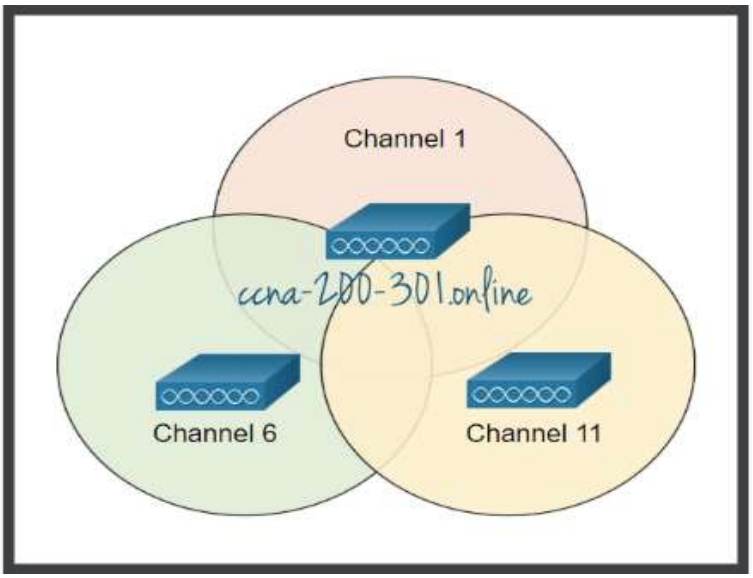

Fig.: 4.8 DSSS non-overlapping channels

Source: Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

One of the most important parameters that is controlled all over the world is transmit power, in addition to frequency and bandwidth distribution patterns. The maximum amount of radiated emission that can be authorized for the DSSS PHY varies from one zone to the next. In the present day, the makers of wireless devices have decided to use 100 milliwatts as the nominal RF transmits power level.

4.5.2.1.3 IEEE 802.11 and the 11-Chip Barker Sequence

For the DSSS PHY layer in IEEE 802.11, the following PN—the eleven-chip Barker sequence—is chosen: This is the set of integers: [1, 1, 1, -1, -1, -1, 1, -1, 1, -1]. We choose this sequence because its autocorrelation is interesting; when the transmitter and receiver are in sync, it shows some very noticeable peaks.

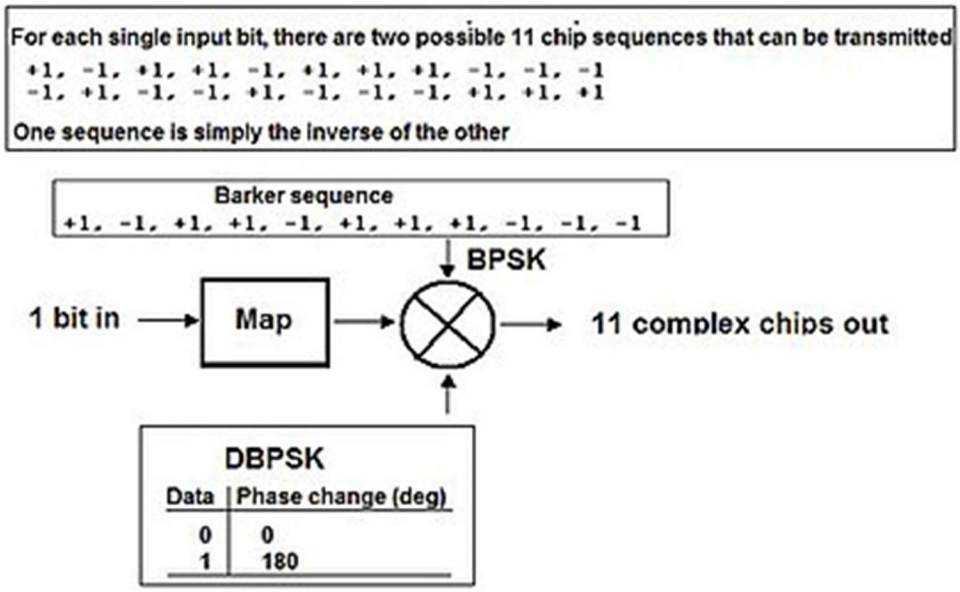

Fig.: 4.9 When compared to the 11-chip Barker sequence, the '10' sequence hits its maximum.

Source: Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

These peaks serve to emphasise the selection of the sequence. Figure 4.9 offers a further example of this in action by showing the relationship between the '10' sequence and the 11-chip Barker sequence. Figure 4.10 shows that these peaks allow the receiver to overcome the 'echo' signals created by the multipath channel by locking on to the strongest signal it has received. With a symbol rate of 1 Megasymbol per second (Msps), the original IEEE 802.11 standard yielded a chipping rate of 1 MHz when employing the Barker sequence. On top of that, it can deliver data speeds of up to 2 Mbps (DQPSK, where 2 bits are sent per symbol) and 1 Mbps (DBPSK).

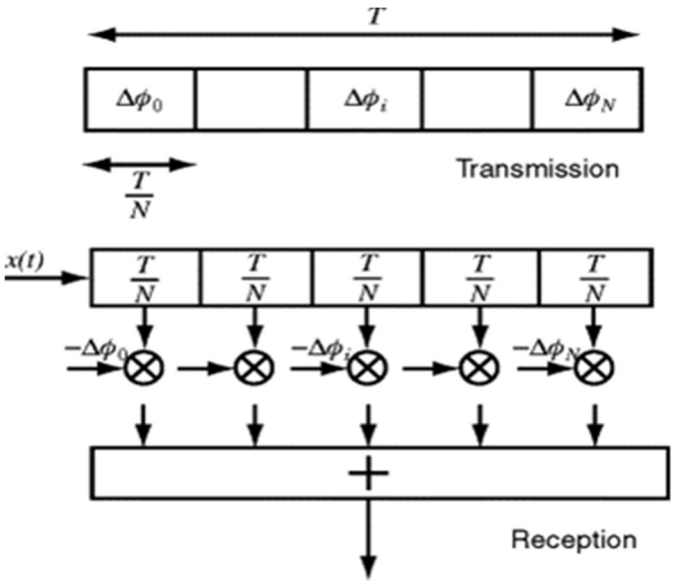

Fig.: 4.10 They should maximise their performance when comparing received sequences to the 11-chip Barker sequence

Source: Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

CHAPTER 5

PROPOSED SECURE ROUTING PROTOCOL

5.1 INTRODUCTION

All of the dangers described and shown in the previous section should be able to be overcome by a good safe routing algorithm. If it promises to efficiently and safely identify and maintain routes, and if it guarantees that no nodes—aside from the potential of nonparticipation—can stop or slow this down, then it is crucial. Therefore, to guarantee an accurate and risk-free execution When exposed to malicious actors, routing activities and route discovery must be protected by a secure ad hoc routing protocol, which must meet many crucial features.

1. Faking routing signals is not something that can be imagined.
2. It is not feasible to introduce faked routing messages into the network. This ability is not available.
3. Changing routing messages while they are in transit is strictly prohibited, unless the modification is necessitated by the regular operation of the routing protocol. This is a strong ban that should be adhered to regardless of the circumstances.
4. The construction of routing loops cannot be the product of hostile behaviour since it is impossible for this to happen.
5. It is not feasible for adversarial actors to cause routes to diverge from the optimal path, which is also commonly referred to as the shortest path.

Sixth, it is necessary to exclude unauthorised nodes from the process of calculating routes and finding new routes. It is important to note that this does not exclude the fact that even peers who have been verified in the past may choose to engage in harmful behaviour. However, we are operating with the premise that public keys, session keys, and certificates are pre-deployed and exchanged in regulated open settings. This is the assumption that we are functioning under.

5.2 MOBILE AD HOC NETWORKS PROPOSED SECURE ROUTING PROTOCOL

Despite the fact that the IETF has created a number of routing protocols for mobile ad hoc networks, none of them give any thought to the myriad of security risks and assaults that are now available. Therefore, MANET routing protocols aren't equipped to prevent attacks or help secure mobile wireless Ad hoc networks from their inherent weaknesses. Because MANETs aren't built to handle vulnerabilities, this is the result. For mobile ad hoc networks to be useful in the modern day, a secure routing protocol is an absolute must.

You absolutely gotta do this. Considering the vulnerabilities of the existing conventional routing protocols and the security of MANETs as a whole, the urgent necessity for a safe routing protocol became crystal evident. "Authenticated Source Routing for Ad hoc Networks" (ASRAN) is a novel secure routing protocol enhancement for MANET that we would like to provide. What I have just said has an immediate and direct impact on this. The DSR protocol, an on-demand source-routing mechanism, forms the backbone of this system.

This routing protocol utilises source routing, which capitalises on the inherent mobility and dynamism of MANETs, making it a good fit for these networks. On the other hand, it won't work in any other kind of network. ASRAN's model protocol, DSR, was selected for its desirable features, superior experimental and simulation performance compared to other prototypical MANET routing protocols (discussed above), and mechanisms that can be easily modified to incorporate security while minimising vulnerabilities. For these reasons, DSR was selected. In addition, as previously stated, DSR outperformed other classic MANET routing protocols in both testing and simulations. It was because of this issue that the DSR protocol was chosen to be the basis for the ASRAN network.

5.3 AD HOC NETWORKS AUTHENTICATED SOURCE ROUTING (ASRAN)

It is necessary for the ASRAN network to rely on cryptographic certificates in order to guarantee the security of its routing capabilities. To achieve this, principles from ARAN,

which is a secure routing protocol that was upgraded to apply AODV, and SAODV, which is another suggestion for boosting security, are combined. This allows for the achievement of the desired result. Both of these ideas are encompassed inside the framework of the system. As a result of the adjustments that DSR makes to the AODV protocol, it is now possible to handle source routing explicitly.

DSR is the company that provides these improvements. As a result of the utilisation of a preliminary certification mechanism and a route instantiation approach, ASRAN ensures that authentication is carried out in an appropriate manner from the very beginning of the process all the way through to the very end of the process. A route may be identified by an ASRAN node by first broadcasting a route discovery message and then waiting for a response from just the node that was meant to be the recipient of the message. This makes it possible for the ASRAN node to identify routes.

Discovering new routes is the name given to this procedure. Once it is feasible to create a route to the destination node after the destination node has been reached, it is no longer necessary for an intermediate node to deliver a reply on behalf of the destination node. This is because the initial node has already reached the destination node. At each hop along the path that runs from the source to the destination and back again, it is essential to do a verification of the routing messages. This includes both the source and the destination. The answer's content has been constructed in such a way that it is capable of accomplishing this goal to the best of its ability.

Fig.: 5.1 MANET Topology That Is Used to Describe ASRAN That Is Not Complicated

Source: Evaluation of on-demand routing in mobile ad hoc networks and proposal for a secur oposal for a secure routing pr outing protocol data collection and processing through by Soke Mathew Onyemelukwe (2013)

5.4 ASRAN'S SECURITY AND APPRAISAL

In this, we give a security analysis of ASRAN by analysing the system's resilience in the presence of the attacks that were discussed in the part that came before this one.

Mitigation of Tunneling Attacks: Hop count is a statistic that is utilised by the DSR protocol, which is the fundamental protocol upon which ASRAN is built. This statistic is utilised by the DSR protocol. Simply comparing the number of hops that are involved in these two routes is not sufficient to conclude with complete certainty if one route is shorter than another. There is no method to ascertain this with total certainty. In the process of developing a method for determining the most effective path in a MANET, it is of the utmost importance to take into consideration the fact that tunnelling attacks, such as the one in addition to other archetypal MANET routing technologies, the scenarios described in the paragraph that came before this one, are able to be supported.

This is because tunnelling attacks tend to be more effective than other types of MANET routing technologies. It is difficult to secure the shortest road without resorting to physical actions if one does not resort to physical measures, such as inserting a date into the process of routing messages. When this occurs, it is difficult to secure the easiest path. On the other hand, according to ASRAN, hop counts are not the only factor that determines whether or not the shortest and best route is considered feasible. The evaluation of a variety of other aspects is also taken into account. Instead, it is mostly a function of the least latency, which can be determined by looking at the timestamps attached to the communication.

The occurrence of this occurred as a consequence of the fact that hop counts are not always accessible. Because ASRAN does not use hop count as the sole factor in determining the

optimal route, it will be difficult for malicious tunnelling attacks to be carried out on MANET nodes that are based on ASRAN. This is because ASRAN does not provide the only factor that determines the optimal route. Due to the fact that tunnelling attacks are not a consequence of ASRAN's use of hop count as the major determinant of the optimal route, this is the reason why tunnelling attacks are not a result of ASRAN. This is the reason why situations are the way they are. As a consequence of this, ASRAN will take action depending on the information it has obtained via the use of timestamps in order to identify the route that is both the most ideal and the most efficient. by utilising the information that is required. As a direct result of this, ASRAN will be able to successfully protect itself against the great majority of tunnelling attacks.

Spoofed Route Signaling: To sign messages that are transmitted from the source node, the source node's own private key is the only method that may be used. Nodes are unable to impersonate other nodes throughout the process of route building or discovery as a consequence of this. In a way that is analogous, the certificate and the signature of the destination node are both included in the reply packet that is transmitted during the transmission. This hinders the finding of routes, which in turn restricts the capacity to reply to just the end destination. Impersonation attacks, in which one node pretends to be another, are prevented from succeeding as a result of this because it prevents the attacks from being successful.

Unauthorized Participation: Packets that have been signed with a certified key that has been issued by a reliable authority are the only ones that can be accepted by the ASRAN nodes that are participating in the network. We did not go into depth on the procedures for since it was not within the scope of this study. Additionally, Schneier has provided a comprehensive list of the mechanisms that are available. There are a huge number of mechanisms. Furthermore, the presence of a central trusted authority in ASRAN renders the system vulnerable to attack and establishes a single point of failure.

Replay Attack: Both a nonce and a timestamp are included in the payloads of the routing messages (RDP and REP) in order to provide protection against replay attacks.

Fabricated Routing Messages: Due to the fact that only nodes that possess certificates are able to generate messages, the only nodes that are capable of producing messages are those that possess certificates. This implies that the only nodes that are able to do so are actual authorized nodes that have been taken over by bad actors. This form of assault, as well as attacks conducted by selfish nodes, cannot be prevented by ASRAN since it does not have any safeguards. However, ASRAN does offer a deterrent in the form of a promise of non-repudiation services. This is a significant advantage. In the event that a node continues to send out deceptive signals into the network, there is a possibility that it may be removed from the calculation of future routes.

Integrity and Alteration of Routing Messages: Between the source and the destination, ASRAN guarantees that all fields of RDP and REP messages are maintained in their initial condition. This is accomplished with the assistance of a system that enforces integrity. Due to the fact that both types of packets are signed by the node that began them, any modifications that were made to them while they were in transit would be promptly spotted by intermediate nodes along the path, which would then result in the altered packet being destroyed. The last node, which may also be referred to as the source, now has the ability to check that the route list has not been altered in any way by utilising the hashed SRR that is included in the REP message. This feature was previously unavailable.

As far as ASRAN is concerned, this is an additional step that is being taken towards strengthening the degree of security that it provides. The SRR that has been added will be hashed using the technique that is now being used, and the hash that is produced will be compared to the one that has been hashed and transmitted from the node to which it is currently being sent. The issue with ARAN is resolved, and it is guaranteed that ASRAN will always be truthful as a result of this.

Neither the beginning nor the end nodes in an ARAN network are intended to be able to detect any modifications that may take place when the network is in operation. Due to the fact that this is the case, there will be a breach in security since the last intermediate node in the chain will be unable to verify whether or not the contents of the packet have been altered. The provision of monitoring capabilities at the terminal node is the means by which ASRAN addresses and rectifies this issue.

5.5 CSRP ARCHITECTURE

A stable and secure method of routing via the network is provided by the CSRP protocol. In this section, we have demonstrated not only the operation of CSRP but also its performance with the aid of an architecture. provides an illustration of both the architecture of CSRP as well as the common secret keys, both of which are susceptible to vary based on the exhibits of secret keys. illustrates the process by which a session key may be created between two nodes.

Each node will ultimately generate a session key with the nodes that are directly next to it, and this process will continue until it arrives at its conclusion. indicates that all of the required components have been put together effectively. Following the generation of the session key, the source node will begin the broadcasting of RREQ, and this process will continue until the RREQ reaches its ultimate destination.

Following that, an RREP is transmitted from the destination to the source along the path that the RREQ first arrived at when it was being transmitted. The data is then encrypted by utilising the session key of two neighboring nodes in that route before it is provided from the source in that route. This occurs before the data was delivered. After then, the data is decrypted by utilising the same session key, and this process is continued until the data reaches its destination. Eventually, the data will arrive at its destination. demonstrates the flooding of RREQ and RREP in the order of inundation, beginning with D and ending with S. provides evidence that the data has been sent by encrypting and decrypting it with the session key.

We are aware that assaults such as spoofing, black-hole, wormhole, and byzantine attacks, amongst others, have a substantial impact on MANET and cause the performance of the network to suffer. These attacks are among the many that have been identified. Consequently, this architecture not only contributes to the security of the data against both active and passive threats, but it also establishes a secure environment for the transit of data. In the first stage of the process of exchanging keys, the source node creates a secret key and trades its public key with the nodes that are located one hop away from it. In the second stage, the source node trades its public key with the nodes that are located two hops away from it and creates a secret key.

Both of these tasks are performed in order to complete the procedure. It will be possible for the node to participate in the routing operation once the key exchange procedure has been successfully completed. When the route is being established, a secure path will be constructed between the sender and the receiver. This will take place during the process. Following the third phase, which entails the secure exchange of public keys between the sender and the receiver, the fourth step involves the formation of a communication secret key, and the fifth step involves the transmission of data.

5.6 A NEW SECURE ROUTING PROTOCOL APPROACH

The fundamental goal of our proposed protocol, A Novel Approach of Secure Routing Protocol (NASRP), is to achieve the goal of providing a safe and secure path for data transfer between nodes. The NASRP protocol mediates communication between the AODV and SRP protocols from their respective points of view. Every step that AODV offers is considered. Note that NASRP differs from DSR in that it restricts routing packets to only two address fields. To the contrary, DSR checks that each intermediary node has enough room in the routing packets. the NASRP routing protocol's structure, where "DA" denotes "Destination Address," "SA" denotes "Source Address," "HC" denotes "Hop Count," and "SN" denotes "Sequence Number."

An address field that is filled out by both the packet sender and the super sender is essential for the Network Address Resolution Protocol (NASRP) to function properly. It is the responsibility of the packet's sender to complete the other address field. So far, we have presumed that all nodes use RSA as their A symmetric key, a hash function, and public and private keys are all components that every node in a public-key cryptosystem will have. A symmetric key will also be a part of the system. NASRP guarantees the integrity and non-repudiation of routing packets. That is something that the protocol guarantees.

5.7 MOBILE NETWORKS AND TOPOLOGY

It is not possible to repeat the experiment under the same conditions since the experimental Manet's simulation of topologic and mobility needs is quite restricted, as mentioned in the preceding paragraph. It is possible for a Manet network's topology to evolve in unexpected ways. Because of these factors, the modelling process is become extremely challenging, if not impossible. Included in this list are elements such as mobility, the flexibility of electromagnetic wave propagation, and the attenuation of signals with distance. Mobility is not limited to the movement of certain nodes in the Manet; it encompasses the dynamics of the entire network as a whole.

The propagation zone is the physical location where the signal is really sent out. Thus, when a door is opened in an interior setting, the connection distribution changes. Similarly, when a vehicle travels between two nodes, the link distribution also changes. The door itself is to blame for this. Link distribution simulation models for mobile networks, sometimes called propagation, are used to evaluate the proposed services based on their topology and mobility metrics. Simplifying real-world occurrences allows for the construction of these models. To build a mobile-friendly network architecture, the research makes use of two distinct kinds of simplified models.

The random graph model is one option for use indoors among several others. It is possible to make use of this specific model. The model states that the number p1 represents the likelihood

of a link existing between any two nodes at any given time. At every given time, this likelihood may be discovered. With the help of a simple technique that explains changes from existing connection states to nonexistent ones and back again, mobility simulations are run. Even if it does, the connection may go down the drain at some point in the future. Each and every one of the nodes, regardless of their location, will have the same probability. Regardless matter where the nodes are located, this remains true.

It states that the propagation circumstances and obstacles between two nodes (such as walls, furniture, etc.) are far more important than the link's actual location inside the room for determining if a connection exists. You can use the other model, the random unit graph model, in conditions where there aren't many obstacles, like inside and outdoors. To be valid in this paradigm, a connection between any two nodes must meet a certain threshold for the distance between them, denoted by d. What this number represents is the maximum possible distance for a wireless interface link. Among the many possible implementations of the mobility idea in this model, this study employs the random point route model. After a node arrives at its target point, it stays there for a specified amount of time (tstop) in this model.

After that, a new destination point is randomly selected from a pool of points distributed evenly over the virtual space. Without leaving the current site, the procedure repeats until the node reaches its ultimate destination. The range of potential values (Vmax and Vmin) is randomly distributed, with no particular pattern. The rate of acceleration is totally dependent on random chance. Even after being stationarized, the distribution of nodes in space will retain its initial evenness if such was the case. Dividing the total number of nodes in the simulation by the area (2D) or the volume (3D) of the space region being simulated is all that is needed to determine the node density stationarily in this particular context.

The Platform that was chosen for this specific simulation environment is the Network Simulator. Ad hoc mobile network extensions built within the Monarch CMU framework were utilised to design this environment. One of the two modules was built specifically for

conversion. One application that could change the format of trace files so they are usable by network analyzers is NS-2 ns2tcpdump.

As an added bonus, tcpdump2mib may use data from incoming and outgoing nodes to produce MIB-II relevant variant values. You may get both of these apps from the app store. Both of these applications are available on the ns2tcpdump website. Using these parts, one can check the legitimacy of the security services being given by using false or fake information. The modules were written in C, and for knowledge on different parts of the capabilities, we looked at a number of libraries, such libpcap and ucd-snmp (Net SNMP). C was important in the completion of the modules.

5.8 OLSR AND DCDP PROTOCOL EXPERIMENTATIONS AND VULNERABILITY

The ability to control MAE's usage is provided via the option -cert. There will be no disruption to self-configuration or routing services in its absence; nevertheless, messages will not have an MAE. Every single one of the produced messages gets a digital signature if the -cert option is used. The addition of parameters to this option may not be necessary. before the circumstance when it is supplied without parameters occurs. The message authentication element (MAE) is a PEM file that includes a user or node certificate, the certificate authority that signed it, and the private key that is associated with the certificate. The purpose of the certificate is to verify the MAE of received messages. When this isn't the case, an authentication element for messages is passed to the option.

The process of renewing the certificate is the only thing that can be achieved through collaboration in this particular circumstance. Managing the node's actions on the collaborative certification services is accomplished by utilising the option -share. If this is missing, the node will be unable to access the ACD private key in any way. This means that without the private key, the node can't join coalitions that provide collaborative certification services. If the -share option is used, the node will also execute an L-Cert instance with the uolsr command. The addition of parameters to this option may not be necessary.

Before joining any coalitions to provide certification services, the node must get its share of the ACD private key through the collaborative method, namely using L-Certs, in the case that no parameters are provided. This holds true regardless of the presence or absence of parameters. In all other cases, its argument will be a PEM file containing the portion of the private key that corresponds to the option. This is going to happen. Changing the private key is the sole operation that will be executed cooperatively in this particular circumstance. Finally, but most importantly, the -autoconf option indicates that this specific node is responsible for the self-configuration process.

If you do not choose this option, the node will not have the ability to configure itself using the self-configuration protocol; instead, only the routing protocol will be executed. Alternatively, it can use the self-configuration protocol to configure itself or react with configuration queries. You may tell the self-configuration service should be active for the provided interfaces by using the -autoconf option. The interfaces in concern will immediately begin manually setting their IP addresses once the installation of the uolsr service is finished. If a certificate is required but cannot be obtained using the option's -cert property, then acquiring a certificate will be part of this startup.

Using or not using an MAE does not affect the feasibility of sending or producing attack messages. The responsibility for controlling this process lies with the -cert option. It is probable that Attacks will be created regardless of whether the MAE is made public, as they are actively in development. When the -cert option is used, a digital signature is issued to every freshly generated message. If you choose this option, you should expect to get a PEM file.

The expected contents of this file include the following: the sender certificate, the certificate of the certifying agency that signed it (to validate the MAE of received messages), and the private key associated with the certificate, which is used to sign those specific messages. If you run the command without any arguments, it will just display incoming and outgoing

messages in real time and act as a network analyzer. When executed in this format, the command functions just as a network analyzer; the usual accompanying parameters are not necessary.

First, we followed the instructions to the letter and performed the OLSR and DCDP procedures. The experiment did not use MAE protection because of this. For this specific scenario, you need to run the uolsrd command without the -cert and -share parameters. Due to this scenario being attacked in every way described in, the protocols were corrupted and were contaminated. As the scenario's outcomes demonstrate, the assailants were the ones that corrupted the procedure. The majority of the time, it will act as a denial-of-service attack, but there may be other consequences, as mentioned above.

By doing this experiment, we hope to be able to test, in a more concrete way, if the hypothesised vulnerabilities hold water. The graphical user interface of the OLSR protocol implementation (uolsrd) allowed for quick evaluation of routing difficulties caused by attacks (such as changes to MPR sets and link symmetry breaking), which is important for network security. The incorporation of the graphical user interface into the system made this possible. A successful DCDP attack on a neighbourhood node that attempts self-configure will result in the adversary's failure to finish the procedure. This is valid for assaults that aim at the server as well as the client.

5.9 SECURITY EVALUATION

The validation of the recently built security services is carried out with the assistance of an experimental Manet that is comprised of ten nodes; the description of this Manet may be provided here. Two of these nodes are used as properly behaved nodes, which implies that they run OLSR and DCDP in addition to L-Cert and L-IDS services in an acceptable manner. In other words, they meet the requirements for good behaviour. The two nodes that are still operational serve as adversaries and are responsible for the attacks that were previously outlined.

Assessment is a procedure that may be broken down into three basic steps. Utilising the routing and self-configuration protocols, in addition to the intrusion detection service, is the first step in the process of constructing the network. This project's objective is to evaluate the effectiveness of the intrusion detection system (IDS) that was built in terms of its ability to make detections. The adversary nodes are the ones that are responsible for carrying out the attacks that have been detailed against the protocols.

The results of the assaults occur in a manner that is analogous to what happens when there is no security mechanism in place. Due to the fact that the corrective protection mechanism, which is comprised of the interaction between L-IDS and L-Cert, is not active, it is possible that the results of the attack will continue to be observed even after it has been established that the assault has taken place. provides an illustration of a particular topology that was utilised by the Manet over the course of the experiment in order to emphasise the detecting procedure.

5.10 DATA DISTRIBUTION ENCODING FOR EFFICIENT MULTIHOP AD HOC NETWORKS

Internet infrastructure is changing at a dizzying rate due to the proliferation of implantable, sensor-packed, network-connected gadgets. The widespread availability of these gadgets has led to this. Due to the ubiquitous nature of the devices presently accessible in our culture, wireless networks provide the most simple way to connect them. The infrastructure-based wireless communication paradigm is also often inadequate to satisfy the demands of an environment defined by ubiquitous computing: Building the foundation of the network from the ground up can be a time-consuming ordeal.

Deploying equipment can also be expensive, which is a major consideration. So, if we want to increase the number of locations that can access the Internet and get standard networking services, one of the best possibilities is multihop ad hoc wireless technology. Because these technologies can support more people, they are more popular. A suite of multihop ad hoc network technologies has been developed to address the large variety of interconnected

devices, from tiny sensors and actuators to multimedia PDAs, and the vast array of communication needs, from localised coverage with a few kilobits of bandwidth to citywide coverage with broadband connections.

Multihop ad hoc network technologies emerged as a result of these many factors. When tiny, inexpensive, and energy-efficient devices (sensors) that don't need a huge data rate to complete their jobs can communicate with one another, we call it a sensor network. In contrast, data collection is the primary motivation for establishing sensor networks. Additionally, there is an alternative that goes by the name of a mesh network. Since it borrows heavily from the architecture of wireless mesh routers, this network type can cover more ground. Devices in a city should be able to talk to each other and transfer media files automatically.

A comprehensive explanation of the ad hoc networking methods is offered in the paper cited in reference number 6. The concepts of these techniques are explained, examples of their potential applications are shown, and any questions or issues that are yet unresolved are addressed in this overview. Opportunistic networks, a type of ad hoc networking, provide the most interesting setting in which to implement the encoding techniques discussed in this chapter. This chapter will go into these approaches. Building opportunistic networks is the next step after developing the idea of a multihop ad hoc network. The limitation of end-to-end connectivity is removed in opportunistic networks. Actually, the end-to-end concept is typically the basis for how mobile ad hoc networks operate.

It follows that there must be a method for information to go from the source to the receiver for communication to be fruitful. Encapsulated end-to-end connection is usually all that's needed for interactive services like VoIP, online gaming, and video streaming. Chatting, emailing, and file sharing are all examples of data applications that might be implemented. continue to execute without issue, even when the end-to-end requirement has been relaxed. However, in theory, they can still function even if a path never exists between the sender and the receiver.

Until a better time to forwards them arises, nodes in an opportunistic network will keep a copy of the messages in local memory. Instead of storing the packets on the network, they are kept locally in case that connection is lost. Because of this, they won't become lost or confused. Conversely, in this scenario, intermediate nodes store messages when there is no chance to forward them (for instance, when there are no other nodes within transmission range or when neighboring nodes are not useful to reach the destination), instead of immediately forwarding them like in the traditional multihop communication method, they instead take advantage of any contact opportunity that comes their way.

Under multihop communications, intermediate nodes keep acting as routers. Conventional approaches to data distribution, developed for the wired Internet, fail miserably in ad hoc settings owing to the inherent limitations of wireless communications, even under static conditions. This remains true even in the absence of change. Systems built for ad hoc networks, with the exception of most older systems, cannot function with the assumption that bandwidth is provided at no cost. They must also be resilient enough to deal with changes in the wireless connections' characteristics that are beyond their control. We also require this. The issue already has several aspects before dynamic topology reconfigurations are applied to it. Possible causes of these reconfigurations include user migration or energy management measures that temporarily disable some nodes.

However, more recent systems may not always be able to handle these limitations because of the inherent complexity of wireless multihop ad hoc networks. Only in wireless multihop applications can these restrictions be felt. Thus, in contexts including multihop ad hoc networking, data distribution systems have recently become a popular subject. These systems can be tailored to suit sensor network uses or built for peer-to-peer and content delivery paradigms. These systems may be modified to by rethinking peer-to-peer and content delivery.

Data encoding techniques are an essential part in dealing with the vast array of problems that might develop inside these systems. One example is the use of erasure coding techniques in

the development of a reliable point-to-point protocol for use in wireless sensor network data transfer. In creating this technique, we made use of the available approaches. Additional uses of erasure coding techniques in WSNs were detailed in the referenced studies. A thorough explanation of these uses was provided. Implemented to aid in distributed data caching across the network and to enable easier data retrieval in the future, they have also been used as a means to achieve energy-efficient data transfers.

Finally, they have been used to reach the goal of energy-efficient data transmissions. They have also been used for data transmissions that require a considerable amount of source power, just to give you an idea. It has been demonstrated that erasure codes are useful for facilitating voice interactions over very efficient mobile ad hoc networks. Because erasure codes shorten the transmission time of data packets, they can be used in scenarios where real-time data processing is essential. For this reason, erasure codes are employed.

For use in multihop ad hoc networks, erasure code approaches have been enhanced by providing several encoding stages for the same data. Their use in these networks has been made possible because of this. The data may then be encoded in a more intricate way because of this. "Network coding" is the English word for this fundamental concept. In the context of the Both the transmitting and receiving nodes, as well as any intermediary nodes, use network coding to encrypt data packets. The proper transmission of the data packets depends on this. To facilitate one-to-many communication, the data-generating node encrypts the information locally before sending it to a selection of its neighbours.

This happens when one-to-many communication is being used. In order to create a fresh set of encoded data packets, these relay nodes use the previously sent data packets as a starting point. This guarantees the highest level of accuracy for the data packets. After they've gotten their hands on them, they'll start scattering them to their ultimate locations. With the evolution of multihop ad hoc networks, network coding has emerged as a feasible approach for data delivery.

Actually, it may offer very high dependability while making very effective use of the available bandwidth. It has been used effectively to guarantee the most efficient use of energy potential in multicast transmissions carried out via mobile ad hoc networks. A great deal of success has been attained in doing this assignment. There has also been a lot of research and consideration into the potential uses of network coding within the framework of mesh networks and vehicle ad hoc networks.

5.11 NETWORK CODING

Within the realm of networking infrastructure, network coding has emerged as a unique and potentially lucrative topic in recent years. This came about as a result of the introduction of network coding. However, despite the fact that network coding, erasure coding, and digital fountains all have certain fundamental concepts in common, network coding is distinct from the aforementioned encoding systems in a number of fascinating areas. This is due to the fact that network coding is differentiated by a significant number of different characteristics. First and foremost, the objective of network coding is in no way related to that of digital fountains on any level.

Between the two, this is the most important distinction. Network coding is developed with the purpose of improving the utilisation of resources during transmissions that take place over the network, particularly with regard to bandwidth and throughput. This is the primary motivation for the development of network coding. Because of this, the idea for the thought has been conceived as a result. Network coding also makes it possible to have optimal latency and a better distribution of traffic throughout the network.

Both of these benefits are made feasible by the network. We are able to accomplish this thanks to the distribution of traffic. As a consequence of this, entire load balancing is achieved, which is particularly encouraging in circumstances where the primary concern is the conservation of power (for example, wireless ad hoc and sensor networks).

It makes the network more resilient to the loss of nodes and connections (even if they are lost permanently), and it makes the network more flexible to changes in its topology. Both of these benefits benefit the network. In light of the fact that the major purpose of erasure coding is to ensure the dependability of transmissions, the primary objective of network coding is to provide the greatest possible utilisation of the network in general. A strategy known as erasure coding, on the other hand, is a technique that aims to lessen the amount of information that is lost while it is being sent.

Additionally, in terms of its durability and flexibility, network coding appears to be very suitable to new evolving conditions of harsh and challenged networks. This is the case considering the fact that it is extremely adaptable. Taking into consideration the fact that it is perfectly appropriate, this is the situation. There are a few instances of use cases that illustrate this sort of application. Some examples are ad hoc networks with intermittent connections, automotive ad hoc networks, underwater acoustic sensor networks, and delay-tolerant networks, which are also referred to as DTNs.

Furthermore, it would appear that the new harsh and complex network circumstances are a good fit for network coding. This is something that ought to be considered. As a result of the fact that nodes in these circumstances may relocate, get corrupted, or simply enter a sleep state in order to conserve energy, the probability of a connection failing is really rather significant. It has been demonstrated that algorithms for data distribution that are founded on network coding result in a high level of success. This is because these algorithms take into consideration the fact that all nodes are interested in learning all of the information that is offered. This is the reason why this is the case.

One of the most significant distinctions between erasure coding and network coding is the use of recursive coding at intermediary nodes. This is in addition to the variations in performance and objectives that exist between the two types of coding. Aside from that, performance and goals are also significant considerations. Both the data that was originally transmitted and/or

the data that is going to be transmitted are encoded at the source nodes as well as the intermediate or relay nodes in a network that makes use of network coding technique. Transmitting data is something that can be done with this kind of network. However, in generic relay systems, relay nodes simply replicate messages in the direction of the successive hops that have been specified. This is in contrast to the situation in other types of relay systems.

5.12 ROUTING PROTOCOLS FOR MOBILE AD HOC NETWORKS

Even in the absence of a network backbone that has been built to an advanced point, wireless ad hoc networks are able to function normally. The construction of temporary networks is something that happens on a frequent basis in order to accomplish a certain goal. One example of an activity that falls under this category is providing communication in the case of an emergency or when engaged in battle. Other examples include communicating during times of conflict. The conditions in which the development of conventional infrastructure would either be impossible or inefficient are the ones in which they perform most effectively.

In the vast majority of instances, this is the situation. To differentiate itself from more traditional network topologies, the regular nodes of an ad hoc network need to be able to perform the tasks that are often assigned to infrastructure components such as access points, switches, and routers. This is necessary in order for the network to be able to function independently. It is imperative that this be done in order for the network to carry out its vital duties. Despite the fact that it is not guaranteed that the nodes that are participating will be online at all times and that they will have limited energy reserves, it is anticipated that the great majority of the time, the nodes that are participating will be mobile.

For instance, in cellular and WiFi networks, the wireless connection is only established up to the point where it is connected to the access point or the base station. This is the case in both types of networks. Within the wired domain, the majority of the routing operations are carried out. Two examples of infrastructure-based wireless networks are wireless local area networks

(WiFi) and cellular networks. As an additional category of wireless networks, cellular networks are also included.

The only thing that a mobile node has to do in order to move from one location to another is to figure out which base station it should interface with or how it should handle the transition between stations. If it wants to be successful, this is the sole thing that it must achieve. Due to the current circumstances, the individual does not have any other choices available to them at this time. Since quite some time ago, wireline routing has been regarded as a well-established field that makes use of methods that have been fully evaluated and demonstrated to be successful. This distinction has been maintained for quite some time.

The topology, bandwidth, routing, and switching resources of the infrastructure are all given in such a way that they are designed to be compatible with the volume of traffic that is expected to be there. This guarantees that the infrastructure is capable of managing the quantity of traffic that is expected to move through it. Routing, on the other hand, becomes a huge difficulty in ad hoc networks since it is maintained by regular nodes and does not require any specialist equipment or a particular placement inside the network. This makes it a significant problem.

Because of this, it provides a tremendous hurdle. Finding a solution to the problem has become more difficult as a result of this new development, which has increased the complexity of the problem and made it more difficult to find a solution. Consequently, the introduction of ad hoc networks marked the beginning of a resurgence in interest in routing, despite the fact that it must overcome a number of obstacles, such as the mobility of the nodes, limited energy resources, heterogeneity (which, in certain circumstances, may lead to asymmetric connections), and a great deal of other challenges.

Despite the fact that a significant number of different routing algorithms have been created as a response to these challenges, the field of ad hoc routing continues to be one that is an area that is always active and evolving. Ad hoc routing algorithms are providing allied

technologies, such as wireless sensor networks and mesh networks, with a supply of ideas and techniques that they may employ in their own development. These technologies can include these ideas and methods into their own development in order to enhance their own growth. As part of the scope of this chapter, we are going to conduct an in-depth investigation of the topic of wireless ad hoc routing.

In spite of the fact that we made an effort to incorporate the great majority of the main algorithms, it is not possible to consider our survey to be exhaustive: A greater number of unique algorithms and versions have been made available than the number of those that have been supplied. In this section, the reader will be given an overview of the challenges, restrictions, and possibilities that are associated with this particular subject. Despite this, we made an effort to cover the majority of the capabilities that are available in ad hoc routing. In order to accomplish our goal, we wanted to give the reader with this summary.

5.13 AD HOC NETWORKS APPLICATIONS

Attending a gathering of people. The use of mobile devices for the purpose of conducting conferences is, without a doubt, one of the applications that has received the most attention. Establishing an ad hoc network is essential for mobile users who need to collaborate on a project outside of the typical office environment. This is because it allows them to interact with one another and allows them to work together on the project. Emergency services are available. Within the field of ad hoc networking, an additional application that fits in naturally is one that deals with responding to emergency conditions such as disaster recovery.

This is an example of an obvious use. A number of mobile users, including police officers, firefighters, and other first responders, who are equipped with a variety of wireless devices, not only need to be able to communicate with one another during times of emergency, but they also need to be able to maintain their connection for extended periods of time. Making connections for the home. It is also possible to establish an ad hoc network using the wireless computers that are located throughout the house.

Within this type of network, it is possible for any node in the network to connect with the other nodes, independent of the location where the nodes were first joined to one another. As an alternative to the common practice of assigning several Internet Protocol (IP) addresses to each wireless device, this technique provides a means of identifying each individual wireless device. Programmes that make advantage of computers integrated inside them. The utilisation of ad hoc networking makes it possible to create communication in a manner that is not only flexible but also efficient. This is a service that is provided by a number of the ubiquitous computing internetworking devices.

A wide variety of mobile devices, including personal digital assistants (PDAs) that are outfitted with wireless ports and Bluetooth radio devices, are already offering wireless components that may be purchased as add-ons at prices that are not prohibitively expensive. There is one example of sensor dust. One may consider this application to be a combination of an ad hoc network and a sensor network for the sake of application. It is recommended to distribute a group of sensors that are equipped with wireless transceivers in order to obtain critical information about an unknown place through the development of ad hoc networks that are constituted of these sensors while dealing with conditions that have the potential to be harmful or dangerous.

Computers and automobiles interacting with themselves. A number of wireless devices (such as a laptop, a personal digital assistant, and so on) that are being used for a variety of purposes at the same time can work together to establish an ad hoc network in a car. This can be accomplished through the collaboration of different wireless devices. It is possible that increased productivity will arise from this partnership. If you are travelling to a new city, for example, you might need to find the car repair shop that has the best reputation in the region in order to get your vehicle mended while you are on your way to the meeting.

As an additional feature, Bluetooth and personal area networks are incorporated. A Personal Area Network, more commonly referred to as a PAN, is a type of network that is established

by linking a number of distinct devices that are either connected to or carried by a single person. Despite the fact that mobility problems are not addressed when devices inside a PAN connect with one another, this is not the case when many PANs are required to communicate with one another. It is possible that the versatility that ad hoc networks provide might be of tremendous advantage to wireless communications between PANs. Bluetooth, for example, is a wireless technology that is currently included into a great number of personal digital assistants (PDAs). The term "piconet" refers to a network that involves up to eight personal digital assistants (PDAs) that are able to communicate.

5.14 PROTOCOLS FOR AD HOC NETWORKS ROUTING

With regard to ad hoc networks, there are currently a number of different routing protocols that are in existence. Each of these protocols is designed to address a certain implementation scenario. On the other hand, the major aim has always been to develop a routing protocol that simultaneously increases throughput while simultaneously reducing control overhead, the ratio of lost packets, and the amount of energy that is used.

As a result of the many settings in which these various sorts of networks may be used (for instance, in the aftermath of a natural disaster, on a battlefield, at a conference, etc.), the requirements and challenges of these various forms of networks are unique from one another. Furthermore, as a consequence of this, the routing protocols that are utilised in ad hoc networks are able to be partitioned into five unique categories according to the architectural foundations upon which they are established.

5.14.1 Protocols initiated from the source

The phrase "source-initiated routing" refers to a category of routing protocols in which the formation of a route does not take place until the source makes a request for one to a point of arrival. This is the case in the aforementioned category of routing protocols. directly after the source makes the request for the route, the network is inundated with one-of-a-kind route

request packets, and the process starts with the neighbours that are directly next to the source. This process will continue until each and every neighbour in the near vicinity has been identified and contacted.

The process of establishing how one can get to a specific area is referred to as destination, and it is considered to be finished when it has either resulted in the development of a route or the acquisition of several pathways to the destination. Through the utilisation of a technique known as route maintenance, the operational routes are preserved in a state of good operating condition over the entirety of their lives.

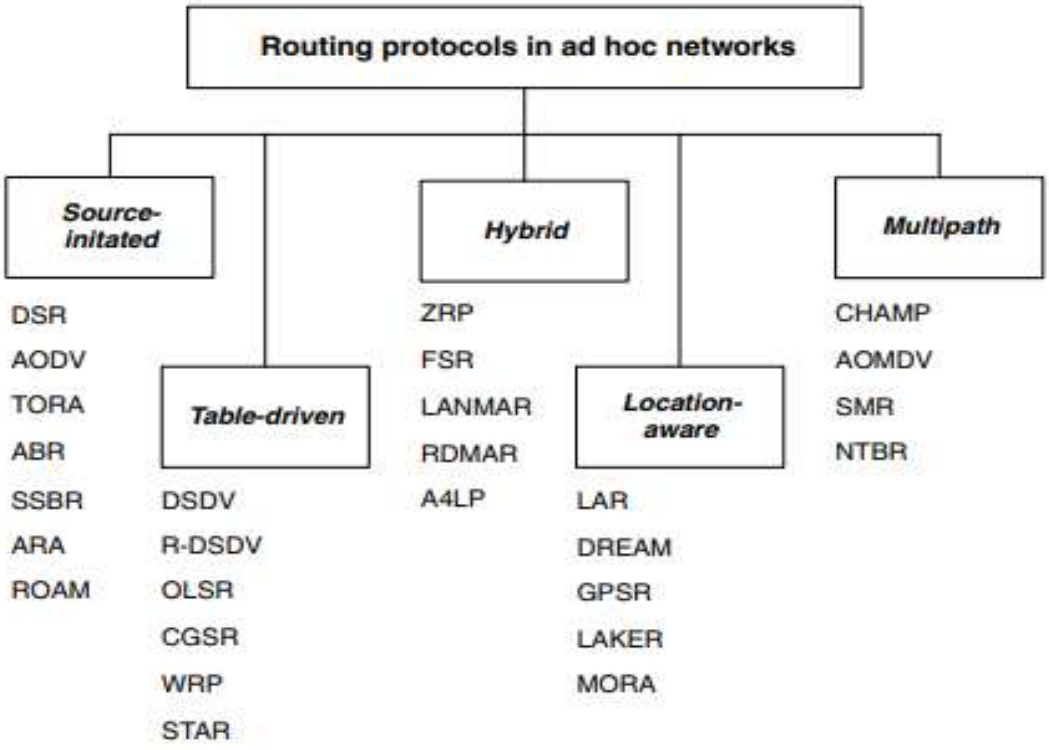

Fig: 5.2 Ad hoc routing protocol classifications

Source: Algorithms and protocols for wireless and mobile ad hoc networks data collection and processing through by Azzedine Boukerche (2009)

5.14.2 Dynamic Source Routing (DSR)

Among the several routing protocols, the Dynamic Source Routing (DSR) protocol is one of the most often discussed protocols. The DSR routing methodology is a "on-demand" routing method that combines both the route discovery and route maintenance stages into its operational process. When performing the operation for route discovery, it is essential to send both route request messages and route reply messages. This is a need. A node that desires to transmit a message is needed to alert its neighbours by sending out a route request packet during the phase of route discovery. This is done in order to fulfil the requirements of the phase. This action is taken in order to ensure that the node is able to successfully relay the message.

Any node that is within range of a broadcast will add its own node id to the route request packet and attach it to the packet before it is sent out again. This is done before a further transmission of the packet. Either the destination itself or a node that is currently connected to a node that is currently linked to the destination will be in a position to receive one of the broadcast messages at some point in the future.

This point in time will be determined by the destination itself. Due to the fact that every node has its own route cache, the node will first check that cache to determine whether or not it already holds the path to the target before examining any other location. When it comes to the process of route discovery, having a route cache that is kept in each node can assist reduce the amount of time and resources that are necessary for the process.

In the event that the route is found in the route cache, the node will send a route reply message to the node that first issued the route request. This is in contrast to the practice of sending the route request to the subsequent node across the network. The information on the route will be made accessible to the initial packet that is transported to the target node without any problems. DSR based its operations on the premise that the route it has got is the one that travels the shortest distance.

This is due to the fact that DSR takes into consideration the time at which the first packet arrives at the destination node. A route reply packet is sent back to the origin from the destination, and it contains information on the whole path that was travelled in order to arrive at the origin. Due to the fact that the sending node is already familiar with the path that is the most efficient to reach the receiving node, it is able to immediately begin delivering data packets. The recent information has been incorporated into the route cache that is situated at the origin of the communication.

During the time that the route is being maintained, there are two distinct types of packets that are utilised. These packets are known as route error packets and acknowledgement packets. By comparing the current routes to the acknowledgements, it receives from the nodes that are in the immediate vicinity, DSR ensures that data packets are being delivered over the right paths. The transmission of data packets is ensured as a result of this. The receiver of a packet receives an acknowledgement message when a node passively detects that its neighbour on the next hop is conveying the packet down the path to its final destination.

This acknowledgement message is provided to the receiver of the packet. The purpose of this action is to ensure that the node is able to communicate to the receiver that the packet has been received. A route error packet is sent out by a node that is experiencing difficulties during transmission. This packet serves as an indication that the node did not get an acknowledgment from the network. It is necessary to send this route error packet back to its point of origin in order to start the process of route discovery all over again. After the nodes have been informed that a route error has occurred, they instantly remove the item from their respective route caches that is reliant on the broken connection. This occurs immediately after the nodes have received the notification.

5.14.3 On-Demand Acyclic Multipath Routing (ROAM)

The ROAM method of routing depends on coordination between nodes along directed acyclic subgraphs. These subgraphs are simply specified by the distances that routers are from their

respective destinations. With the addition of this new capability, the DUAL routing algorithm has gone through an expansion. The fundamental reason for this is that traditional on-demand systems have a propensity to employ floods during route discovery on a recurrent basis until a destination is discovered. This is the primary reason why this is the case. In the event that the initial part of the search does not uncover any routes, the sources are uncertain as to whether or not they should proceed with the second phase of the search.

It is possible that this will become a problem if a rogue router searches the network indefinitely for a route that does not exist, which might result in congestion on the network. No mechanisms that offer protection against assaults of this nature are included in the standard protocols that are in implementation. When using ROAM, a search query will either offer the path to the target or it will convince all of the intermediate routers that it is impossible to connect to the destination host. Both of these potential outcomes are feasible results. Every single ROAM router functions independently and is accountable for its own independent monitoring and maintenance of the distance, routing, and link cost.

While routing maintains a column vector that contains the distance to each destination, the feasible distance, and the reported distance, the distance keeps track of the distances of nodes for each destination as well as neighbours from the relevant node. In addition, the distance also keeps track of the neighbours of the relevant node. The distance, on the other hand, is only a measurement that keeps track of the distance between the nodes that are in way to a particular destination. The connection price takes into account the whole cost of, which includes the bandwidth that is necessary to establish a connection with each of the router's neighbours. The routing protocol makes use of three distinct types of control packets.

These packets make up the routing protocol. Questionnaires, responses, and updates are included here. In the event that a router wishes to add an entry for a particular destination, modify its distance to the destination, or delete the entry for the destination, it will be necessary for the router to change its routing for the destination. ROAM routers can be in

either an active or passive mode, depending on the configuration of the router. If a router has questioned all of its neighbours and is presently waiting for a response from those neighbours, then it is regarded to be in an active state. If it has not queried all of its neighbours, then it is considered to be in a passive state.

In order for a router to select a neighbour as its successor through the selection of loop-free paths, the neighbour in question must be a plausible successor. Only then is the router allowed to make this choice. This provides a path to the objective that is both free of loops and as short as feasible, and the determination of this path is based on two different algorithms, one of which is passive and the other of which is active. A diffusing search is initiated whenever a router makes a request for a path to a destination. This is the event that sets off the search. After then, this packet makes its way via more routers in the network that do not yet have an entry for the node.

The information on the distance to the node is transmitted back to the source by the first router that possesses a route through which it is possible to reach the destination. By the time this search is over, the origin either has an estimate of the distance that needs to be travelled in order to reach the destination or has arrived at the conclusion that the destination is not reachable. The adjustment of the connection costs is also determined by the number of packets that are received after they have been sent. Should the passive and active successor algorithms be utilised in the process of selecting the successors, the ROAM will generate multipaths that do not contain any feedback loops. This algorithm is well-suited for usage in wireless networks that have constrained mobility because of the intrinsic qualities that it possesses.

5.14.4 DSDV, or destination-sequenced distance vector

As its basis, the Bellman-Ford routing algorithm serves as the basis for the distance-driven DSDV (Destination Sequenced Distance-Vector) routing protocol. Target Sequenced Distance-Vector is what the abbreviation DSDV stands for. Every mobile node is accountable for the upkeep of its own routing table, which includes a list of all the possible destinations as

well as the number of hops that are necessary to reach those destinations. Additionally, for each item, there is a sequence number that was assigned by the recipient.

This number is included in the package. The utilisation of sequence numbers may be utilised to achieve both the task of locating duplicate data as well as the task of halting cyclical processes. It is necessary to often broadcast any modifications to the network's routing in order to maintain the network's routing in a consistent and uniform manner. The full dump updates and the incremental updates are the two distinct types of updates that are accessible.

5.14.5 OLSR, or Optimized Link State Routing

The OLSR makes a contribution to the optimisation of a link state that is pure by virtue of its capacity to reduce the quantity of retransmissions that result in flooding the whole network. As a result of this, the OLSR is able to reduce the amount of data that is transmitted along with each message and reduce the total control overhead. This is a significant benefit. For the purpose of effectively flooding control messages throughout an entire network, this approach takes use of a multipoint relaying mechanism. If we make advantage of the multipoint relay, we will be able to greatly reduce the number of local retransmissions that are required. In order to serve as multipoint relays (MPR) for the network, each node selects a group of its close neighbours to serve in this capacity.

We selected these neighbours using a random selection process. The non-MPR nodes that are neighbours of the node do not pass the packets even if they process them. This is due to the fact that the node only sends any broadcast messages to the other nodes that are MPRs. During the process of putting together the collection of multipoint relays, it is essential to make a thoughtful decision in order to ensure that the coverage area covers all of the neighbours that are located within two hops.

It is imperative that this collection be reduced to an absolute minimum, to the degree that it is even remotely conceivable, in order to guarantee that the least amount of packets be

transmitted as is remotely possible. Every single one of a node's neighbours that are within two hops of N has to be able to interact in both directions with the nodes that are a part of N's multipoint relay set (MPR set). This is a requirement.

Through the transmission of HELLO packets at certain intervals, which contain information on all of the neighbours and the links that have been created, it is possible to conduct an exhaustive evaluation of the current condition of these relationships, which is beneficial to all parties involved. A route is nothing more than a series of hops that travels from the origin to the destination. This is due to the fact that the multipoint relays of the network are located within the system itself. In order for messages to be forwarded, the source only has to know the information that is required for the next hop along the route; hence, it is not essential for the source to know the information that is required for the complete route itself.

5.14.6 CGSR, or Cluster-Head Gateway Switch Routing

Clustering is a process that may be carried out with the assistance of the CGSR protocol, which is a decentralised method that is known as the Least Cluster Change (LCC). A framework for the creation of new features for channel access, bandwidth allocation, and routing is formed by aggregating nodes into clusters and providing the leaders of those clusters control over those clusters. This framework is called a framework for the development of new features. Through communication with the nodes, the cluster head is able to establish connections with other cluster heads that are present inside the network.

Because frequent transitions in the leadership of the cluster have the ability to wreak havoc on the effectiveness of the algorithms that are used to allocate resources, selecting a cluster head is a procedure that is of the utmost importance. Selection of a cluster head is a task that is of the utmost importance as a result of this. As a consequence of this, it is of the highest significance that the consistency of the cluster be preserved over the length of this design. Because the leadership of a cluster will only change in one of two conditions, the LCC method is dependable.

The first scenario is when the leaders of two different clusters get within range of one another, and the second scenario is when a node in the network loses connection with all of the other clusters. CGSR is an effective method for assigning channels across the various clusters because it maximises the potential of the space that is available for reuse and makes the most efficient use of the space that is available. As an illustration of one of the criteria that CGSR puts on the link layer and the MAC scheme, the following is an example: Each and every cluster possesses a unique CDMA code that may be utilised for the purpose of identifying it.

5.14.7 Hybrid Protocols

The utilisation of hybrid routing techniques, which combine on-demand routing with protocol-driven routing, has seen an increase in recent years. These strategies have been utilised more often. Static routing is often utilised at the perimeter of the network, which is characterised by a reduction in the frequency of route alterations in comparison to the core, which lays a larger focus on on-demand routing. These strategies have the ability to increase overall performance while also contributing to the process of bridging the gap that exists between the two major types of routing protocols.

5.14.8 ZRP, or Zone Routing Protocol

The ZRP routing protocol is a well-known hybrid routing system that functions most effectively for widespread networks. With this capability in mind, it was created from the beginning. It derives its name from the fact that "zones" are used to define the transmission radius for each node that is a member of the network of which it is a part. The identification of nodes that are located within a node's immediate neighbourhood is performed via the use of a proactive approach in this protocol. On the other hand, communication across zones is accomplished through the utilisation of reactive methods.

The ZRP protocol takes use of the fact that communication between nodes in ad hoc networks is typically restricted. As a consequence of this, changes in the topology of nodes that are

situated in close proximity to a node are given priority attention. For the purpose of designing a framework for node communication that is interoperable with other protocols that are already in existence, ZRP makes use of this trait. The neighbourhood communities, which are also referred to as.

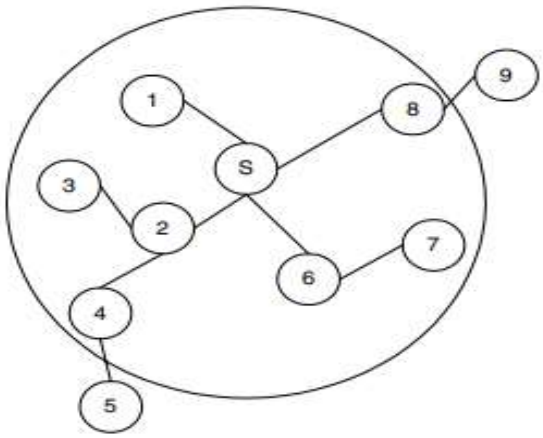

Fig.: 5.3. Routing zone example with = 2

Source: Algorithms and protocols for wireless and mobile ad hoc networks data collection and processing through by Azzedine Boukerche (2009)

Identifying neighboring nodes in a network may be accomplished through the utilisation of either the Intrazone Routing Protocol (IARP) or the more easy "Hello" packets. The Internet Address Resolution Protocol (IARP) guarantees that the routing is always maintained up to date by using a proactive approach. IARP is sometimes referred to as a "limited scope proactive routing protocol" due to the fact that its application is restricted to a specific section of the network. This is due to the fact that the IARP has a somewhat limited scope. Instead of flooding the network with pointless route inquiries that come from outside the zone, route requests that are derived from the zone's boundary (hop counts equal to) are broadcast.

This prevents the network from becoming overloaded with useless route queries. Interzone Routing Protocol (IERP) takes into consideration the locations of the endpoints in each zone

before creating a connection between two zones. This is done before the connection is established. a methodology that is reactive to the circumstance. Inquiries about routes are transmitted to nodes on the perimeter of the network by means of the Bordercast Resolution Protocol, often known as BRP.

Due to the fact that a node does not resubmit the query to the node from whom it initially obtained the query, the control overhead is significantly reduced. This is because the node does not have to repeat the question. Additionally, the number of questions that are duplicated is reduced to a minimum. The ZRP protocol provides a hybrid architecture of protocols, which enables users to choose any routing strategy that is appropriate for the particular conditions that are now being considered. There is the possibility of modifying it in such a way that it maximises the benefits of the advantages supplied by any protocols that are already in existence.

5.15 FSR, OR FISHEYE STATE ROUTING

FSR is a hierarchical routing system that adds many scopes with the intention of reducing the amount of control packet overhead. The protocol is what allows this to be performed. The "fisheye" technique that Kleinrock and Stevens proposed is implemented through the use of a data-driven protocol, which, in its most fundamental form, is a protocol that is driven by data.

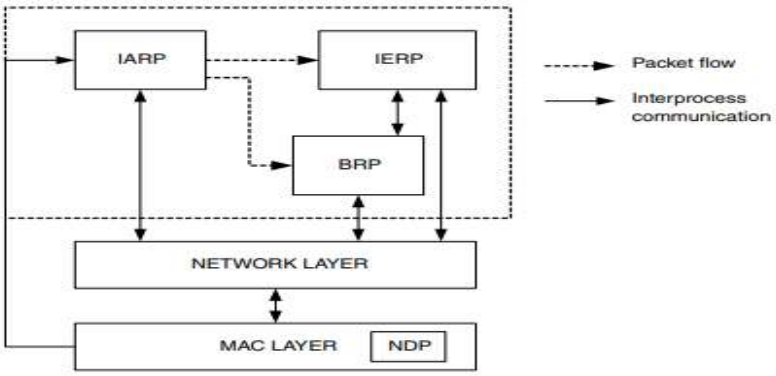

Fig.: 5.4 ZRP architecture

Source: Algorithms and protocols for wireless and mobile ad hoc networks data collection and processing through by Azzedine Boukerche (2009)

The quantity of data that has to be kept in order to effectively display graphical data may be significantly reduced by using this approach, which is notably more efficient than other methods. The theory behind it is that the view that is closer to the focal point of a fish's eye is captured with better detail by the fish's eye, however the detail of the picture that is further away from the focal point is captured with less clarity. This is the basis for the concept.

In this aspect, FSR is analogous to link state routing due to the fact that it keeps a routing at each node. The only important difference is in the type of maintenance that should be performed on them. The FSR standard incorporates the concept of scopes, which adjust themselves in accordance with the number of hops that a packet encounters on its journey from its starting point to its final destination. When nodes are located in closer proximity to one another, the number of update packets that are generated is often greater. On the other hand, when nodes are located further apart, the number of updates that are generated is typically smaller.

Every node in the network possesses a local topology map that provides information about the shortest paths, and this data is regularly transmitted between the nodes for the purpose of facilitating communication. Within the context of the fisheye state routing, the use of distinct exchange times for each of the routing's entries is made easier. During the process of analysing these scopes, the distance that separates each node is taken into consideration. There is a possibility that the size of the message can be decreased, which is the most significant advantage. This is because the routing information of distant nodes does not need to be transmitted. It may become necessary to apply a "graded" frequency update technique across all scopes in order to lower the amount of overall overhead as the size of the network expands.

This is done in order to bring the total amount of overhead down. This protocol is successful for large networks, and it does so while preserving the integrity of route calculations and

requiring just a small amount of control overhead. It accomplishes this without compromising its capacity to scale. However, when a packet comes closer to its destination, its path will become more accurate. This is the case despite the fact that routes to sites that are further away may appear to be out of current.

5.16 LANMAR (LANDMARK AD HOC ROUTING)

By applying a mix of connection status and distance vector techniques to compute the connections between the nodes in a subnet, this protocol generates subnets of nodes that are more likely to travel together as a unit. Within every one of the subnets, a node will be selected to serve as a landmark, carrying out responsibilities that are quite comparable to those of the FSR. The most evident difference that can be made between the FSR protocol and the LANMAR protocol is that the former takes into account all of the nodes in the network, whilst the latter only takes into account the nodes that are included within the scope and the landmark nodes.

This is the most significant difference that can be made between the two protocols. Due to the fact that the landmark nodes are regarded as the most significant nodes in the network, this results in the situation described above. The destination of the packet is compared to the neighbour database that is kept on the node that is responsible for forwarding the packet while the operation of forwarding is taking place. In the case that this is the set of circumstances, the data packet will be dispatched to the address that has been designated as its destination.

Instead, if the distance between the source and destination nodes of the packet is relatively vast, the packet will be sent to the node that is geographically closer to the landmarks that are associated with the packet. This happens when there is a significant amount of distance between the nodes that are the source and the destination of the packet. When the packet comes closer to its ultimate position and acquires more exact information on the best path to take to get there when it gains this information, it is likely that it may avoid the landmark node and be routed directly to its target.

This is because the packet will gather more information as it gets closer to its goal. To reiterate, the process of changing the connection status is analogous to the protocol that is used for FSR. Updates to the topology are distributed among the nodes and the neighbours that are immediately next to them. An extra distance vector is included in each and every update packet, and the computation for this vector is determined by the total number of landmarks. As a result of this approach, the routing entries that had sequence numbers that were lower are being upgraded to ones that have sequence numbers that are higher.

5.17 APPROXIMATE DISTANCE RDMAR (MICRO-DISCOVERY AD HOC ROUTING)

Because it comprises the tried-and-true methods of route discovery and route maintenance, the RDMAR protocol is analogous to other reactive protocols that are currently in use. This is because the RDMAR protocol integrates these operations. The maximum number of hops that a route discovery broadcast message is permitted to make is, however, controlled by the distance that separates the origin and the destination. This maximum number is considered to be the maximum number of hops that a message can make. Each node maintains a routing table that includes information such as the neighbour of the next hop for each known destination, the estimated relative distance between all known source and destination nodes, the time the current entry was made, the timeout field at which the route will no longer be active, and a flag that indicates whether or not the route still exists.

All of this information is stored in the routing table. Each node is responsible for maintaining the information included in the routing table. In addition to this, we maintain a record of the estimated relative distance that separates each source node from the node that corresponds to it as the destination node. The source nodes are the ones that are responsible for measuring the estimated distances. In order to do so, they take into consideration the most recent distance that was measured between each pair of nodes, the most recent time that the route was updated, and the estimated speed of the node that is the destination.

In addition, the upkeep of two more data structures is the responsibility of each individual node. The data retransmission buffer and the route request are both included in this category. The former is used to store data that is being relayed in a queue until an explicit acknowledgement is received, whilst the latter is used to store all of the necessary information that is linked to the most recent route discovery. Both of these functions function until an explicit acknowledgement is received.

The process of discovering and maintaining routes consists of two phases: either broadcasting route request packets or waiting for a route reply packet from the destination. Both of these processes are necessary for the process to be completed. Moreover, in order to determine whether or not there are bidirectional linkages, every node will occasionally send a packet over the connection that it has most recently received a packet. This is done in order to test for the presence of such links.

5.18 SLURP, SHORT FOR SCALABLE LOCATION UPDATE-BASED ROUTING PROTOCOL

The major goal of the SLURP is to build an architecture that is flexible enough to accommodate networks of varied sizes. In a way that is decentralised, a system that is known as a location update mechanism is responsible for maintaining the most recent version of the location information of the nodes. The mechanism in question is responsible for mapping node Identifiers for diverse geographical subregions of the network. Each node within a region is accountable for ensuring that the location data of all other nodes in that region is maintained as up to date as feasible. Initially, the sender will run queries on nodes that are situated in the same geographic subregion as the destination.

The purpose of these inquiries is to build an approximate estimate of the location of the destination. Following that, the data packets are sent to a system that is utilised for the typical implementation of geographic routing. Due to the fact that the cost of providing a position update is directly proportional to the velocity of a node, a greater number of messages to

update the location of a location are transmitted when the node in question is moving at a quick rate.

With N representing the entire number of nodes in the network and v representing the usual speed of a node, theoretical research indicates that the routing overhead increases at a rate of O(N3/2), where N is the total number of nodes in the network. Because the overhead of routing packets rises in a linear way with the existing number of nodes and N3/2, it is crucial that you keep this in mind as you attempt to extend your network. This is because the overhead increases in a linear fashion.

CHAPTER 6

AD HOC NETWORKING

6.1 INTRODUCTION

The fact that people who use computer systems are beginning to place a greater emphasis on their freedom of mobility is a development that is quite positive. As a result of advancements in technology, wireless communication devices and computers are able to be made more powerful while simultaneously dropping in size and cost. This is a potential benefit of technological advancements. Users will have the option to take advantage of more freedom, the capability to maintain connectivity even while travelling over a big region, and the possibility to share information with one another. There are a number of regions that are now in the process of establishing base stations and access points in their respective territories in order to give the essential support for mobile computing.

When mobile customers make use of this infrastructure, they are able to keep their connection intact regardless of where they are, whether they are at their place of home, at their place of job, or when they are travelling. In a number of different scenarios, it is possible that one could have the wish to have mobile communication; nevertheless, there are not always solutions available for this kind of mobility assistance. Because of the high cost that is necessary, the low demand that is expected, and the poor performance, there is a possibility that access points may not be installed. This might take place at outdoor conferences or during times of crisis, such as when a natural disaster occurs or when military manoeuvres are carried out on land controlled by an adversary.

Both of these scenarios raise the possibility of this happening. This might also take place during times of conflict, which is another possible scenario about it. In circumstances when there is no current support structure, users of mobile devices are forced to establish an ad hoc network in order to connect with one another since there is no preexisting support structure.

More attention is going to be paid throughout the entirety of this chapter to the topic of mobile ad hoc networking, which will be investigated in greater depth. Following the explanation of their qualities, a consideration of the complexity and design restrictions connected with them, and the presentation of our findings regarding them, we subsequently identify the current routing algorithms as belonging to this group.

6.2 ADHOC MOBILE NETWORKS

The mobile ad hoc network, sometimes referred to as a MANET, is a type of wireless network that is composed of mobile computer devices, also referred to as nodes, that connect with one another through the use of wireless transmission. The term "mobile mesh network" and "wireless ad hoc network" are two more terms that may be used to refer to this form of network. There are a few other names for this particular architecture of a network, including mobile ad hoc networks and mobile mesh networks. Unlike cellular networks and wireless local area networks, this kind of network does not need to have a centralised management system or a base station.

It also does not need access points like those found in wireless local area networks. Access points are not necessary for a wireless local area network, which is another similarity. This particular type of network, on the other hand, is decentralised and is reliant solely on the users themselves. Instead, it is able to perform the duties of Due to the fact that the nodes are free to travel in any direction and organise themselves in any way that they deem appropriate, the wireless architecture of the network is prone to quick and unexpected modifications in configuration. Depending on the circumstances, a network of this kind may operate independently or it may be connected to the Internet, which is the more extensive network. Whatever the case may be, it has the capability of functioning.

Mobile ad hoc networks, in contrast to more conventional mobile wireless networks, do not require the presence of a central coordinator and instead function in a manner that is self-organized since they are able to function independently. In contrast to this, mobile wireless

networks are currently in use. Wireless connections allow mobile nodes that are situated in close proximity to one another and within the radio range of one another to communicate directly with one another. This is possible because the nodes are able to interact with one another.

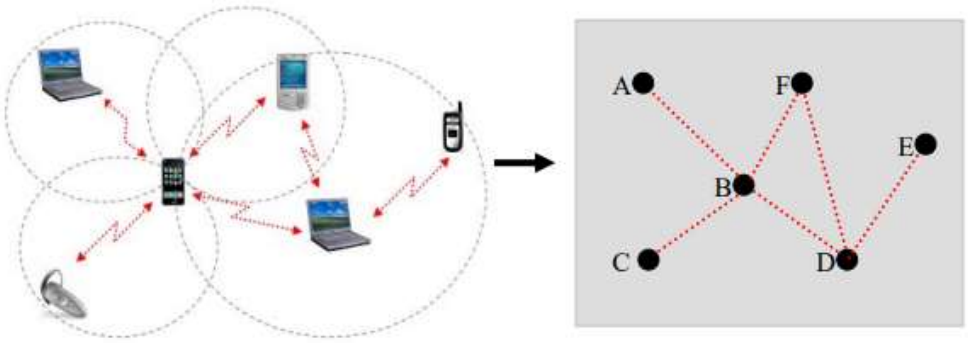

Fig.: 6.1 A Typical Mobile Ad Hoc Network

Source: A Novel Approach of Secure Routing Protocol for Mobile Ad Hoc Network data collection and processing through by Imran Hossain Faruk (2013)

Wireless medium: In an ad hoc network, the nodes interact with one another through wireless techniques, and they share the same medium (such as radio, infrared, or other forms of communication). Stations are unable to receive network frames if they are located outside of these constraints since the wireless medium does not have any absolute limitations or boundaries that can be plainly observed. This means that the channel is not protected against signals that are coming from the outside, which makes it a great deal less reliable than media that is linked.

Autonomous and infrastructure less: The MANET system does not depend on any preexisting infrastructure, nor does it need administration to be conducted in a centralized place. Each node is responsible for its own data creation, acts as its own independent router,

and carries out its responsibilities in a distributed peer-to-peer manner. It is necessary for the administration of the network to be distributed over a number of nodes, which makes the process of problem diagnosis and management much more difficult.

Dynamic and changing network topology: Because nodes in mobile ad hoc networks are at liberty to relocate to any location they choose, the topology of the network, which is often multi-hop, is prone to alterations that are both frequent and unexpected. This is because of the free movement of nodes in the network. Because of this, there is a possibility that routes will be altered, that the network will divide often, and that packets may be lost.

Limited availability of resources: Because of the restricted power supply given by the batteries carried by each mobile node, there is a restriction placed on the amount of processing power that can be used. Because of this, there is a limit imposed on the variety of applications and services that may be provided by each node. Because each node in a MANET act as both an end system and a router at the same time, a higher amount of energy is required for the transmission of data packets. Because of this, the difficulty of the situation continues to increase.

6.3 MANET APPLICATIONS

Because of the ease with which they may be deployed and the reduced financial investment that is necessary, ad hoc wireless networks have the potential to find use in a wide range of contexts. The following are examples of some of them:

- Uses in the military, such as allowing communication among members of a squad for the purpose of conducting tactical operations in places where it would be difficult (or impossible) to build up a permanent wireless network due to the presence of hostile troops or the existence of unfavorable geography in those regions. When it is not possible to establish a permanent wireless network infrastructure, this software comes in quite helpful.

- Systems designed for use in times of emergency, such as those that improve the ability of first responders to communicate with one another in the event of a catastrophe.
- Two applications of this technology that are now being utilized in the business world are community networking and interaction between participants and instructors.
- Computing that is both collaborative and dispersed.
- Wireless networks for sending messages and wireless networks for sensors

6.4 MOBILE AD HOC NETWORK ROUTING APPROACHES

Several different routing protocols for mobile ad hoc networks have been developed ever since the introduction of DARPA packet radio networks in the early 2000s. They may be broken down into three primary categories: on-demand routing protocols, reactive routing protocols, and hybrid routing techniques. Each of these categories is a basis for further analysis. The most popular type of routing protocol is called on-demand routing.

Driven or Proactive Protocols: An attempt is made by proactive routing systems to maintain the consistency and accuracy of the routing information between every pair of nodes in the network. This is accomplished by propagating route modifications at intervals that have been established. All of this is made possible through the utilisation of proactive routing. For this reason, the protocols are sometimes referred to as data-driven protocols.

This is because they are commonly retained in. This is due to the fact that the information that is generated by the protocols is normally kept in. In the realm of proactive protocols, some examples include the utilisation of the Destination-Sequenced Distance Vector (DSDV) method for routing, the Clustered Gateway Switch Routing (CGSR) algorithm, the Wireless Routing Protocol (WRP) algorithm, and the Optimised Link State Routing (OLSR) algorithm. Nevertheless, this list does not contain everything.

On-demand or Reactive Protocols: In contrast to the more conventional approach of driven routing, reactive or on-demand routing functions as an alternate option. When these factors

are taken into consideration, the conventional approach of the Internet is not followed. The difference between driven protocols and reactive protocols is that the latter do not construct a path to a destination until it is absolutely required to do so.

During the phase of the network's discovery process that is referred to as "discovery," the source node is often the one that initiates this request. Once a route has been established, the node will continue to keep it in place until one of the following conditions is satisfied: the destination can no longer be reached; the route is no longer being utilised; or the route has completed its journey and is no longer legitimate. Common reactive routing systems include the Ad hoc On Demand Distance Vector (AODV) routing system, the Associativity Based Routing (ABR) algorithm, and the Temporally Ordered Routing Algorithm (TORA) algorithm. All of these algorithms are instances of reactive routing systems.

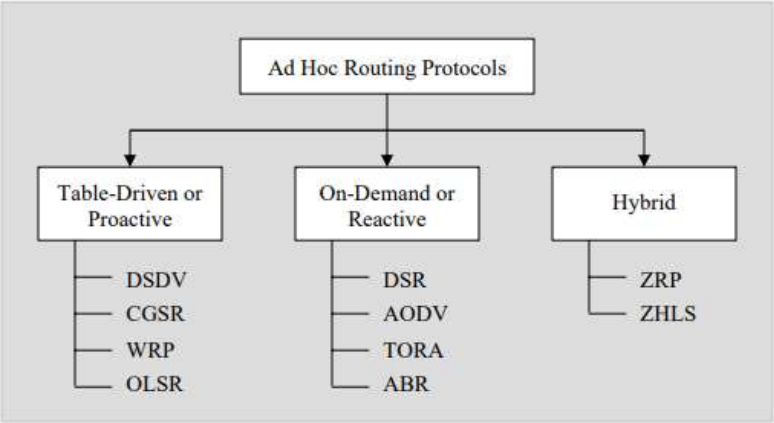

Fig.: 6.2 Classifications of Ad Hoc Routing Protocols

Source: A secure zone-based routing protocol for mobile ad hoc networks data collection and processing through by Niroj Kumar Pani (2009)

Hybrid Routing Protocols: In a constrained network environment, protocols that are either entirely proactive or purely reactive may function well. However, since ad hoc networks are used for such a broad variety of applications that span a wide range of operating circumstances

and network configurations, it may be difficult for a single protocol to function exploring such circumstances to a great depth. Techniques like as reactive routing, for instance, operate very effectively in networks where the call-to-mobility ratio is quite low. On the other hand, proactive routing methods are perfectly suited to such a ratio, which makes them an excellent choice for networks with such a ratio. If you utilize it on portions of ad hoc networks that are located between two specific points, it will the middle of the two extremes, the performance of either class of protocols suffers.

6.5 OLSR PROTOCOL (OPTIMIZED LINK STATE ROUTING)

The standard link state routing format has been used as the basis for the development of a new protocol that is known as the Optimised Link State Routing (OLSR). This new protocol was developed with the intention of achieving greater success in ad hoc networks than the traditional link state routing would have been able to achieve. The utilisation of multipoint relays (MPRs), which helps to decrease the overhead of network floods and the amount of space required for connection status changes, is the primary characteristic that may be used to differentiate OLSR from other similar systems.

Because of this, it is one of the aspects of OLSR that is most readily apparent. Every node computes its own MPRs by taking into account the neighbours to which it is linked and those neighbours are connected to the internet. If a node broadcasts a message, all of its two-hop neighbours will be able to receive it because of the retransmission that the MPR set offers. This is because of the way that the MPR set is created. This happens as a result of the MPR set being configured to retransmit messages in the same sequence in which they were initially broadcast. The selection of the MPR set in such a fashion is the cause of this particular occurrence.

Figure 6.3 illustrates that the MPR set for a particular node is the set of neighbours that contains the node's two-hop neighbourhood. This collection of neighbours is known as the MPR set. It is possible to view this definition in its entirety in the image. The collection of

neighbours that was discussed before is what makes up the MPR set set. It is possible for nodes to acquire knowledge about their set of two-hop neighbours, which are the nodes that are immediately next to them, through the exchange of Hello messages on a regular foundation. Every node in the network will send out a "Hello" message at predetermined intervals. This message will include a list of the other nodes that are located in close proximity to it. A component of the attribute that is connected with each neighbour is the directionality of the connection to that neighbour. This is not the only component of the property.

One of the many characteristics that are connected to each neighbour is this particular quality. If it can be demonstrated that the connection between a node and its neighbours may function in either direction, then the node in question has the potential to be regarded as symmetric. A node is deemed to be asymmetric if it received a Hello from a neighbouring node, but the connection was not confirmed to flow in both directions.

This is the opposite of what is meant by the term "symmetric." That the link was only going in one direction would be shown by the presence of the Hello in this scenario. When a node eventually learns everything there is to know about its two-hop neighbour set at a certain point in time, this is the moment when it realises that it has done so since it has gotten the Hello message from all of its neighbours once it has finally learned everything there is to know about its neighbours. In addition, if it adds its own address in the "Hello" message, it is aware that the relationship with that neighbour is a link that goes in both directions (a street that goes in both directions). As a consequence of this, it is feasible to modify the state of that neighbour in such a way that it is symmetrical.

According to the approach, the following is one way that the MPRs for the set may be calculated. Every node has an MPR set, and these sets are initially devoid of data. The set of neighbors with whom there is a bidirectional connection after one hop is marked by the letter N, and the neighbors with which there is bidirectional connectivity after two hops are represented by the letter N2. The nodes in the MPR set that are picked first are those in N that

are the only neighbors of a node in N2; this is because these nodes have the greatest likelihood of being selected and are thus the ones to be chosen first.

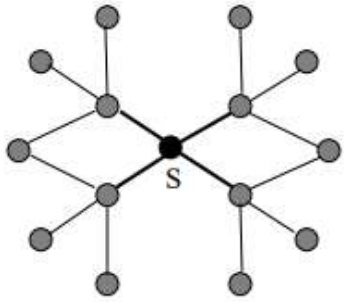

Fig.: 6.3 Multipoint Relays

Source: A secure zone-based routing protocol for mobile ad hoc networks data collection and processing through by Niroj Kumar Pani (2009)

After that, the degree of each individual node in N that is not part of the MPR set is calculated. The degree may be thought of as the number of nodes in N2 that are in no way connected to any of the nodes that make up the MPR set. In conclusion, the MPR set only contains the node in N that has the highest degree of all of the nodes in that set. When each of the nodes in N2 has been properly accounted for, the operation will proceed to its conclusion.

6.6 ROUTING USING AN AD HOC ON DEMAND DISTANCE VECTOR (AODV)

The Ad Hoc On-Demand Distance Vector (AODV) routing protocol is constructed with the DSDV algorithm serving as its basic building element. AODV is better to DSDV since it generates routes depending on demand rather than predefined courses, which typically results in fewer broadcasts being completed. This makes AODV a more desirable alternative. Utilising predetermined paths, DSDV is able to generate its routes. On the other hand, the DSDV algorithm maintains a comprehensive inventory of all the various travel paths that are

available to be taken. The label indicates that AODV is an elaboration on DSDV, which is the underlying concept.

For further information about DSDV, please refer to the explanation provided by AODV. The people who created AODV refer to it as a pure on-demand route acquisition system. This is due to the fact that it does not need nodes to maintain routing information or participate in routing exchanges until they are on a path that has been assigned for them. This is due to the fact that AODV does not necessitate the storage of routing information by nodes. One reason for this is because it has the potential to be abused by nodes that are not currently participating in the route selection process. This is the reason why this is the case. In the event that a source node desires to send a message to another node but is unable to ascertain an adequate path to that destination, the source node will begin the process of path discovery in order to locate the other node.

In order to ensure that the message will be sent by the node of origin, this operation is carried out. Additionally, in order to achieve this, it sends out a packet that is known as a route request, or RREQ, into the network. It then requests its neighbours to pass it along until it reaches either the destination that it was meant for or an intermediary node that is familiar with the path. It has been determined that there is a route to the target that offers "fresh enough" conditions. contains a representation of the procedure that is followed in order to transmit the broadcast RREQs over the network.

In order to ensure that all routes are free of loops and contain the most recent information on routes, AODV employs a variety of different ways, one of which is the use of destination sequence numbers. The use of destination sequence numbers is another method that may be undertaken. Additionally, it is the responsibility of each individual node to ensure that its own sequence number and a distinct broadcast identity are kept up to date.

It is possible to generate a one-of-a-kind identifier for the RREQ by using either the broadcast ID of the RREQ itself or the IP address of the node that was responsible for delivering it. Both

of these options are possibilities. This ID advances by one at the beginning of each newly begun RREQ that is launched by the node. This is done in order to ensure maximum efficiency. The RREQ includes the sequence number of the source node, the broadcast ID, and the sequence number of the destination that is the most recent. It also includes the broadcast ID. This is due to the fact that the node that is responsible for transmitting the data packets incorporates the sequence number into those packets for transmission.

This particular sequence number is going to be utilised by the RREQ in order to generate outcomes. They make a note of the MAC address of the node along the path from which they acquire the first broadcast copy of the packet when intermediate nodes relay RREQ packets. This is done in order to ensure that the packets are transmitted correctly. In this way, the packets are more likely to be transmitted in the proper manner. As a consequence of this, a back channel is created, which allows the data to go through another channel.

Therefore, in order for intermediate nodes to be able to respond to the RREQ, it is required for them to have a route to the destination that has a sequence number that is either greater than or equal to the one that is provided in the RREQ. This is because the RREQ determines the sequence number of the route. It is possible that the packets in question will be destroyed in the case that it is determined that further copies of the identical RREQ were received at a later period.

The final node or the intermediary node will transmit a route reply (RREP) packet back to its original neighbour when the RREQ reaches its ultimate destination or an intermediary node with an up-to-date route. This will occur when the RREQ reaches its ultimate destination. This will take place when the RREQ arrives at its ultimate destination or at an intermediary node that has a route that is complete and accurate. Because of this, it is expected that the intended outcome will be accomplished. to ensure that the route is maintained up to date. This is done in order to ensure that the neighbour always has access to the most up-to-date information on the route possible at all times.

Along the path that the RREP packet travels back along, nodes add forward route entries to their route that refer to the node from which the RREP packet originated. These entries are added to the route of the RREP packet. The nodes that are located along the path that the RREP packet goes back along are the ones that insert these forward route entries. The occurrence of this occurs when the RREP packet is transmitted along the reverse way in order to arrive at its intended destination. Indicating the forward path that is now being utilised is the presence of these items, which are a component of the forward route.

The database has a route timer that is associated with each route entry. If the route timer determines that the entry has not been utilised within the allotted amount of time, the route timer will cause the record to be removed from the database. In the event that an entry is not utilised within the specified length of time, it will be deleted from the database. Only the use of symmetric connections inside the network is compatible with AODV. This is the only configuration that is compatible. The RREP packet is always transmitted along the route that was generated by the RREQ packet, which is the reason why this is the case. This is the reason why this is the case.

6.7 ZONE ROUTING PROTOCOL (ZRP)

A completely proactive or a fully reactive strategy might be taken when developing a routing protocol for a MANET, as was mentioned earlier. Both of these approaches are viable options. These two methods, on the other hand, each have their own individual set of constraints that must be considered. Given that the Zone Routing Protocol (ZRP) seeks to bypass these constraints by incorporating the most favourable features of proactive and reactive techniques, it is plausible that it may be classified as a hybrid proactive/reactive routing protocol. This is because ZRP strives to circumvent these restrictions.

A discussion of this hybrid method, which integrates the most advantageous parts of both proactive and reactive techniques, may be found in. When it comes to a MANET, it is acceptable to presume that the majority of the communication that takes place takes place

between nodes that are situated in close proximity to one another in space. Because of this, ZRP restricts the range of proactive measures to a zone that is centred on every node, and it employs a reactive approach in the regions that are outside of the zone. This is because of the fact that ZRP is a zone-based protocol.

In the event that a node is in possession of a data packet that is destined for a certain destination, the node will perform a check in order to determine whether or not the destination is situated inside its zone. When it is determined that the packet is already within the zone, a proactive path is selected for it to travel in order to avoid any surprises. In the event that the destination is discovered to be located outside of the zone, reactive routing tactics will be implemented.

There is just one object that constitutes a node's zone, which is also frequently referred to as its routing zone. This zone is comprised of the region that constitutes the immediate neighbourhood of that node. For the purpose of establishing the size of a zone, normal geographical units are not utilised; rather, a radius of length is utilised, and the number of hops to the zone's perimeter is utilised to signify the size of the zone. It's possible that this will come as a shock to you.

This may come as a bit of a shock to some individuals. It is likely that at first glance, this will appear to be contradictory; yet, it turns out that this is actually the way that it operates. There is a possibility that every node might be located inside a selection of zones that overlap one another, and the dimensions of those zones could be different from one another.

An illustration of a routing zone is presented in Figure 6.4. This illustration illustrates that further nodes A-I are contained inside the routing zone of node S, however node K is not included in this routeing zone. An example of the concept of a routing zone is provided here for purposes of demonstration. In the graphical representations, the radius is depicted as a circle with the node of interest serving as the circle's centre.

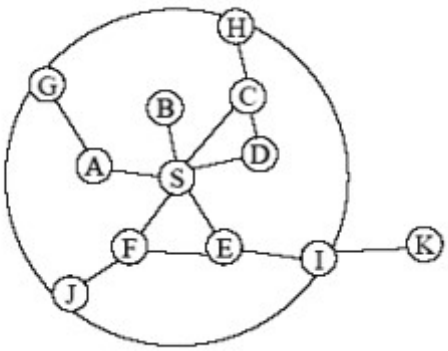

Fig.: 6.4 Node S's routing zone, having a zone radius of 2

Source: A secure zone-based routing protocol for mobile ad hoc networks data collection and processing through by Niroj Kumar Pani (2009)

When it comes to network security, MANET poses its own distinct set of challenges due to the fact that it is a wireless mobile ad hoc network. The information and physical security concerns that are associated with mobile ad hoc networks are significantly higher than those associated with cable networks and wireless networks that are backed by infrastructure, respectively. The reason for this is because mobile ad hoc networks have certain characteristics that are not shared by other networks.

In the next chapter, we will discuss a variety of distinct security demands (objectives) for wireless ad hoc networks, as well as the several types of threats that might potentially damage such networks. At the same time as we study the new opportunities and challenges that this new networking environment brings, we also investigate the many methods in which communication might be protected within this new ecosystem.

6.8 CONCERNS AND DIFFICULTIES WITH PROVIDING SECURITY

Because of factors such as the shared nature of the radio channel, the absence of a centralized authority or set of rules governing how nodes should associate with one another, and the

scarcity of available resources, ad hoc routing presents a unique set of challenges when it comes to the design of a robust security protocol. Ad hoc routing also makes it difficult to find resources to use in the design process. In the following paragraphs, you will find a condensed explanation of the reasons why it is so difficult to apply security measures in an ad hoc wireless network.

Shared radio channel: In wired networks, each pair of end users may be given their own dedicated transmission line. However, in ad hoc networks, the radio channel that is used for communication is broadcast and shared by all nodes. In wired networks, each pair of end users may be assigned their own unique transmission line. On the other hand, wired networks are able to provide a transmission line that is solely dedicated to the use of a single customer or customer pair. The data that is transferred from one node to all of the other nodes that are in direct line of sight will be received by those nodes. Because of this, it is simple for a rogue node to steal information as it travels across the network as it is being sent.

Insecure operational environment: It is possible that the operating environment in which MANETs are often utilized, such as a battlefield, could not necessarily be a secure one. In such a setting, it is possible for nodes to migrate into and out of hostile and unsecure enemy territory, making them very susceptible to assaults on their security.

Lack of association rules: Since nodes may In a MANET network, nodes are able to leave or join the network at any time; thus, in the absence of a good authentication method utilized for associating nodes with the network, attackers are able to simply join the network and begin their assaults. This is because individual nodes in the network are free to come and go as they like at any given moment.

Limited availability of resources: Within an ad hoc network, resources like as bandwidth, battery power, and compute power are in short supply. As a result, it is challenging to implement intricate security procedures that are based on cryptography in these kinds of networks.

6.9 SECURITY ATTACKS ON AD HOC ROUTING PROTOCOLS

Due to the complexity and uniqueness of the MANET design, multiple access networks (MANETs) are far more vulnerable to security threats than their cable counterparts' counterparts. The distinction between passive and active attacks on ad hoc wireless networks is dependent on whether or not the assaults interfere with the regular operation of the network. Attacks on ad hoc wireless networks may be separated into two categories: passive and active.

An example of a passive attack is one in which the attacker does not interfere with the normal operation of the network. Instead, the passive attack consists of the attacker just monitoring the data that is transmitted inside the network without making any modifications to it. In this particular circumstance, the need of maintaining confidentiality has been violated. As a result of the fact that a passive assault does not disrupt the operation of the network itself, it may be exceedingly challenging to determine when such an attack is taking place. It is possible that one of the solutions to the problem is to involve the utilisation of advanced encryption technologies in order to encrypt the data that is being transported. Because of this, it will be impossible for an adversary to extract any information that is pertinent from the data that has been overheard.

Active attacks are assaults that actively seek to change or destroy the data that is being delivered across a network, with the ultimate objective of stopping the network from functioning correctly. Active attacks are a type of attack that is considered to be an active attack. There are two possible origins of active assaults: the inside and the outside. External attacks are those that originate from nodes that are not a part of the network and are referred to as "external." The nodes within the network that have been compromised are the source of attacks that originate from within the network.

When taking into mind the fact that the adversary is already ingrained into the system, internal assaults pose a greater threat than exterior attacks do. Finding evidence of an assault that is being carried out from within is a much more challenging endeavour. Impersonation, also

known as masquerade or spoofing, modification, fabrication, and duplication are all potential methods that might be utilised in an active assault that is initiated by a compromised internal node or an external alert. Some of these methods include duplication, modification, and fabrication.

Active attacks can be initiated by either an advisory from the outside or by a compromised node from the inside. Both of these methods are possible. At each given layer of the network protocol stack, it is feasible to launch either a passive or an aggressive assault. Both can be carried out simultaneously. The other thing is that this is solely concerned with attacks on the network layer, sometimes known as routing attacks.

Attacks that leak information, impersonation attacks (such as masquerading or spoofing), modification attacks, fabrication attacks, and replay attacks are the five unique categories that may be used to classify routing assaults. Each of these categories is defined by the precise method that the attacker employs. The disclosure of confidential information is an example of a passive assault, whereas the other ways are instances of approaches that are considered to be aggressive attacks.

6.10 ATTACK ON INFORMATION DISCLOSURE

In this scenario, a hacked node in the network may leak secret information to other nodes in the network that are not allowed to receive it. This kind of information could include details on the structure of the network, the geographic locations of individual nodes, or the most efficient paths to reach illegal nodes inside the network. Attacks that fall into this category include those that disclose a location and those that analyze traffic.

6.10.1 Attacks that impersonate others

The goal of an attack known as impersonation is for the attacker to get access to confidential information by pretending to be a valid node in the network. Either to make use of network resources that would otherwise be unavailable or to disrupt the usual operation of the network

by introducing false routing information are both plausible motives for doing so. The latter would include making use of network resources that would otherwise be unavailable. An impersonation attack is referred to as a denial-of-service attack.

There are a number distinct approaches to use while attempting to impersonate another individual. It is possible for an attacker to correctly guess the credentials of the lawful node that has been identified as the target node. The attacker may even listen in on a conversation that is taking place between the two parties and find out the authentication credentials of the target node using this information. The following are some examples of assaults involving impersonation:

Man-in-the-Middle Attack: In this kind of attack, a malicious node will impersonate the sender with regard to the receiver, and then the receiver will impersonate the sender with respect to the receiver. Neither party will be aware that they are being attacked, and the attacker will be able to read or change the messages that are being sent between the two parties.

Sybil Attack: During a Sybil assault, the attacker will act as if they had more than one identity. A malicious node might pretend to be part of a bigger network of nodes by impersonating other nodes or just claiming bogus identities. This could be done by claiming a fictitious identity or by impersonating other nodes. The findings obtained from accomplished in one of two ways. There are three different types of Sybil attacks: those that include direct or indirect communication, manufactured or stolen identities, and simultaneous the activity in question.

Direct communication occurs when Sybil nodes interact with genuine nodes, whereas indirect communication occurs when messages designed for Sybil nodes are passed through malevolent nodes. Sybil nodes interact directly with real nodes. When Sybil nodes communicate to actual ones, this is an example of direct communication.

An attacker has the option of either creating a new identity or just stealing the previous one, depending on whether the impersonated node was destroyed or temporarily disabled. All of

the Sybil identities have the potential to take part in the network at the same time, or they might just be rotated through.

6.10.2 Modification-based attacks

This attack causes disruption to the operation of routing by having the attacker make unauthorized changes to the content of the messages being sent. Redirecting traffic by altering the route sequence number and redirection with a changed hop count are two examples of the types of attacks that fall under this category. The following is a list of some of the attacks that include the manipulation of packets:

Misrouting Attack: During a misrouting attack, an illegitimate node will transmit the routing message in the wrong direction and will deliver the the incorrect location for a data packet's destination. This vulnerability may be exploited in one of two different ways: either by modifying the destination address of the data packets or by sending them to the incorrect hop in the network.

Byzantine attack: During an attack of this kind, one or more compromised intermediary nodes work together to carry out malicious operations such as the creation of routing loops and the transmission of packets over inefficient pathways. pathways, and deleting packets deliberately. Byzantine failures are difficult to identify because, during these types of assaults, the network may seem to be functioning correctly.

6.10.3 Security Mechanisms and Solutions

After going through the many different forms of attacks that might be launched against ad hoc routing, we will now investigate the many different strategies that are used to defend against these assaults. There are two distinct categories of security measures, namely preventative and detective. The use of message encryption methods is normal for preventative measures, while the use of digital signatures and cryptographic hash functions is typical for investigative mechanisms.

6.10.4 Message Encryption

The act of encoding a message or sending it across a transmission medium When a communication is encrypted, it is transformed into a disguised form that cannot be read by anybody who is not authorised to do so. However, the message may be decoded and read in its original form by the person who it is meant for. Encryption is a process that involves both the science and the art of converting a message into a disguised form. Through the use of encryption, sensitive information may be protected from being read by individuals who are not authorised to do so.

When it comes to cryptography, the form of communication that has not been altered is referred to as plaintext, whereas the version of the message that has been encrypted is referred to as ciphertext. Plaintext is the form of communication that has not been altered. One view of encryption is that the plaintext may be transformed into the ciphertext by the execution of specific programmes or processes. Other interpretations of encryption include the following. To decrypt a message, you must first conduct actions in the reverse sequence to how they were performed during encryption.

The usage of a key, which is a discrete piece of data, is required in order to achieve the process of encrypting and decrypting information through the application of cryptographic methods. There is a requirement for keys for both procedures. Using keys is required for both of these actions to be completed. The symmetric key and the asymmetric key are the two fundamental types of encryption technology. Both of these keys are recognised by their respective names.

6.10.5 Digital signature and Hashing

Encrypting a communication is the only way to ensure that it will remain private while it is being sent from one party to another. Message integrity, authentication, and non-repudiation are some of the additional aspects of security that may be attained by the use of a technique known as digital signature. Other aspects of security that can be attained include non-

repudiation. The sender then applies a digital signature to the message by using a signature algorithm as well as the sender's private key to complete the process. The message and the signature will both be sent to the recipient's inbox simultaneously.

The receiver conducts the verifying algorithm on the pair that consists of the message and the signature once it has received both the message and the signature. The verification procedure requires a verification key, which is a public key that was given by the signer in order for it to be able to verify the document. The public key was supplied by the signer. In the case that the result during verification is found to be incorrect, the message won't be acknowledged; rather, it will be denied. Hashing may be part of the process of producing a digital signature in some circumstances, such as when the message that has to be signed is particularly long.

Before the message is signed using this approach, it is hashed utilizing a process that may be referred to as a cryptographic hash function or a one-way hash function, depending on the context. It is a that creates a compressed representation of the message in the form of a hash value, which is also known as a message digest. This approach is also known as message compression. This number, which is unique to the message, is often quite a bit less than the message itself and is only accessible via the message. Even when the same hashing method is used, the result of the message's hash will be different if any of its components are changed. This is true even though the algorithm remains the same.

Neither a pure proactive nor a pure reactive approach can provide a comprehensive answer to the problem of providing secure ad hoc routing that is also capable of functioning well over a wide range of operational circumstances and configurations of the network. Both strategies have been deemed inadequate to address the issue. As a result, it is of the utmost importance to have a solution for safe routing that is not only all-encompassing but also efficient, adaptive, and effective, and that works well with the many applications that may be run on ad hoc networks. This chapter will focus on the Secure Zone Routing Protocol (SZRP), which is currently the solution that is being advised to be implemented.

Its objective is to provide a solution to the issue that has been recognized. The architecture of the proposed protocol has been broken down and analyzed in great detail, and its robustness in a broad range of networking contexts as well as in the face of a wide variety of possible security threats has been reviewed.

6.10.6 Certification Process

The Secure Zone Routing Protocol, also known as SZRP, necessitates the existence of reliable certification servers inside the network, which are referred to as certification authority (CAs). All valid CNs have access to the public keys of the CAs, therefore it may be presumed that they are trustworthy. The CA and each CN have a preexisting connection that allows for the generation and exchange of keys a priori.

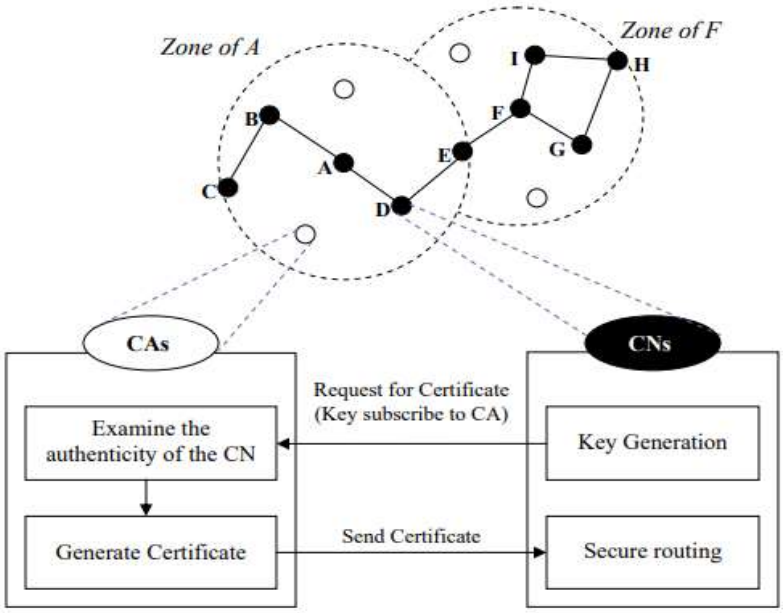

Fig.: 6.5 Certification Process in SZRP

Source: A secure zone-based routing protocol for mobile ad hoc networks data collection and processing through by Niroj Kumar Pani (2009)

This may take place outside of the band. Each node, prior to joining the ad hoc network, makes a certificate request to the CA that is geographically closest to it. After successfully validating their identity to the CA in a secure manner, each node is issued precisely one certificate. Figure 6.5 illustrates the concept well. There are several possible methods for providing secure authentication to the certificate server; thus, it is up to the developers to decide.

6.10.7 Secure Inter-Zone routing

SIERP is used in order to accomplish secure interzone routing. The on-demand secure route discovery phase is the first step in the interzone routing process. During this phase, the source locates the path that leads to the interzone destination of their choosing. The data packet is subsequently sent from the source via this path. When it comes to our scenario, if A wishes to send a packet to Z, A will check its SIARP routing to see whether there is a legitimate route to Z. A is unable to discover the path since Z is not located inside its zone of influence.

In this particular scenario, A kicks off the process of discovering a secure path to Z. Following the completion of the secure route discovery procedure, A is provided with the genuine path to Z, at which point A sends the data packet via this route to Z. SIARP is responsible for monitoring the local connectivity information, and in addition to performing secure route discovery, SIERP also provides route management services based on this information. There is discussion over the upkeep of the route.

6.10.8 Network Scenario

For the purpose of the investigation, both of these field configurations were replicated. The first one consisted of ten nodes dispersed across a terrain of 700 metres by 700 metres, while the second one consisted of twenty nodes dispersed across a terrain measuring 1200 metres by 1200 metres. Through our investigation, we were able to ascertain that the node has a transmission range of 250 metres. During the initial phase of the construction of the nodes, the positions of each node were selected at random as part of the process.

Utilising the random waypoint mobility model allowed us to duplicate the motions of nodes, which was a significant accomplishment. In this approach, every node moves to a location at random at a pace that has been determined in advance from the beginning. When it finally arrives at its destination, it waits for a period of time that may be altered to suit your needs before moving on to yet another location at random.

Throughout the entirety of our simulations, we ensured that the speeds of the nodes remained at 1, 5, and 10 metres per second, respectively. The duration of the pause was always thirty seconds. Within the implementation, communication between CBRs was carried out through the use of UDP, which made use of the 802.11 MAC layer.

When we performed the simulation, we simulated five CBR sessions using random source and destination pairings. This was done each time we completed the simulation. At a pace of four data packets per second, each session generated a total of 500 data packets, each of which was composed of 512 bytes and was produced at a different rate. There was a total of one minute and fifty seconds of simulated time that was spent running each and every simulation. presents two different representations of the simulation scenario, one of which has ten nodes and the other of which contains twenty nodes.

6.10.9 Measures of performance

In order to determine how well the Secure Zone Routing Protocol (SZRP) performs, the ZRP and SZRP routing protocols were both tested using the same mobility patterns and traffic situations and then compared to one another. We just utilized the most fundamental version of ZRP, which did not contain any optimizations.

Because of this, it is possible to compare the outcomes in a consistent manner. This particular implementation of ZRP was a contribution made by Robin Poss back in. When comparing the performance of ZRP and SZRP, we looked at two different categories of indicators. The first category of metrics assesses both protocols assuming that there is no malicious activity taking

place on the network. It is taken as a given in this class that all of the nodes get along with one another and are willing to lend a helping hand when needed. The efficiency of their techniques was evaluated utilizing the second set of measurements in a hostile environment where there were dishonest nodes present in the network. The results of this evaluation were positive.

6.11 A NON-ADVERSARIAL ENVIRONMENT'S METRICS

In order to do an apples-to-apples comparison between the proposed protocol and ZRP while operating in a trusted environment in which all of the nodes in the network are presumed to be good, we tested four performance indicators. The following is a discussion of them:

Average packet delivery fraction: This is the percentage of the data packets that were created by CBR sources and were successfully delivered to the destination. This statistic is essential since it assesses the capability of the protocol to find routes.

Average routing load in terms of packets: This measure is similar to the one described above; however, in this case, the calculation involves determining the ratio of control packet overhead to data packet overhead.

Average route acquisition latency: How much time it takes, on average, for a source to transmit a secure route discovery packet to a destination and get the first related route reply from the destination. This time is measured in milliseconds. In this calculation, we include in all of the time that was wasted during the route discovery phase and the route reply phase owing to validating and updating signatures. The processing of the packets according to the standard is also provided. In the event that a route request ran out of time and had to be resent, the time it took to send the request the first time was factored into the latency measurement.

6.12 METRICS FOR A HOSTILE NETWORK CONFIGURATION

The performance of SZRP versus ZRP, when all of the nodes in the network are behaving appropriately, is compared using the metrics given in the preceding section. In order to

establish the impact that malicious node activity has on the two protocols, we carried out several more tests. In order to do this, we used the field configuration of twenty nodes that were spread out over a 1200m x 1200m region and performed simulations with twenty percent and thirty percent of the nodes being malicious for each protocol.

CHAPTER 7

DIRECTIONAL ANTENNA SYSTEMS

7.1 INTRODUCTION

Researchers have been working towards the objective of improving the capabilities of ad hoc networks by using a wide range of unique ways. This has been done in order to achieve the goal. Among the most major technological limits that contribute to the capacity limitations, the omnidirectional nature of gearboxes is one of the most critical limitations. The dispersion of energy in all directions other than the direction that the destination node is intended to be in not only causes undesirable interference to other nodes in the neighbourhood, but it also lowers the feasible range of transmissions. This is because the destination node has to be in the direction that it is intended to be in. Indeed, it is.

The assumption that transmission is omni-directional was used in the development of all of the MAC and routing protocols that were covered in preceding chapters. This assumption was made for the purpose of design. The amount of pressure that can be put on the capacity of the system is effectively limited as a result of this, despite the fact that it makes things simpler to comprehend. the findings of an intensive examination of the capabilities of the ad hoc system are presented here. It has been established in this study that the throughput that each node is capable of achieving may be broken down into the following categories:

$$\Theta\left(\frac{W}{\sqrt{n \log n}}\right)$$

In this equation, W stands for the data rate, and n is the total number of nodes that make up the network. There is a capacity limitation that exists independent of the routing protocol or channel access mechanism that is being considered. This constraint is there. It has also been

proved that the partition of the channel into sub-channels does not have any impact whatsoever on this value. This is yet another item that has been demonstrated. Directional antenna systems are becoming more recognised as an efficient way for expanding the capacity, connection, and covertness of microwave access networks (MANETs), as a rising number of individuals are beginning to realise this fact.

It is possible for directional antennas to focus electromagnetic energy in a particular direction, which allows them to expand the coverage range while keeping the power level the same. In addition to this, they reduce the amount of interference that occurs between co-channels and the amount of noise that is present in a contention-based access scheme. This, in turn, leads to a decrease in the chance that conflicts will arise. Furthermore, in addition to this,

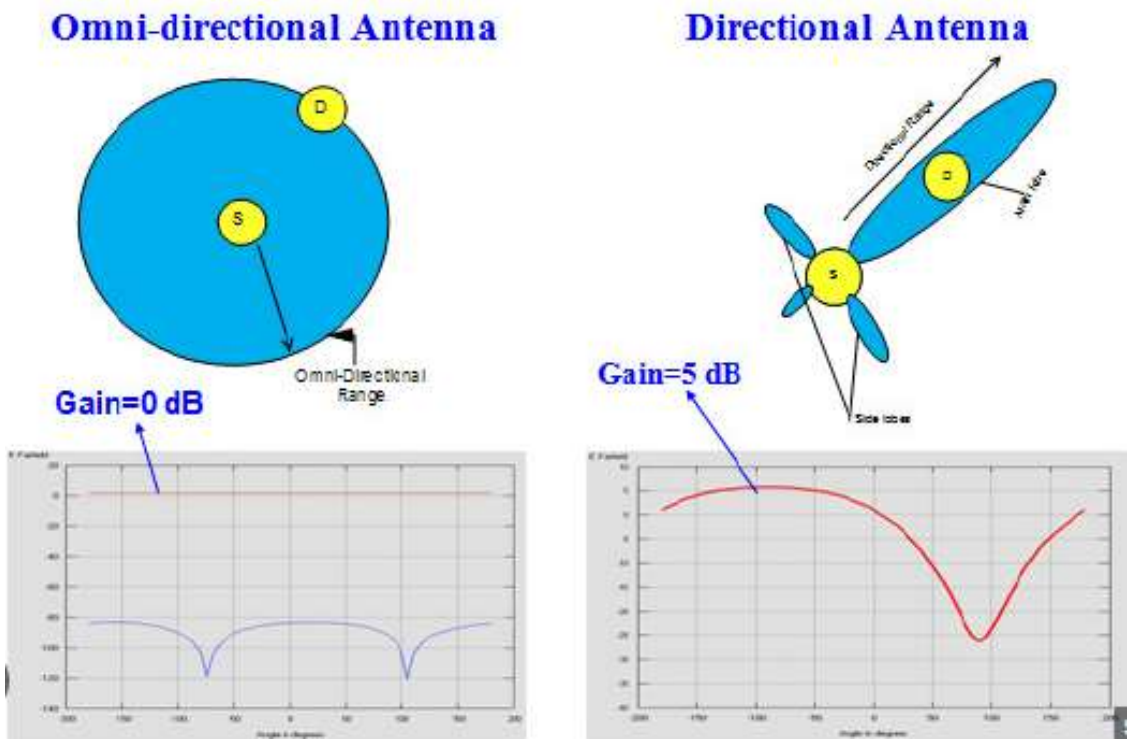

Fig.: 7.1 Communication using omni-directional antennas (a) and the increased spatial reusability when employing directional antennas (b) [Taken from http://www.crhc.uiuc.edu/~croy/presentation.html]

Source: Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

With increased signal strength and fewer multipath components, they provide connections that are either more stable or have a larger range. This is because of the combination of these two factors. Improvements in network capacity can be achieved by the use of greater spatial reuse and longer ranges, in addition to the provision of deeper connections. For this reason, larger ranges offer more connection, as well as more simultaneous transmissions and fewer hops, which in turn allows for more simultaneous broadcasts. There are directional antennas that enable a node to select and receive signals only from a certain direction that it has chosen [Libertil999].

Additionally, these antennas can be found on the receiving side. Figure 6.1 illustrates the increased capacity for spatial reuse that is made available by the use of directional antennas in circumstances when nodes C and D, as well as X and Y, desire to achieve simultaneous communication. As can be seen in Figure 6.1(a), there is only one pair of nodes that are able to interact with each other when omni-directional antennas are utilised throughout the communication process. The reason for this is that nodes D and X are located within the same radio range of one another. In spite of the fact that we are restricting our discussion to nodes C, D, X, and Y at the moment, it is essential to bear in mind that when omni-directional antennas are used, all of the nodes that are within the radio range of these nodes (i.e., nodes A, B, E, and F) are also under the possibility of being affected.

For the scenario represented in Figure 6.1(a), if we make the assumption that nodes C and D were the ones to initiate their communication first, then all of the nodes that are next to C and D, including node X, will remain silent during the length of their interaction. This is because nodes C and D are the ones that initiated their communication earlier. As illustrated in Figure 6.1(b), however, it is feasible for both the C-D and X-Y node pairs to carry out their communication at the same time when directional antennas are deployed.

This means that the communication can take place simultaneously. Because of this, the capacity of the network may be considerably expanded, and the total interference can be minimised. Both of these outcomes are possible through this. This is due to the fact that broadcasts are now directed towards the receiver that is supposed to receive them.

Because of this, it is now feasible for numerous broadcasts to take place concurrently in the same neighbourhood utilising the same channel, which is something that is not conceivable with omni-directional antennas. On the basis of five factors that are self-explanatory, the following table presents a condensed comparison between omni-directional antennas and directional antennas.

Table 7.1 An examination of the differences between directed and omnidirectional antennas

Characteristics	Omni	Directional
Spatial reuse	Low	High
Network connectivity	Low	High
Interference	Omni	Directional
Coverage range	Low	High
Cost and complexity	Low	High

Source: Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

The goal of this chapter is to offer an introduction to the use of directional antenna systems for the purpose of ad hoc Internet networking. The objective of this article is to provide a detailed introduction of directional antenna systems, as well as the challenges that are associated with their utilisation in ad hoc and sensor networks, as well as potential solutions to these challenges. In addition to providing a discussion of research problems in the areas of physical, MAC, neighbour identification, and routing with directional communications, this article offers a summary of the present state of the art in the field.

7.2 ANTENNA CONCEPTS

The antennas that are utilised in any communication system are largely responsible for compensating for the loss of signal strength that happens during the transmission in both directions. This loss of signal intensity occurs when a signal is transferred from its source to its destination (and vice versa). Resonant devices, which are able to work well within a specific frequency range that is quite narrow, make up the vast majority of antennas. Their frequency range is rather narrow.

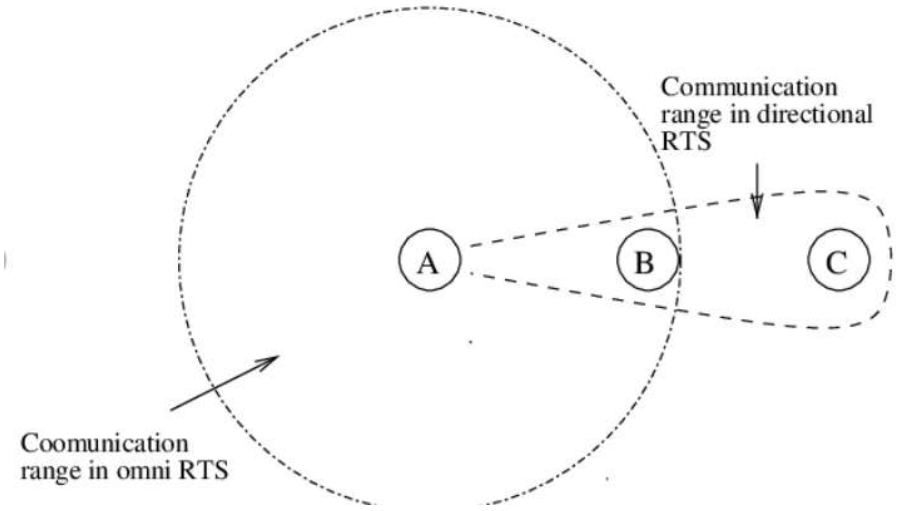

Fig.: 7.2 Both omni-directional and directional broadcasts are included in the coverage range

Source: Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

Adjusting an antenna to the same frequency range that the radio system to which it is attached operates in is required in order to prevent interference with reception and/or transmission. This is important in order to avoid interference with either of these processes. Prior to a relatively recent period of time, antennas were the components of personal communications

systems that received the least amount of attention. It is necessary for electromagnetic energy to be transported from one medium (space) to another medium (wire, coaxial, waveguide, etc.) in order for radio antennas to work correctly.

When it comes to the utilisation of the wireless spectrum, the manner in which energy is sent into space and recovered from space has a considerable influence on the utilisation of the spectrum. It is an example of one of the first designs that was used, and it is a conventional dipole antenna. The length of the antenna is controlled by the wavelength X, and it is supposed to be isotropic. The radiation pattern of these antennas is designed to be symmetric in all directions, as seen in Figure 6.2. Additionally, these antennas are known as omni-directional antennas. When it comes to highly concentrated directional antennas, which are more popularly known as "yagi" antennas, the reverse is true. The energy that is sent or received by these antennas is concentrated in a single direction.

7.2.1 Gain

Inexperienced radio users all over the world tend to feel a sense of dread in their hearts and thoughts whenever they hear the term "gain" in connection to antennas. This is the case regardless of where they are located. Nevertheless, despite the fact that it is commonly used to make a reference to a secret signal amplifier of some type, it is never totally understood. On the other hand, contrary to the belief held by the vast majority of individuals, an antenna that has a "higher" gain does not amplify the signal more than another antenna that has a "less" gain. What actually takes place is that an antenna with a greater gain just focuses the energy of the signal in a different manner.

Let's discuss the concept of "gain" in relation to a loudhailer so that we may get a deeper comprehension of it. You have the option of selecting any of the two options that are listed below in the case that you decide to deliver your message at a stadium with a large number of spectators: The first choice is to shout into it as loudly as you possibly can, and the second choice is to direct the focused end of the loudhailer towards the person who is listening to

what you have to say. In addition, the process of transmitting a radio signal can make use of these two motions during the procedure.

Therefore, you have two choices: either you can increase the transmit power (according to FCC Part 15, spread spectrum radios are restricted to a maximum of 1 Watt), or you may "aim" the radiating power from the antenna towards the receiver. Both of these alternatives are available to you. The act of targeting the power is what is meant by the term "gain" in this statement. Taking this a step further, if someone else in the stadium also had a loudhailer and was extremely interested in hearing what you had to say, they could place their loudhailer to their ear and point the open end towards you, which would allow them to concentrate on what is being relayed from your location. It is also feasible for a receiving radio to achieve "gain" by pointing the direction of the "listening" antenna in the direction of the source. This is another method which may be utilised.

Simply explained, gain is nothing more than the method in which the radiated energy is concentrated at the transmitter and the manner in which the ear of the receiver is focused. This is another way of saying that gain is the same thing. Within this part, we will provide an explanation of the process by which gain is applied to the two sorts of antennas that are employed in spread spectrum industrial radio setups the majority of the time. There are omni and yagi antennas in this set. In order to explain it in the simplest terms possible, omni antennas are able to produce and transfer power (the signal) in all directions while simultaneously listening for incoming signals from all directions as they occur.

In addition to having an ear that is more focused on listening for incoming signals, Yagi antennas, which are also known as directional antennas, are able to direct the power that they radiate and broadcast in a particular direction. Yagi antennas, on the other hand, have a propensity to send a signal further than omni antennas do when they have the same intensity. This is because of the reason stated above. When it comes to antennas, yagis are comparable to megaphones in terms of their capabilities.

7.2.2 Radiation Pattern

A method of defining the relative strength of the field that is radiated in different directions from the antenna, at a distance that is either fixed or constant, is referred to as the radiation pattern. This pattern is also known as the antenna pattern. With the assistance of this, it is possible to specify the gain values in each and every direction of the space. A major lobe that has a peak gain and side lobes that have a smaller gain are typically the components that make up this structure. The term "peak gain" refers to the highest and most significant gain that may be achieved in any direction.

According to one interpretation, the word "lobe" might also be interpreted as "beam." Beam width is a concept that serves a similar purpose within the framework of the antenna system. "Half power beam width" is a phrase that is used in the context of the antenna radiation pattern. This term refers to the angular space that occurs between the half power points, which are locations where the gain is equal to one half of the peak gain. Generally speaking, the beam width of a more directed antenna is often smaller, but the gain of the antenna is typically bigger.

7.2.3 Beam Width

There are several definitions of beam width (or simply beam width), and these meanings might vary depending on the radio system that an antenna is being used in. One definition that is frequently used is the 50% power beam width. After the peak radiation intensity has been identified, the dots that are positioned on each side of the peak indicate the locations of half of the power of the peak intensity.

The beam width is equal to the reciprocal of the angular distance between the half power points that are travelling through the peak. Because the power is -3dB, the beam width that corresponds to half the power is frequently referred to as the beam width that corresponds to 3dB.

7.3 EVOLUTION OF DIRECTIONAL ANTENNA SYSTEMS

In the following paragraphs, we will offer a brief description of the various directional antenna systems that are now functioning. It is feasible to examine the evolution of directional antennas at many different stages, beginning with fundamental sectorized and diversity antenna systems and proceeding even further to more advanced smart antenna systems. This is something that can be done. As a result, the objective of this presentation is not to cover every aspect of the technology; rather, it is to provide the principles in a manner that is not only informal but also obvious.

It is done in this manner so that it may serve as the basis for comprehending the ramifications of the technology at the MAC and routing levels, which will be discussed in a later section. In the event that you are a reader who is interested in acquiring further information regarding this topic, you may want to consult [Libertil999]. There are three separate categories that may be used to classify the current generation of directional antenna systems. These categories include sectorized, diversity, and smart. After this, we will proceed to present an explanation of each of these different systems each.

7.3.1 Sectorized Antenna Systems

A base station separates the standard cellular region into independent sectors, and each of these sectors is handled as a sub-cell. These antenna systems are utilised widely in cellular networks, which are characterised by their widespread use. The range of each sector may be improved by employing antennas that are segmented into sectors. Additionally, sectorized antennas enhance the likelihood of channel reuse while simultaneously lowering the amount of interference.

7.3.2 Diversity Antenna Systems

The presence of a lot of antenna components on the receiving side is something that diversity systems make sure to have. These components have been physically isolated from one another

in order to improve reception by lowering the likelihood of multipath occurring. Diversity schemes frequently make use of two different ways, and they are as they are described below:

Switched Diversity: For the sake of this scenario, it is assumed that at least one of the antennas is located at a distinct physical place that is in a favourable position at a certain instant in time. In addition to this, the system is able to transition between various components in a continuous manner in order to make use of the component that has the highest output. Although these systems make an attempt to increase throughput, they do not take advantage of the gain that may be produced by utilising several antennas since they only utilise one of them at any given time. This is because they only use one antenna at a time.

Diversity Combining: These systems make use of the idea of diversity combining, which involves the mixing of multipath signals that have been received at various antenna components, the correction of phase errors in those signals, and the combining of their power in order to achieve gain and take into account multipath and fading characteristics.

7.3.3 Smart Antenna Systems

Sheikh (1999) defines a smart antenna system as a combination of an antenna array and a digital signal processing capability that enables the receiving and transmission of signals in a manner that is both adaptive and spatially sensitive. This type of system is able to receive and transmit signals in a manner that ensures optimal performance. In order to accommodate the wireless environment in an appropriate manner, these systems are equipped with the potential to automatically modify the directionality of their radiation patterns. If they are employed in the suitable manner, smart antenna systems have the ability to significantly increase the performance of a wireless ad hoc system.

This is provided that they are appropriately utilised. Although the concept of intelligent antenna systems has been known for quite some time, its application in commercial items has been delayed by budgetary restrictions until relatively recently. This is despite the fact that

the notion has been around for quite some time. This is because of the development of software-based signal processing techniques and algorithms, as well as the introduction of powerful low-cost digital signal processors, application-specific integrated circuit (ASIC) design, and other technological advancements.

These advancements have made it possible for these systems to be utilised not only in cellular environments, but also in ad hoc networks. With regard to smart antennas, there are two types that may be distinguished from one another. Both of these categories are distinguished by the use of an array of omni-directional antenna components inside the system. Systems of antennas that make use of switching beams for: A switched beam system is comprised of a collection of predefined beams (see Figure 6.3(a)), from which the beam that is selected is the one that is able to receive the signal from a particular user in the most efficient manner.

This beam is the one that is selected. Because the beams have a small main lobe and tiny sidelobes, signals that arrive from directions that are not the intended direction of the main lobe are substantially muffled. This is because the major lobe is in the direction of the beam's intended direction. The cellular systems that are currently in use are a good example of one form of smart antenna system that is analogous to the ones that are used by those systems. They employ transmission through directed beams that have a limited number of predetermined radiation patterns, and in addition to that, they offer interference suppression along extra beam directions. Steerable antenna systems are a sort of switched beam antenna system that may also be used to steer the beam in order to continuously track a transmitter or receiver.

Steerable antenna systems resemble switched beam antenna systems. Utilising switched beam antenna systems allows for the promotion of spatial reuse due to the fact that these systems focus energy in a particular direction exclusively. The generation of lobes, nulls, and regions of medium and minimal gain occurs in directions that are distant from the main lobe of a switched beam antenna. This occurs when the primary lobe of the antenna is directed in the

direction of the user, which results in improved gain. The direction in which these regions are located is the opposite of that of the main lobe.

Adaptive antenna arrays: Adaptive beamforming antenna systems are another term for the devices that fall under this category. The most cutting-edge and cutting-edge smart antenna that has ever been built is currently this one. It is the most cutting-edge smart antenna. When it comes to constructing the beam patterns and suppressing interference, it provides the highest possible degree of adaptability. Patterns of radiation that can be altered in real time are accessible to adaptive antenna arrays, which have an infinite number of potential patterns (see to Figure 6.3(b) for further information).

Beamforming techniques allow them to position nulls in the direction of the signals that are creating interference from other users while simultaneously directing the main lobe of the beam in the direction of the user that is being sought. This is made possible by the fact that they are able to direct the beam in the direction of the user that is being sought. By employing these signal processing techniques, these antenna systems are able to successfully locate and track signals. This enables them to limit interference and enhance the quality of signal reception, which improves the overall quality of the signal reception.

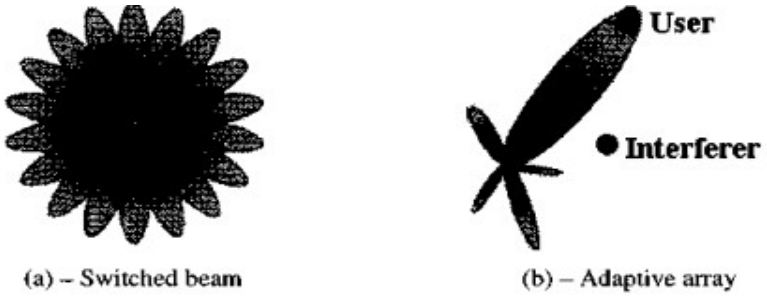

Fig.: 7.3 The switching beam antenna system and the adaptive array antenna system are compared

Source: Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

A network of omni-directional antenna elements is the building block of smart antennas; these components receive the signal and adjust its phase and intensity as needed. The production of the major lobe and nulls in certain directions are made possible by this array of complex values that constitute a steering vector. You can provide the desired directions' (L-l) maxima and minima, or nulls, with an L-element array. To achieve this, while determining the beamforming weights, constrained optimisation approaches are employed. The degree of freedom of an L-element array is the capacity to fix the pattern at (L-l) positions.

Because of its adaptability, the array may be utilised in several scenarios. Figure 6.4 shows the transmission ranges of several smart antenna technologies. According to the data shown in the picture, the adaptive system may reject interference and provide a substantially wider coverage area than the sectorized or switched beam systems. A technique known as multiple inputs multiple outputs (MIMO) systems is created when a communication link uses multiple antennas at both ends. Both network reliability and spectrum efficiency are significantly improved by this approach.

Modern technology has made it possible to use many antennas on each end of a connection to multiplex the data stream and create many data streams using the same frequency spectrum. The result is a linear bandwidth for the system with no extra power consumption needed. Historically, the high price tag has been the main deterrent to commercializing adaptive antenna array technologies. The specialised digital signal processing controllers used by each of the many antenna beams add a substantial premium to the system's total cost. However, with the advent of commercial equipment that employs MIMO (such as the IEEE 802.1 The criterion discussed in Chapter 4 indicates that the cost issue is progressively losing importance.

Up until now, most studies on directional antennas for ad hoc networks have focused on either adaptive antenna arrays or switching beam antenna systems. The majority of studies on switching beam antennas have concentrated on the read, MAC, and routing aspects of

networking that are relevant to their uses. Nevertheless, most research on adaptive antenna arrays has focused on the physical layer, with very little investigation into the media access control (MAC) and routing levels.

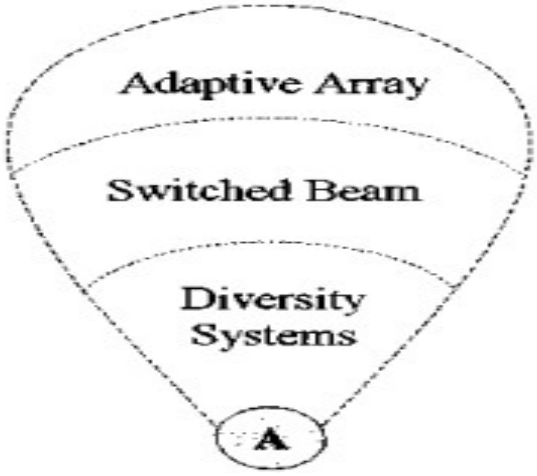

Fig.: 7.4 Coverage Range of Directional Antennas

Source: Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

7.4 ADVANTAGES OF USING DIRECTIONAL ANTENNAS

The performance of wireless systems has the potential to be significantly improved by technological breakthroughs in directional antennas for wireless systems. The use of directional antenna systems may be helpful for both infrastructure-based networks, which are also referred to as personal communication systems, cellular networks, and wireless local loop networks, as well as ad hoc networks. In the following, we will talk about some of the advantages that come along with the use of directional antennas [Sheikh 1999].

In ad hoc networks, a node is able to concentrate its whole transmission energy towards a particular direction by utilising several antenna beams. This allows the node to increase the

range of its transmission, which in turn increases its range. In the field of physics, this phenomenon is known as antenna gain. Generally speaking, this is what people mean when they talk about transmission gain. Similarly, on the receiving side, a node has the capacity to selectively accept the packet at a given antenna beam; An array gain is attained when numerous antennas in a smart antenna system are able to combine the signal energy in a coherent manner. As a consequence, the signal-to-noise ratio (SNR) at both the source and the destination is increased as a consequence of this outcome.

variety Gain: As was indicated earlier, the geographical variety that is supplied by many antennas has the potential to be an important instrument in the fight against channel fading. When diversity is employed, it is feasible for a node to switch between several antenna components in order to get the best possible signal strength. This is achievable because variety allows for higher signal strength.

Using the concept of a smart antenna system, it is now possible to combine many antennas in an adaptive manner in order to selectively cancel out or prevent interference and pass the signal that is necessary. Interference suppression is the term used to describe this phenomena. It is possible to reuse frequency at angles that are covered by different antenna beams, provided that directional antennas are utilised. This is referred to as angle reuse. Using a method that is usually known as space-division multiple access (SDMA), this technology is able to accommodate numerous users at the same time inside the same frequency channel.

It is necessary to regulate the signal separation of co-channel beams at each level of the network. Regarding this particular matter, it is important to take it into mind. Due to the existence of dispersion and mobility, which both make signal separation difficult, angle reuse has not been shown to be a viable technique in MANETs. This is because of the limitations of the technology.

Through the utilisation of a technology known as spatial multiplexing, it is now possible to dramatically increase the bit rates of a wireless link. This is a huge advancement in the field

of wireless communication. Utilising multiple antenna beams at both ends of the wireless communication is the method that is utilised to achieve this success. A partitioning of the information stream into N distinct streams is carried out within the context of spatial multiplexing. Each of these streams is modulated and sent in a single stream per antenna, all inside the same radio channel.

This allows for the utilisation of the capacity that is required to support sub-streams that operate at substantially lower rates. If the receiving antenna is correctly separated, it is feasible to merge the sub-streams that have been received in order to retrieve the high bit rate stream that was initially received. This is only possible if the antenna is well separated. Greater spectrum efficiency can be achieved through the use of spatial multiplexing when the channel conditions are suitable. In addition, it does not need any prior knowledge of the channel, which is another component that contributes to its high level of dependability.

7.5 DIRECTIONAL ANTENNAS FOR AD HOC NETWORKS

It is projected that in the future, a wide range of applications will require the utilisation of a variety of antenna systems in order to satisfy requirements such as cost, size, energy constraints, performance, and so on. There are many applications that will require this. The principal applications of ad hoc networks may be broken down into many separate categories, according to what we have learnt up to this point [Ramanathan2001]. These categories include applications for the military, applications for outdoor conditions or disaster recovery, and applications for interior environments.

It is feasible that the cost of even the most modern antenna might be regarded to be within acceptable limitations. This is due to the fact that the nodes (tanks and aeroplanes) that are used in military applications are so costly. Beamforming antennas have the ability to give increased protection against jammers and enable enhanced security provisioning, which is an additional advantage of using these antennas. For the purpose of communicating with a number of different nodes, a switched antenna beam may be utilised when the operation is

carried out at fixed outside locations. Within the context of this particular application, it is feasible that steerable beam antennas might be prohibitively expensive.

To add insult to injury, when we take into account the use of directional antenna systems for tiny portable devices, laptops, and personal digital assistants (PDAs), the size of the antenna becomes an additional component that makes the problem more complicated. As an illustration, a cylindrical array that is comprised of eight components will have a diameter of around eight centimetres when it is operating at 2.4 GHz spectrum. Alternatively, the size is reduced to 3.3 centimetres for the frequency band of 5 GHz, while the size would amount to around 0.8 centimetres for the ISM band of 24 GHz.

Both of these sizes are mentioned in the previous sentence. As a result, the use of directional antennas for small devices looks to be fairly promising. This is especially true when taking into mind the fact that future devices are anticipated to make use of communication channels that are less crowded and higher in frequency. Additionally, because to the multiple advantages that these systems provide, the military is progressively embracing directional antenna systems rather than other types of antenna systems. This pattern is gradually becoming more prevalent.

7.5.1 Antenna Models

The classification of antenna types that was discussed earlier has a significant impact on the performance of the media access control (MAC) and the routing, as will become obvious in the subsequent sections of this chapter. When working with a wireless ad hoc network that does not have a central coordinator, it is of the utmost importance to keep this into consideration. Before beginning the process of developing the medium access control scheme, it is necessary to take into consideration the type of antenna that will be used in relation to the MAC. This action is taken in order to guarantee that the concealed and disclosed terminal problems are appropriately addressed and resolved. It is feasible that the routing protocols will need to be modified in order to take into consideration a number of concerns.

This is something that should be considered in relation to the routing protocols. In addition to a great deal of other concerns, these challenges include the exact direction in which a node can be positioned, the introduction of new neighbour discovery procedures, the potential of several pathways going to the same destination, the implications of directional antennas on the procedure for route discovery, and a great deal more. In light of this, it is of the highest importance to do research on the fundamental antenna system that is being utilised at the physical layer in order to gain an understanding of the impact that it has on the higher layers.

Following this, we will now talk about two distinct models of antennas, namely the switching beam antenna model and the adaptive antenna arrays model. Both of these models are quite different from one another. As was said earlier, they are the most often used choice for implementing in MANETs, and they serve as the basis upon which the bulk of the solutions that are now available are constructed. It is abundantly clear that these are only abstract models of antennas, and the results that are accomplished by the systems that are based on these models are only as good as the abstractions themselves. In the future, it will be important for research to investigate antenna models that are more exact in order to develop upper layer protocols in a manner that is appropriate.

7.5.1.1 Switched Beam Antenna Model

The Omni and Directional modes are the two separate modes that are included in this specific model to choose from. An omni-directional antenna and a switching beam antenna are two types of antennas that may be distinguished from one another. Both types of antennas have the ability to point in any direction that is specified. Both the Omni and Directional modes are capable of being used for the purpose of broadcasting and receiving signals. In a general sense, this is the case. On the other hand, the Omni mode is solely employed for the purpose of receiving signals, and the Directional mode is concurrently utilised for transmission and reception. To put it another way, the transmission procedure never makes use of the Omni mode under any circumstances.

By utilising beamforming in this fashion, both the transmitter and the receiver are able to make use of the increased coverage range that it gives. When a node is running in Omni mode, it is able to receive signals from any direction and has a gain of G° overall. Additionally, it is able to receive signals from any direction. When a node is not actively providing or receiving data on a regular basis, often known as when it is idle, it will frequently keep Omni mode activated. When a signal is detected, a node is able to determine the antenna via which the signal is strongest. This is possible after the signal has been detected. After that, this node switches to the Directional mode in this particular antenna, which causes it to lose its ability to hear in any other direction.

This is made feasible by the usage of a diverse selection process. When operating in the Directional mode, a node has the ability to direct its beam in a certain direction by utilising a gain of Gd (with Gd often being greater than G°). Utilising an array of beams, which is essentially a collection of antennas, is the means by which this is done. When compared to nodes operating in Omni mode, those running in Directional mode have a greater range than those operating in Omni mode due to the higher gain. In addition, the gain is proportional to the number of antenna beams: this is due to the fact that more energy may be focussed on a given direction, which eventually leads in an increased coverage range in that particular direction as a consequence of the larger energy concentration.

For example, a twelve-antenna array has a wider coverage range than a six-antenna array, whereas a six-antenna array covers a larger area than a four-antenna array. Both of these arrays are examples of antenna arrays. The entire process is carried out while preserving the same quantity of energy that is available for transmission. Among the many concepts, there are those that take into consideration this quality, while there are others that do not. It is likely that in order for a transmitter to carry out a broadcast using this specific type of antenna, it will be necessary for the transmitter to carry out as many directional transmissions as there are antenna beams in order to reach the whole territory that surrounds it. This is because the antenna beams will be able to cover the entire region.

When it comes to beamforming, it is usually assumed that there is a minimum delay in each of the many directions. This process is known as sweeping, and it allows for the transmission of light. Figure 6.5 provides a visual representation of the switched beam antenna model that it is possible to find. This concept is taken into consideration by a considerable number of the MAC and routing systems that are now available (MAC and routing systems). Using this setup, the node is encircled by a total of M beams that do not overlap with one another in any way.

The numbering of the beams starts at three o'clock and continues in an anticlockwise direction, with the first beam being numbered 1 and the final beam being numbered M on the anticlockwise direction. The ability to receive and send data for a node is possessed by each and every one of these M antenna beams. Last but not least, it is usually assumed that nodes would maintain the direction of their beams regardless of movement. This is due to the fact that dynamically tracking a user is a tough effort. With the use of a device that is capable of locating directions, such as a compass, it is possible to execute this particular task.

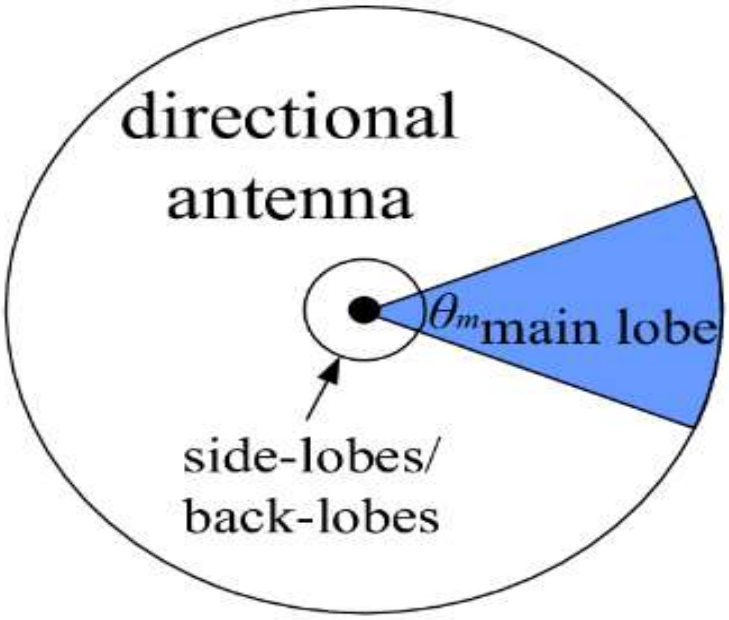

Fig.: 7.5 The antenna model

Source: Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

7.5.1.2 Adaptive Antenna Array Model

Both the adaptive antenna array and the switched beam antenna models have a number of distinguishing characteristics, the most important of which is that the former allows for multiple simultaneous receptions or transmissions (although simultaneous transmission and reception is not possible), whereas the latter only allows for a single transmission or reception to take place. Consider the example shown in Figure 6.6 in order to better understand the distinguishing characteristics of the adaptive antennas array concept. The nodes in this configuration are outfitted with adaptable antenna arrays, and the beam width of each beam is about JI/2 radians when measured.

In this diagram, the beams that are receiving are represented by solid lines, while the beams that are broadcasting are represented by dashed lines. In the image, it is shown that a certain node, which we will refer to as node A, gets information from two distinct nodes, B and C, which are located in different receive beams of A. As a result of this, A is able to concurrently receive packets from several nodes, each of which contains a packet for it. It is possible for a node to concurrently broadcast to numerous nodes at the same time. This is because transmission and reception are activities that are the opposite of one another. Note that although though the regions that are covered by the transmit beams of nodes B and C overlap, they do not produce a collision at node A.

This is something that can be seen shown in Figure 6.6. This is due to the fact that the direction of the electromagnetic energy that is impinge on an adaptive antenna array is the most important characteristic that provides assistance in the formation of a receive beam [Lal2004]. This means that a specific adaptive beam may be understood as the matching of the antenna system to a certain set of directions, or more specifically, a set of angles for the incoming or outgoing RR.

The receive beams of node A provide an illustration of the incidence angles that are experienced during receipt. Therefore, because the incident energy from nodes B and C is significantly different from one another in terms of the angle at which it strikes node A, they do not interact with one another when they are received at node A. There is a possibility of interference occurring when a certain beam possesses sidelobes that are oriented in an abnormal manner. In spite of this, the majority of the research that has been done in the field of ad hoc networks has been based on the assumption that perfect switched beams are created in the required directions and that sidelobes are unimportant.

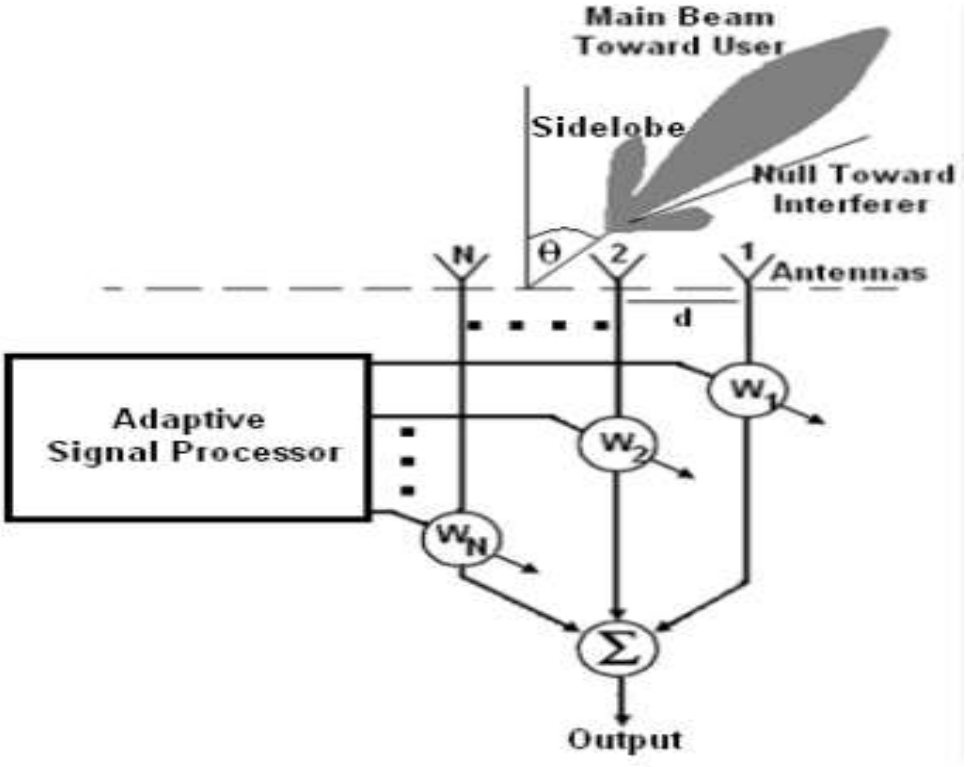

Fig.: 7.6 Example of the adaptive antenna array model [Taken from IEEE Publication Lal2004]

Source: Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

7.6 PROTOCOL ISSUES ON THE USE OF DIRECTIONAL ANTENNAS

This section will cover a variety of protocol concerns that pertain to directional antennas, namely those that are associated with MAC and routing. It is important to note that some of the problems that will be mentioned in the next section might not be present in all of the protocols that have been proposed for directional antennas. This is because them are very dependent on the antenna model that is being considered.

7.6.1 Directional Neighborhood

It is well knowledge that the neighbourhood of a node is made up of all the nodes that are in close proximity to that node and may engage in direct communication with it. In contrast, when it comes to directional antennas, the idea of a neighbour needs to be rethought in comparison to omni-directional antennas. This is because directional antennas produce a different kind of signal. During the process of doing a full "broadcast" in a directional antenna system, it is possible that a node will be required to deliver the broadcast packet in a circular way as many times as the antenna beams. The technique that is being described here is called "sweeping."

This sort of design is a simulation of a broadcast that is carried out by an omni-directional antenna, and from a theoretical point of view, it ought to fulfil the same aims as the aforementioned broadcast. In spite of this, the procedure is not as simple as it would appear to be. This is due to the fact that the sweeping approach is accompanied by a substantial delay, and it is essential to send the same packet many times. Increasing the number of beams that are added causes the sweeping delay to increase in a proportional manner. This trade-off, along with other successful ways for broadcasting using directional antenna systems, will be discussed in a later portion of this article.

In addition, when we take into account the enhanced gain that is provided by the directional antennas, the idea of directional neighbourhood becomes significantly more complex from

that point on. We are going to illustrate this specific idea using the assistance of Figure 6.7. Let us assume that nodes A and B in Figure 6.7(a) are not actively listening to media in either direction, and that they have a gain of G°. This is for the sake of this illustration. As a consequence of this, node C makes the decision to establish a connection with node A by increasing its gain to Gd and submitting its packet for transmission. Despite the fact that it is only receiving with gain G°, node A is in close enough proximity to node C to be able to receive the packet. This is the case within the context of this circumstance.

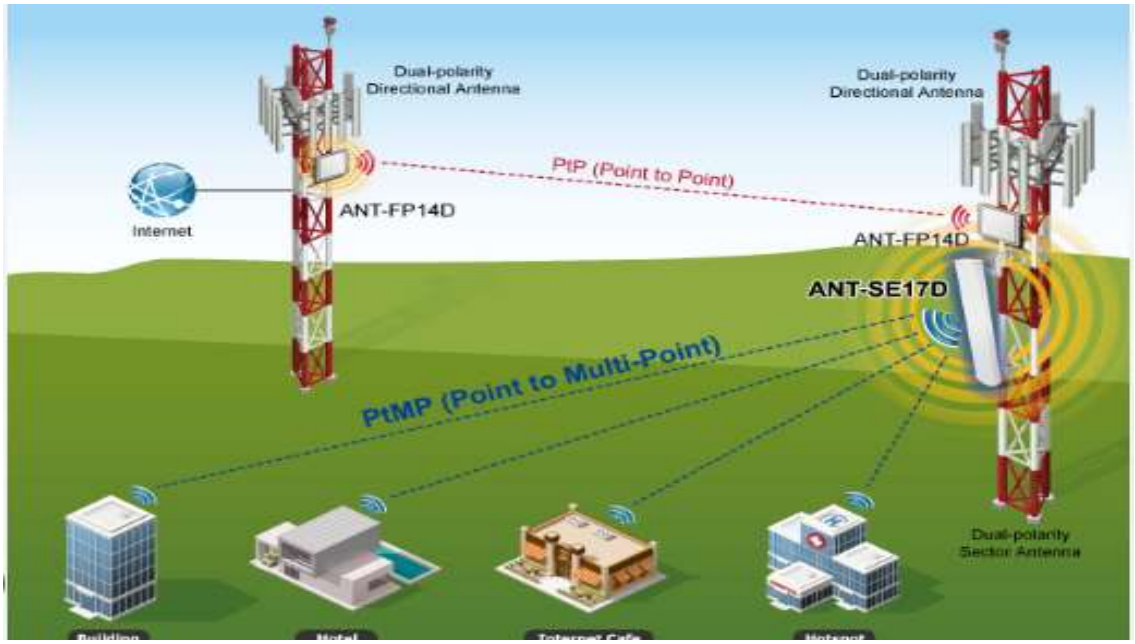

Fig.: 7.7 When it comes to directional antenna systems, the neighbourhood in the direction

Source: Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

On the other hand, because it is operating in omnidirectional mode and, as a consequence, has a receive gain of G°, node B is unable to receive the packet transmission that was sent from node C. This is because it is unable to receive the packet transmission. In contrast to the fact that C and A are regarded to be Directional-Omni (DO) neighbours, C and B are not

considered to be DO neighbours. Consider the scenario depicted in Figure 6.7(b), in which node B tunes in the direction of node C, hence raising its gain to Gd in this particular direction.

This is the circumstance in which the case is illustrated. Due to the fact that both node B and node C are successfully engaging with gain Gd in a directed manner, it is now possible for node B to receive packets from node C in this specific case. Therefore, the only time that nodes B and C are deemed to be neighbours is when they are located in a directional mode that is oriented in the direction of each other. From the perspective of this definition, C and B are deemed to be directional-directional (DD) neighbours.

As can be seen from this particular illustration, the concept of neighbours in directional antennas requires a significant amount of reevaluation. Additionally, broadcasting is another issue that should receive greater attention in addition to it. In the following sections, we will give some suggestions that are aimed at minimising or resolving the neighbouring problems that have emerged as a result of the implementation of directional antenna infrastructure.

CHAPTER 8

SENSOR NETWORK DATA RETRIEVAL

8.1 INTRODUCTION

Considering that Wireless Sensor Networks (WSNs) are still in their infancy, there are a great deal of issues regarding them that have not yet been resolved. As time goes on and further applications for these technologies are researched, there will be a great deal more of them. In Chapter 8, we discussed the fundamentals of a wireless sensor network (WSN). After the Sensor Nodes (SNs) have been established, we will consider the means by which we might acquire data from the Wireless Sensor Network (WSN).

Therefore, the primary problem is the manner in which data is transmitted from all of the SNs to a central location, which is on occasion referred to as a sink or Base Station (BS). This must be done regardless of whether or not a wireless sensor network (WSN) is clustered. When this occurs, it indicates that every WS is required to either communicate the detected values directly to the BS or employ a multihop protocol through its CH in order to deliver them.

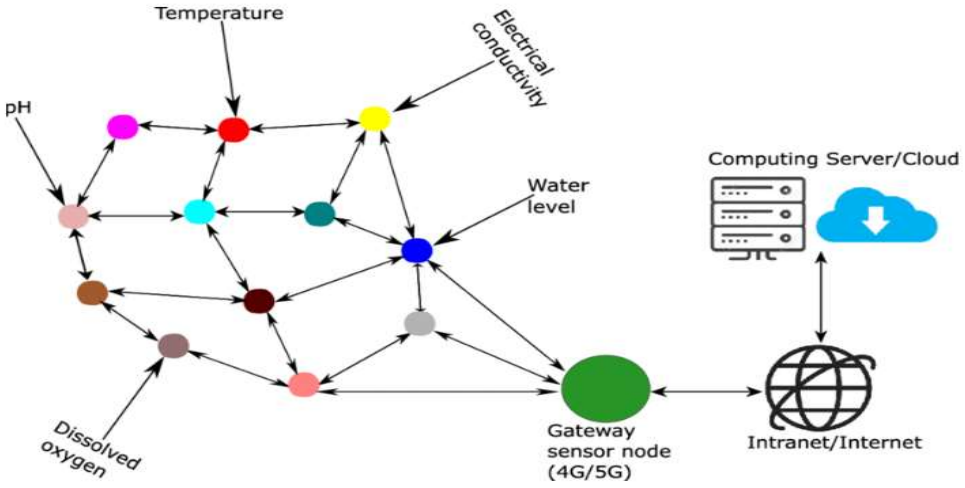

Fig.: 8.1 The installation of sensors and the establishment of networks

Source: A secure zone-based routing protocol for mobile ad hoc networks data collection and processing through by Niroj Kumar Pani (2009)

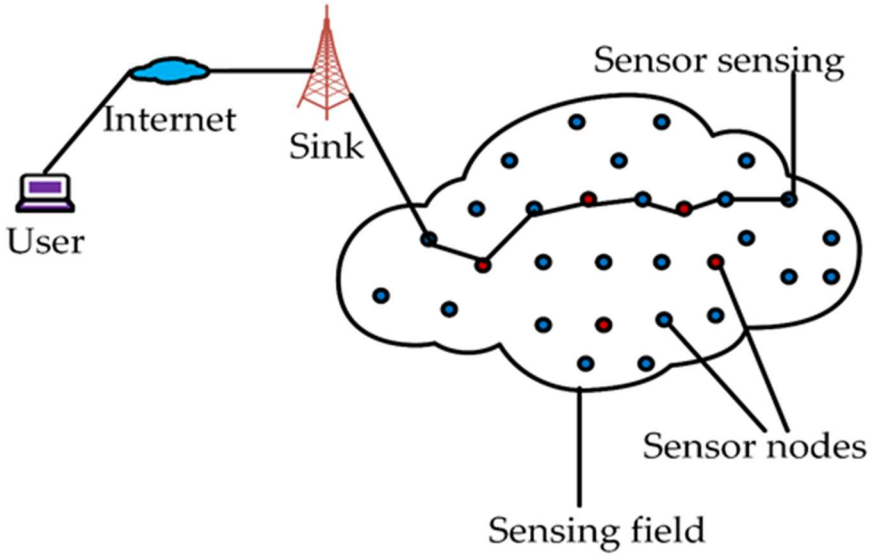

Fig.: 8.2 WSN and Query injection/response

Source: A secure zone-based routing protocol for mobile ad hoc networks data collection and processing through by Niroj Kumar Pani (2009)

a style that is the result of power being restrained. Consequently, it is essential to provide pathways that connect the SNs to the BS networks. In a typical SN node, there are a number of transducers that are capable of measuring a wide range of physical characteristics. At any one time, the software has the ability to select which of these transducers to utilise. According to Jain (2005a), the base station (BS) in a wireless sensor network (WSN) has the ability to inject the query, which determines the overall goal.

In actual life, a low-flying aircraft, an unmanned aerial or ground vehicle, or a sturdy laptop may generally operate as a base station (BS) or sink (Figure 9.1), and they typically have a sufficient power source. As can be seen in Figure 9.2, this enables the BS to send a query

message at a very high-power level, which in turn enables it to simultaneously communicate with all of the WSs that are located within a certain region. The query may additionally contain information on some critical query attributes; the objective of this broadcasting is to make it possible for all WSs to start processing the request. When the base station (BS) is only able to reach a limited number of adjacent wireless sensor networks (SNs), the query can be routed to a particular region of interest or even the whole wireless sensor network (WSN) by utilising one of the multicast routing algorithms discussed in Chapter 3.

Utilising the multi-hop pathways in the same manner as the response is communicated is the recommended course of action. In certain cases, the type of query that is utilised is determined by the requirements of the application. Depending on the query, you can be required to identify and convey values for a large number of parameters all at once, over a period of time, or even make use of previous data in order to get statistical information. Temperature, pressure, humidity, and other variables may be included in this category of factors. On the basis of this, we are able to divide the question into three separate categories:

1. One-time queries.
2. Persistent queries.
3. Historical queries.

In one-time inquiries, the information about the sensed value is required just once, maybe as a snapshot of the present values. On the other hand, persistent queries require data to be collected over an extended period of time, preferably at regular intervals. The historical query takes into account the information that has been gathered over a previously determined amount of time. As was noted previously, the query is not injected to any particular WSs; rather, it is intended to get information on the values of all sensors readings that are in accordance with the requirements that are specified in a query.

An example of a question may be a temperature that is higher than 35 degrees Celsius. Given that this can be met by any of the sensors, it is necessary to broadcast the query to all of the

sensors that are located within a certain region. This qualifies a wireless sensor network (WSN) as "data centric" since the replies are generated by sensors that are positioned in random locations. In the event that the replying SNs are aware of the position of the BS, then the response could be directed towards the BS. This approach of directed diffusion has the potential to significantly cut down on routing overheads and might be of great assistance in reducing the amount of energy that is used.

8.2 CLASSIFICATIONS OF WSNS

It is essential to determine the frequency with which the sensed values are gathered whenever a WSN is deployed since its primary purpose is to collect data that has been felt by various WSs. While there are many different methods in which one might make use of the network's resources, wireless sensor networks (WSNs) can be categorised according to the mode of operation or functionality they utilise, as well as the kinds of applications they are designed to serve. As a result, we will now divide wireless sensor networks into three kinds:

- **Proactive Networks -** The nodes in this network periodically switch on their sensors and transmitters, sense the environment and transmit the data of interest. Thus, they provide a snapshot of the relevant parameters at regular intervals and are well suited for applications requiring periodic data monitoring.
- **Reactive Networks -** In this scheme, the nodes react immediately to sudden and drastic changes in the value of a sensed attribute. As such, these are well suited for time critical applications.
- **Hybrid Networks -** This is a combination of both proactive and reactive networks where sensor nodes not only send data periodically, but also respond to sudden changes in attribute values.

As soon as the type of network has been determined, it is necessary to build protocols that effectively route data from the SNs to the users. It is possible that an appropriate MAC protocol will be utilised in order to prevent collisions and the associated expenditure of energy

to prevent them. Since it is not typical to anticipate the presence of specialised high-energy nodes in a network, it is important to make an effort to ensure that energy dissipation is distributed uniformly among all of the nodes in the network. The proactive, reactive, and hybrid protocols are discussed in this chapter. Additionally, the importance of the protocols being closely tied to the needs of the application is emphasised throughout the discourse.

8.2.1 Architecture of Sensor Networks

Because of the fundamental disparities in application situations and the communication technology that lies behind them, the design of wireless sensor networks (WSNs) will be dramatically different, not only with regard to a single wireless sensor (WS), but also with regard to the network as a whole. The following components will typically make up the hardware platform of a wireless sensor node:

- Microcontrollers that are more straightforward and embedded, such as the Atmel or the Texas Instruments MSP 430. The answer to the important question of whether and how these microcontrollers can be put into various operational and sleep modes, the number of sleep modes that are available, the amount of time it takes to switch between these modes, and the amount of energy that is required to do so is a decisive characteristic in this case. This is in addition to the critical power consumption. Additionally, the requisite chip size, computational power, and on-chip memory are also critical considerations.
- Radio transceivers that are now in use include the RFM TR1001 or devices manufactured by Infineon or Chipcon; comparable radio modems are available from a variety of vendors. When it comes to modulation, ASK or FSK is typically utilised, but Berkeley PicoNodes utilise OOK modulation. The notions of radio, such as ultra-wideband, are currently at an advanced level (for example, the projects that are being carried out by the IEEE 802.15 functioning group).

- The development of a wake-up radio concept that is capable of functioning pretty well would be an important step forward. This idea could either wake up all of the SNs that are in close proximity to a sender or even only some of the nodes that are directly addressed. The use of a low-power sensing circuit is all that is required for a wake-up radio to enable an SN to go to sleep and then be roused from its sleep by appropriate broadcasts from other nodes. In addition to radio communication, additional transmission mediums, such as optical communication or ultrasonic communication for underwater applications, are also taken into consideration. On the other hand, this variable is very dependent on the application;
- Batteries supply the necessary amount of energy. The management of batteries, as well as the question of whether or not energy scavenging can be done to recharge batteries while they are out in the field, is an essential topic. Additionally, the self-discharge rates, self-recharge rates, and lifespan of batteries might be problematic depending on the application;
- The operating system and the run-time environment is a topic that is the subject of intense dispute in the research literature. It is necessary to have flexible means of combining protocol building blocks, as meta information must be used in many places in a protocol stack (for example, information about location, received signal strength, etc., has an influence on many different protocol functions).
- On the one hand, it is necessary to have a minimal memory footprint and execution overhead. Other than that, it is necessary to have flexible means of combining protocol building blocks. As a consequence of this, we are of the opinion that structures such as blackboards, publish/subscribe, or tuplespaces provide an intriguing starting point for the run-time environments of such SNs.

8.2.2 Network Architecture

According to what was covered in chapter 8, the design of the WSN has to cover a required region in order to provide sensing coverage and to ensure communication connectivity. As a

result, the density of the wireless sensor network (WSN) network is essential for the efficient utilisation of the WSN. The life-time of a wireless sensor network (WSN) cannot be measured in a way that is clearly defined. Depending on the circumstances, some people believe that the network's lifespan is determined by the failure of a single sensor or by the battery power running out. It is possible that a more accurate definition would be to define the life-time of the network as the proportion of sensors that stop functioning, provided that the network continues to function.

In the event when the percentage of failure is determined by the nature of the application, a wireless sensor network (WSN) may be regarded operational so long as the region is sufficiently covered by the sensors that are functioning. There is also the possibility of having some quantitative measures, such as the monitored region being covered to the extent of 95%. The SNs have not yet reached a point where they are affordable enough to be deployed with a certain amount of redundancy. As an illustration, it is a reliable statement to assert that a region may be monitored by several sensors at the same time.

On the other hand, this is still a concept that exists only in theory, as the coverage of a region by a single sensor is sufficient at the moment. Additionally, the degree of data reduction achieved through collaborative aggregation is an important factor in determining the extent to which energy usage is reduced. It is possible that a more dense deployment of sensors and transmission of sensed data would result in an increase in the amount of energy used as well as an increase in the delay. Transmission of data between two sensors that are located at a great distance from one another, on the other hand, may result in an increase in energy consumption due to the higher energy usage in

transmission via wireless networks (Figure 8.3)." In light of this, there is a distance between two sensors that is ideal and would result in the greatest possible sensor lifespan. Therefore, if there is a large density of sensors, it is possible to put some of the sensors into sleep mode in order to get a distance that is very near to the ideal spacing between the sensors.

Additionally, the design of the network as a whole need to take into consideration a variety of factors, including:

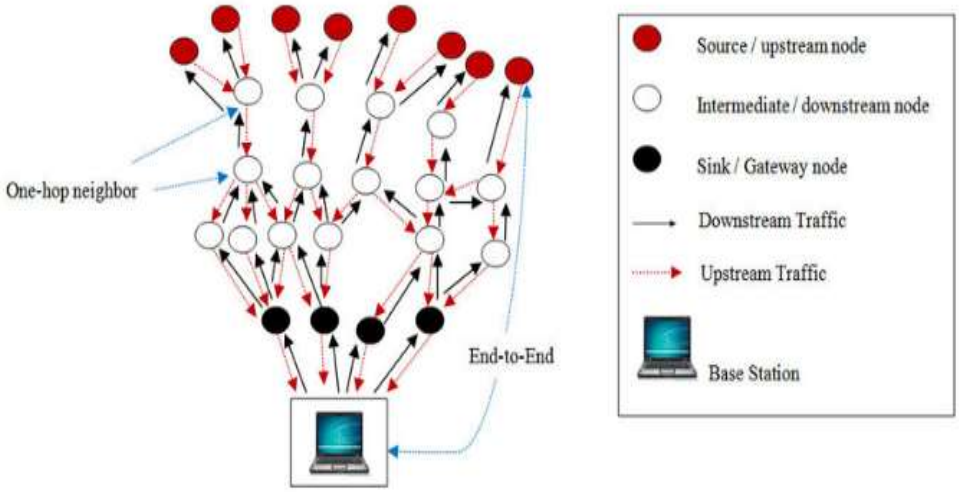

Fig.: 8.3 Transmission strategies between two sensors

Source: A secure zone-based routing protocol for mobile ad hoc networks data collection and processing through by Niroj Kumar Pani (2009)

- The protocol architecture has to take both application- and energy driven point of view;
- QoS, dependability, redundancy and imprecision in sensor readings have to be considered;
- The addressing structures in WSNs are likely to be quite different: scalability and energy requirements can demand an "address-free structure" [Estrin2001]. Distributed assignments of addresses can be a key technique, even if these addresses are only unique in a two-hop neighborhood. Also, geographic and data-centric addressing structures are required;
- A crucial and defining property of WSNs will be the need for and their capability to perform in-network processing. This pertains to aggregation of data when multiple

sensor readings are converge casted to a single or multiple sinks, distributed signal processing, and the exploitation of correlation structures in the sensor readings in both time and space. In addition, aggregating data reduces the number of transmitted packets;

- Based on such in-network processing, the service that a WSN offers at the level of an entire network is still an ill-defined concept. It is certainly not the transportation of bits from one place to another, but any simple definition of a WSN service ("provides readings of environmental values upon request", etc.) is incapable of capturing all possible application scenarios;
- As these services are, partially and eventually, invoked by agents outside the system, a gateway concept is required: How to structure the integration of WSNs into larger networks, where to bridge the different communication protocols (starting from physical layer upwards) are open issues;
- More specifically, integration of such ill-defined services in middleware architectures like CORBA [CORBAwww] or into web services is also not clear: how to describe a WSN service such that it can be accessed via a Web Service Description Language (WSDL) [WSDLwww] and Universal Description, Discovery and Integration (UDDI) [UDDIwww] description?;
- Other options could be working with non-standard networking architectures, e.g., the user of agents that "wander" around a given network and explore the tomography or the "topology" of the sensed values; and
- From time to time, it might be necessary to reassign tasks to the WSN, i.e., to provide all its SNs with new tasks and new operating software.

8.2.3 Physical Layer

When it comes to protocols that are ideally suited to the requirements of WSNs, very little work has been done. When it comes to radio transmission, the most important concern is how to transfer energy in the most effective manner possible, taking into consideration all of the

expenses that are associated with it (such as possible retransmissions, overhead, and several other things).

Some strategies for modulation that are efficient in terms of energy consumption have been explored in [Schurgers2001]. In [Gao2001], the hardware component of CDMA in sensor nodes is taken into consideration, and modulation challenges are explained. In the document [Shih2001b], there is a discussion of the design of communication protocols that are based on the physical layer.

In light of the work that is being done at the IEEE level (for example, the IEEE 802.15.4 standard), as well as the little research that has been conducted in this field, we have decided not to delve into the specifics of the physical layer for sensor networks' implementation. However, we would like to point out that this is a very significant matter that will require serious study from both the academic community and the business sector.

8.3 MAC Layer

The MAC and the routing layers are the most active research areas in WSNs. Therefore, an exhaustive discussion of all schemes is impossible. However, most of the existing work addresses how to make SNs sleep as long as possible. Consequently, these proposals often tend to include at least some aspects of TDMA. The wireless channel is primarily a broadcast medium. All nodes within radio range of a node can hear its transmission.

This can be used as a unicast medium by specifically addressing a particular node and all other nodes can drop the packet they receive. There are two types of schemes available to allocate a single broadcast channel among competing nodes: Static Channel Allocation and Dynamic Channel Allocation.

- Static Channel Allocation: In this category of protocols, the bandwidth is split into N equal sections in frequency (FDMA), in time (TDMA), in code (CDMA), in space (SDMA), or in schemes such as OFDM or ultra-wideband. This occurs when there are

N network nodes (SNs). Due to the fact that every SN is given its own private section, there is either no interference or very little interference between several SNs. The performance of these protocols is exceptional in situations where there are only a limited and consistent number of SNs, each of which has a buffered (large) load of data;

- Among the protocols that fall under the category of dynamic channel allocation, there is no predetermined allocation of bandwidth assigned. In situations where the number of active SNs is subject to dynamic changes and data becomes bursty at random SNs, the use of a dynamic channel allocation method is the most recommended course of action. These are systems that are based on contention, in which SNs compete for the channel at times when they have data while simultaneously minimising collisions with the transmissions of other SNs. The simultaneous networks (SNs) are compelled to retransmit data whenever there is a collision, which results in an increasing amount of energy being wasted and an infinite delay. Protocols like as CSMA (both persistent and non-persistent, etc.) are typical examples.

As we will see in a moment, after clusters have been constructed in a hierarchical clustering model, it is ideal to maintain a constant number of nodes inside the cluster. Furthermore, when hierarchical clustering is carried out, the number of nodes that are included within each cluster is not kept at a high level. Therefore, it is possible that some of the static channel allocation systems might be more suitable. There has been research done on the application of TDMA for wireless sensor networks. Using this method, every node sends data to the cluster head in its designated slot, and at all other times, the radio on that node may be turned off, which allows for significant energy savings.

Since the data packets are of a predetermined size, the nodes are able to employ nonpersistent cross-protocol multiple access (CSMA) when it is not possible to use TDMA. TDMA is an appropriate protocol for networks that are either proactive or reactive in nature. By assigning a slot to each node in proactive networks, we are able to prevent collisions from occurring.

This is because the nodes in these networks broadcast at regular intervals. Because neighbouring nodes in reactive networks contain data that is comparable to one another, once there is a quick change in any characteristic that is being sensed, all of the nodes will immediately respond to the change.

Collisions will occur as a result of this, and it is likely that the data may never be sent to the user in a timely manner. Because of this, time division multiple access (TDMA) is utilised such that every node is assigned a slot, and they only transmit inside that slot. It is preferable to the energy consumption that is incurred as a result of dynamic channel allocation systems, despite the fact that this would result in an increase in latency and the possibility of many slots being vacant.

In order to prevent collisions between different clusters, CDMA can be utilised. Despite the fact that this results in a greater amount of data being communicated for each bit, it affords the possibility of numerous transmissions utilising the same frequency. For the purpose of avoiding intra- and inter-cluster collisions in sensor networks, the use of TDMA/CDMA combination has been cited as having a variety of different advantages.

8.3.1 Design Issues

As with MAC protocols for traditional MANETs, WSNs have their own inherent characteristics that need to be addressed. Below we discuss some of the most important ones involved in the design of MAC protocols for WSNs.

8.3.1.1 Coping up with Node Failure

When many SNs have failed, the MAC and routing protocols must accommodate formation of new links and routes to other SNs and the BS. This may require dynamically adjusting transmit powers and signaling rates on the existing links, or rerouting packets through regions of the network with higher energy level.

8.3.1.2 Sources of Resource Consumption at the MAC Layer

There are several aspects of a traditional MAC protocol that have negative impact on wireless sensor networks including:

- **Collisions -** When a transmitted packet is corrupted due to a collision, it has to be discarded. The follow-on retransmission increases the energy consumption and hence increases the latency;
- **Overhearing -** SNs listen to transmissions that are destined to other SNs;
- **Control packets overhead -** Sending and receiving control packets consume energy and reduce the payload. This overhead increases linearly with node density. Moreover, as more SNs fail in the network, more control messages are required to self configure the system, resulting in more energy consumption;
- **Idle Listening -** Waiting to receive anticipated traffic that is never sent. This is especially true in many sensor network applications. If nothing is sensed, SNs are in the idle mode for most of the time.

8.3.1.3 Measures to Reduce Energy Consumption

One of the most cited methods to conserve energy in sensor networks is to avoid listening to idle channels, that is, neighboring nodes periodically sleep (radio off) and auto synchronize as per sleep schedule. It is important to note that fairness, latency, throughput and bandwidth utilization are secondary in the WSNs.

8.3.1.4 Comparison of Scheduling & Reservation-based and Contention-based MAC Design

There is a method of MAC design for wireless sensor networks (WSNs) that is based on reservation and scheduling. For instance, TDMA-based protocols are more energy-efficient than contention-based protocols such as the IEEE 802.11 DCF. This occurs as a result of the

radio's duty cycle being raised, as well as the absence of contention-induced overhead and collisions. The establishment of the cluster, the management of communication between the clusters, and the dynamic adaptation of the TDMA protocol to variations in the number of nodes in the cluster in terms of its frame length and time slot assignment are still the most significant issues.

8.3.2 MAC Protocols

As it is very impractical to recharge the batteries, wireless sensor networks are designed to function for an extended period of time. The majority of the time, however, when there is no sensing taking place, nodes are in an idle state. Measuring has showed that the amount of energy that a typical radio uses in the receiving mode is comparable to the amount that it consumes in the idle state. As a result, it is essential that nodes have the capability to function in low duty cycles.

As far as the MAC layer is concerned, some of the most current and pertinent studies in this area include those that are conducted by the field of STEM. Due to the fact that many of these protocols have similar qualities, we will only be discussing those that are the most prominent and essential in order to comprehend the others in subsequent sections. In addition, it is essential to keep in mind that more conventional MAC schemes, such as FDMA, TDMA, CDMA, SDMA, and a mix of these, can also be utilised. On the other hand, because these methods are already well-known, we will not be discussing them.

8.3.2.1 The Sensor-MAC

Additionally, the Sensor-MAC (S-MAC) protocol [Ye2002] investigates design trade-offs for the purpose of energy conservation at the MAC layer. The following causes of radio energy consumption are reduced as a result of this: collision, control overhead, overhearing needless traffic, and idle listening. In order to implement S-MAC, all of the SNs are put into a low-duty-cycle mode, which consists of listening and sleeping at regular intervals.

When SNs are listening, they adhere to a contention rule in order to get access to the media. This rule is comparable to the DCR that is used by IEEE 802.11 Instead of sleeping on their own at random, SNs in S-MAC make an effort to communicate and coordinate their sleep patterns with one another.

Before each SN begins the periodic slumber, it is necessary for it to select a timetable and communicate it to its neighbours at the same time. To prevent clock drift over an extended length of time, every SN sends out a SYNC packet that contains its schedule on a periodic basis. S-MAC encourages neighbouring SNs to pick the same schedule, although it is not a necessity for them to do so.

This is done in order to decrease control overhead requirements and simplify broadcasting. In the beginning, an SN will listen for a certain amount of time, which is at least the amount of time required to deliver a SYNC packet. It will follow the schedule of any neighbour that sends it a SYNC packet, and it will do so by adjusting its own schedule to be the same as the neighbor's schedule. In the event that this does not occur, the SN will independently select a timetable following the initial listening period.

It is possible that two neighboring SNs have two different schedules. If they are aware of each other's schedules, they have two options:

- Following two schedules by listening at both scheduled listen time;
- Only following its own schedule, but transmitting twice as per both schedules when broadcasting a packet.

If the listen intervals of the two SNs do not overlap in any way, it is possible that the two SNs will not be aware of the presence of each other under certain circumstances. S-MAC allowed each SN to periodically do neighbour discovery, which means listening for the entirety of the SYNC period, in order to detect unknown neighbours on a network. This was done in order to fix the problem.

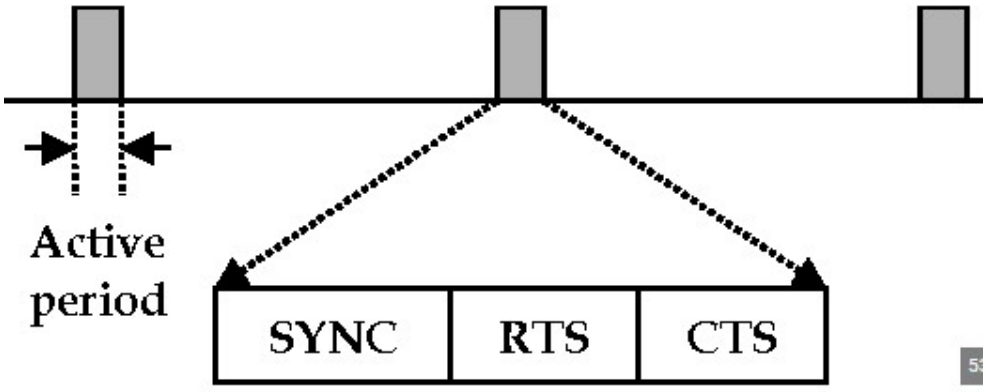

Fig.: 8.4 Low-duty-cycle operation in S-MAC

Source: A secure zone-based routing protocol for mobile ad hoc networks data collection and processing through by Niroj Kumar Pani (2009)

timetable that is distinct. A representation of the low-duty-cycle operation of each SN is shown in Figure 8.4. There are two distinct components to the listen interval, one for SYNC packets and the other for data packets. Before each SYNC or data (RTS or broadcast) packet is sent, there is a contention window for randomised carrier sense time. This window is known as the contention window. SN A, for instance, wishes to transmit a unicast packet to SN B, therefore it first performs carrier sensing during the period when B is listening for data. Node A will transmit a request for service (RTS) to node B if the carrier sense indicates that the channel is idle. Node B will then respond with a CTS if it is prepared to accept data.

Following that, they will make advantage of the typical period that they are sleeping in order to send and receive real data packets. The RTS/CTS protocol is not utilised by Broadcast because of the possibility of collisions occurring on repeated CTS replies. As a result of the fact that a node may only begin communicating when the intended recipient is listening, low-duty-cycle operation decreases energy consumption; however, this advantage comes at the expense of increased latency. In order to lessen the amount of time that a multi-hop transmission takes to complete, S-MAC devised an adaptive listen strategy.

The fundamental concept is to allow the node that is responsible for overhearing the transmissions of its neighbour (preferably simply RTS or CTS) to wake up for a brief amount of time at the conclusion of the transmission. If the SN is the next-hop node, then its neighbour is allowed to quickly send the data to it, rather than waiting for its planned listen time. This is because the SN is the next-hop node. It is possible for the SN to return to sleep mode if it does not receive any information while it is engaged in adaptive listening.

Authors Details

ISBN: 978-81-19534-43-2

Dr. Jasleen Kaur, is working as Assistant Professor in Post Graduate Department of Computer Science at Gujranwala Guru Nanak Khalsa College Ludhiana, Punjab, India. She received her Ph.D. degree in Sensor Network from the CT University, Ludhiana, Punjab, India. Her research interests include deep learning, sensor network and information security. She has around 20 years of teaching and 6 years of research experience. She has published 5 research papers in reputed International Journals and Conferences.

Dr. Balkar Singh, is working as Assistant Professor in Post Graduate Department of Computer Science at Gujranwala Guru Nanak Khalsa College Ludhiana, Punjab, India. He received his Ph.D. degree in Image Processing from the Thapar Institute of Engineering and Technology, Patiala, Punjab, India. His research interests include deep learning, image processing, sensor network and information security. He has around 12 years of teaching and 8 years of research experience. He has published 15 research papers in reputed International Journals and Conferences.

Dr. Anuj Kumar, is an Assistant Professor in the Department of Computer Science and Engineering at the School of Engineering and Technology, Sharda University, Uttar Pradesh, India. He holds a Postgraduate Degree (M-Tech in Software Engineering) from G.B.U. G.B.Nagar, and a Doctorate Degree (PhD in Computer Science and Engineering) from A.K.T.U. Lucknow, India. With a strong background in teaching and industry exposure, he is actively engaged in research in the fields of Software Testing, AI, and Machine Learning.

Dr. Ram Paul, is working as an Assist. Professor in Amity School of Engineering and Technology, Amity University, Uttar Pradesh, Noida. He received his Ph.D. degree in Image Processing from the Thapar Institute of Engineering and Technology (formly Thapar University), Patiala, Punjab, India. His research interests are Digital Image Processing, Machine Learning and Mobile Communication. He completed his M.Tech(CSE) degree from the Guru Jambheshwar University of Science & Technology, Hisar, Haryana, India in 2005. He has around 18 years of teaching and 8 years of research experience. He has published 19 research papers in reputed International Journals and Conferences.

Xoffencer International Publication
838- Laxmi Colony. Dabra,
Gwalior, Madhya Pradesh, 475110
www.xoffencerpublication.in

MRP: ₹ 550/-

ISBN
9 788119 534432