Wireless Sensor Network- Challenges and Possibilities

Amit Rathee
Department of CSE
PIET, Panipat, India

Randeep Singh
Department of CSE
IEC University, HP, India

Abhishilpa Nandini
Department of CSE
IEC University, HP, India

ABSTRACT

Wireless Sensor Network (WSN) is the current research field in computer science & has growing use in day to day life. As a new technology, it has several research challenges and vast opportunities for the researchers. This paper highlights WSN, its architecture, challenges, applications and classification of various protocols concerning it. It also classifies various security protocols to make WSN a secure network.

General Terms

Wireless Sensor Network, Survey Paper.

Keywords

Sensor Network, WSN, Routing, Security, Key Management, MAC, Localization.

1. INTRODUCTION

A wireless sensor network is consisting of a large number of spatially distributed devices called sensor nodes that are densely deployed inside the environment which we want to sense or close to it. The position of sensor nodes in network need not be engineered or predetermined i.e. nodes are random deployment in inaccessible terrains or hazardous environments. In WSN we generally have a unique node called Base Station (BS) and all other nodes will send data to it either directly or through multihop communication. A BS may be either fixed or mobile node and provides WSN connectivity to outside world. It is generally more capable than other nodes in the network. A typical structure of a WSN and node structure is shown in figure 1.

Some of the most important application areas of sensor networks include military, natural calamities, health, and home.

When compared to traditional ad hoc networks, the most noticeable features of sensor networks is that, they are limited in power, computational capabilities, and memory. Also replacing battery is not always feasible in WSN. Hence optimizing the energy consumption in WSNs has recently become the most important to make it sustain long.

A typical WSN is designed on following communication standards [37] given by Working Group for data communication devices:

- IEEE 802.15.4 (LR-WPANs) standard for low cost, short-range, low power, and low data-rate communication for sensor networks. This standard is mainly designed for maximizing battery life. This standard has layered architecture and make use of standards such as ZibBee, 6LowPAN, WirelessHART & ISA100.11a in upper layers.
- IEEE.802.15.4a is anUltra-Wideband RF-based communication technology.
- Bluetooth & Bluetooth low energy (BLE) for WPAN & is currently managed by the Bluetooth Special Interest Group.
- Z-wave standard for remote control applications and is given by Zensys.
- ANT Technology for ultra-low power networking applications.
- Dash7 is anultra-low power, and long-range wireless sensors networking technology based on the ISO 18000-7 open standard.

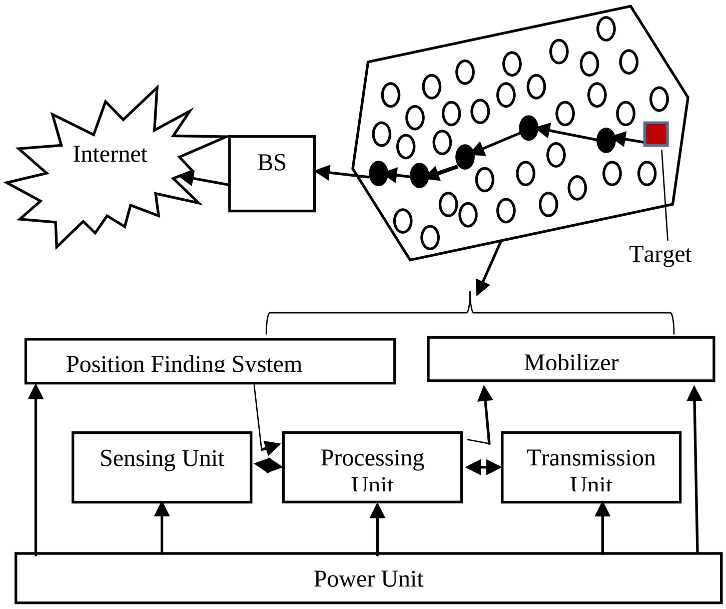

Figure 1: Typical Structure of a WSN and Node Components

2. CHARACTERISTICS OF WSN

The important characteristics of a typical WSN which differ it from other wireless adhoc networks can be summarized as below:

- Limited computational capacity.
- Limited energy resources.
- Limited memory capacity.
- Frequently changing infrastructure as against adhoc networks due to mobility.
- Problem in assigning and maintaining unique global identification due to very large number of nodes present.
- Higher chances of failure of nodes due to harsh environment and limited energy capacity.
- More densely placed nodes.

3. RESEARCH AREAS IN WSN

As we know that WSN is very latest and sensitive topic of today's research. So we have identified various research areas in it and they can be summarized as below:

- Routing Protocols for WSN.
- Energy/Lifetime enhancement for WSN.
- Key Management in WSN.
- Security Protocols for WSN.
- Data Gathering & Processing in WSN.
- Quality of Service for WSN.
- Deployment of nodes in WSN.
- Clustering of nodes in WSN.
- MAC protocols for WSN.
- Real time delivery of data for multimedia application in WSN.
- Reliability of WSN.
- Congestion Control in WSN.

4. ROUTING PROTOCOL SURVEY IN WSN

Usually, the WSNs are classified as data-centric networks because of the nature of the network that data is usually requested from sensor nodes on the basis of certain attributes relevant to the environment concerned (i.e., Attribute-Based Addressing). So, routing in WSN is very challenging because of relative large number of sensor nodes (so, traditional IP based routing protocols can't be applied), generally unique flow of sensed data to a single Base Station (BS) in most applications (multicast or peer to peer), less mobility of nodes as compared to other traditional wireless networks, redundancy in sensed data, sensor nodes are highly constrained in terms of energy, processing & storage and finally sensor networks are application-specific.

Due to these differences many new algorithm/protocols have been proposed to handle routing in WSN. All the algorithms can be classified into following categories based on following parameters [1]:-

1. **Network Structure/ Topology-** In this classification scheme, the routing is based on the manner in which the nodes are connected they route the information through the network. Based on network structure all the routing protocols can be classified as Flat/ Data Centric, Hierarchical and location-based. In flat network topology, all nodes play the same role i.e. they have same capability & no hierarchy is present among nodes, while in hierarchical structure, protocols try to cluster the nodes so that cluster heads can do some aggregation and reduction of data in order to save energy. Location-based protocols try to utilize the position information of sensor nodes to relay the data to the desired regions rather than the whole network in order to save energy. Among all topologies based routing protocols, hierarchal routing protocol technique is more popular regarding the power saving of sensor nodes.
2. **Protocol Operation/ Communication Model used-** Based on this parameter routing protocols can be classified as multipath-based, query-based, negotiation-based, QoS-based and coherent-based.
3. **Route Finding-** Based on how the source finds its route to destination node to deliver data all routing protocols can be classified as proactive, reactive, and hybrid. In proactive protocols, all network routes are calculated before they are really needed. So, they are also known as table-driven protocols.While in reactive protocols, all data routes are calculated on demand i.e. when needed. Hybrid protocol schemes combines the best of both proactive & hybrid schemes. When sensor nodes are static, it is preferable to have table-driven routing protocols rather than reactive protocols because a significant amount of energy is wasted in route discovery and setup phase of reactive protocols each time we want to send data.
4. **Cooperation-** Another classification of routing protocols is known as cooperative. In cooperative routing scheme, the nodes sends data to a central node where data can be aggregated and it may be subject to further processing there, hence reducing route cost in terms of energy use for sending data.

We mainly study routing protocols based on network structure and figure 2 shows the classification of WSN routing protocols based on network topology with examples.

Flat Routing- In flat networks, each node typically plays the same role and sensor nodes collaborate to perform the sensing task. We know that due to the large number of WSN nodes, it is not feasible to assign a global identifier to each node. So, this consideration has led to data-centric (DC) routing, where the BS sends queries to certain regions and waits for data from the sensors located in the selected regions. Since data is being requested through queries, attribute-based naming is necessary to specify the properties of data. The main idea of the DC is to combine the data coming from different sources by eliminating redundancy, minimizing the number of transmissions; thus saving network energy and prolonging its lifetime. In DC protocols all communications are only neighbor to neighbor,no global identification and random deployment.

Hierarchical Routing- The main aim of hierarchical routing is to efficiently maintain the energy consumption of sensor nodes to increase system scalability, lifetime by using multi-hop communication and maintaining various clusters. In each cluster the higher energy node is elected as cluster head & is assigned the responsibility of data aggregation and fusion, while low-energy nodes can be used to perform the sensing in the proximity of the target. The main idea is to decrease the number of transmitted messages to the sink. Cluster formation is typically based on the energy reserve of sensors and sensor's proximity to the cluster head.

Location-Based Routing- Location based protocols plays important role in energy saving because such protocols are based on the location of nodes and hence always measures distance between the nodes. The distance between nodes is estimated by the signal strength received from those nodes or by GPS means. More the distance more will be the energy consumption. In this scheme, sensor nodes are scattered randomly in an area of interest and addressed by their geographic position. Since this scheme requires specific hardware components and other significant computational Overhead so this approach cannot be easily used in resource-constrained wireless sensor networks.

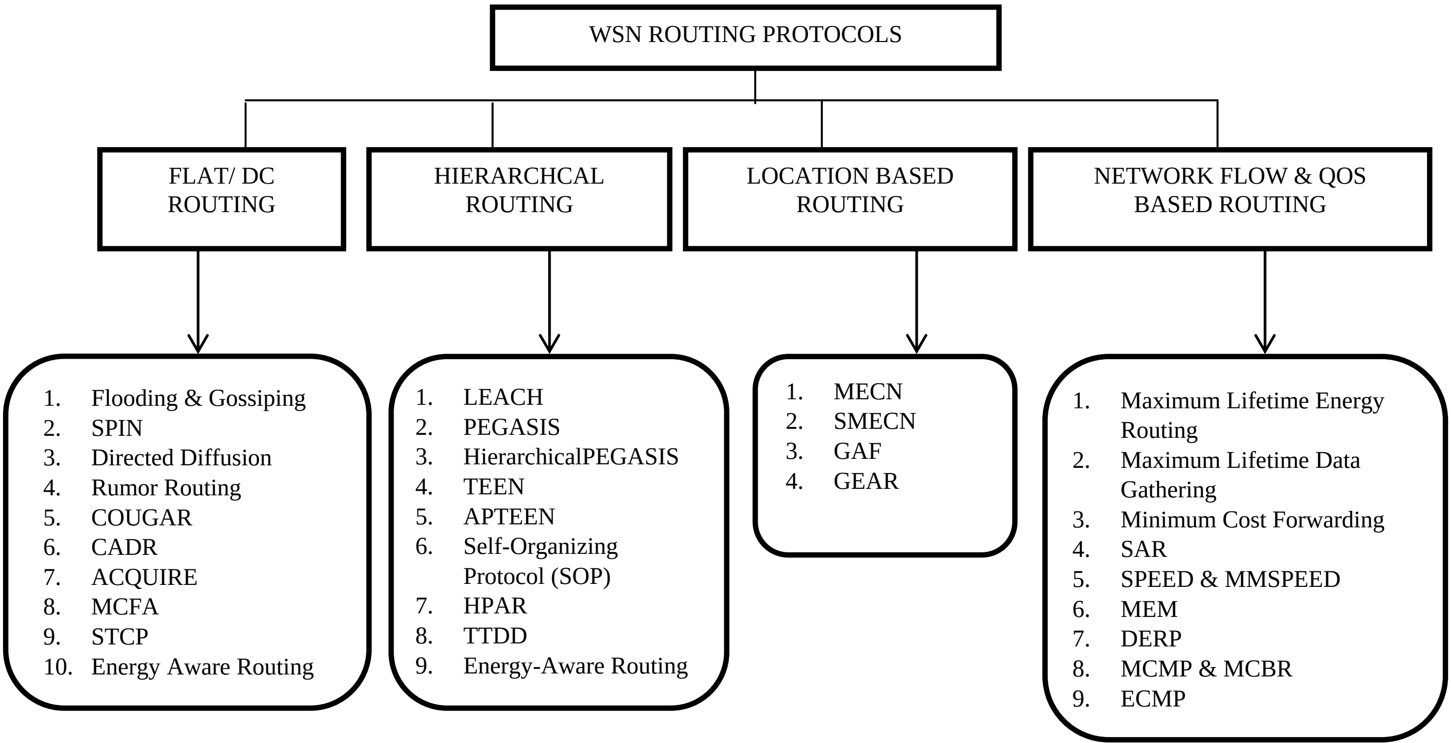

Figure 2: WSN Routing Protocol Classification

Network Flow & QoS-Based Routing- In QoS-based routing protocols, the network have to balance between energy consumption and data quality. In particular, the network has to satisfy certain QoS metrics (delay, energy, bandwidth, etc.) when delivering data to the BS.

5. CLUSTERING IN WSN

Cluster formation in another major research area in WSN because it helps maintain scalability and also provide energy efficiency. Clustering involves grouping of sensor nodes based on transmission range proximity to each other and electing one of the nodes in the group as leader called Cluster Head (CH) so as to enhance lifetime of the network. Clustering also reduce routing table size and reduce the bandwidth requirements because all intra cluster communication takes place between few elected CH's only rather than all the sensor nodes. A CH is generally a more capable node in terms of resources and processing capability and is generally less mobile so as to maintain the cluster structure. The diameter size of the clusters determines the control architectures as single-hop clustering and multihop (K-hop) clustering. In single-hop clustering every member node is never more than 1-hop from CH. Thus all the member nodes remain at most two hops space left from each other within a logical cluster. In multi-hop clustering, nodes are allowed to be present in serial k-hop distance to form a cluster. The clustering technique has following objectives:

1. Load Balancing by efficiently processing and aggregating cluster data.
2. Fault-tolerance by reorganizing cluster if one of the CH fails.
3. Clusters must be made so as to reduce delay and increase connectivity of various clusters.
4. Minimum number of cluster in the network.
5. Maximize network lifetime.

The various distributed clustering algorithm's classification [2] is shown in figure-3& there main aim is to maintain scalability of the network. In *Variable Convergence Time Algorithms* time is considered as significant factor in the convergence of the network & various example protocols are also shown in the figure-3. In *Constant Convergence Time Algorithms* the network converges after a fixed number of iterations irrespective of the size of the network & various example protocols are also shown in the figure-3.

Each of the clustering algorithm must identify various clustering parameters viz cluster count, intra cluster communication, Nodes & CH mobility, cluster formation methodology and CH selection criteria. There are two cluster formation methodologies- static & dynamic. In static methodology, the CH's are predefined and fixed while in dynamic methodology, the CH's can change over time based on the energy left of current CH.

6. MAC PROTOCOLS IN WSN

Efficient MAC protocols designs are another major research area in WSN. We know that WSN are energy constraints and wireless radio is the most energy consuming unit in a node. The radio of a node can be in four states: transmit, receive, idle and sleep. Each state is having different degree of energy consumption. The MAC layer provides most control of the transceiver of a node so that all nodes will efficiently share common medium by switching the radio on and off. The existing MAC protocols for Adhoc network cannot be used for WSN because they result in more collision of packets, overhearing of nodes for packets, extra overhead in terms of

Control Packets (RTS/ CTS Signals), idle listening and over emitting due to mismatch in Transmission rates.

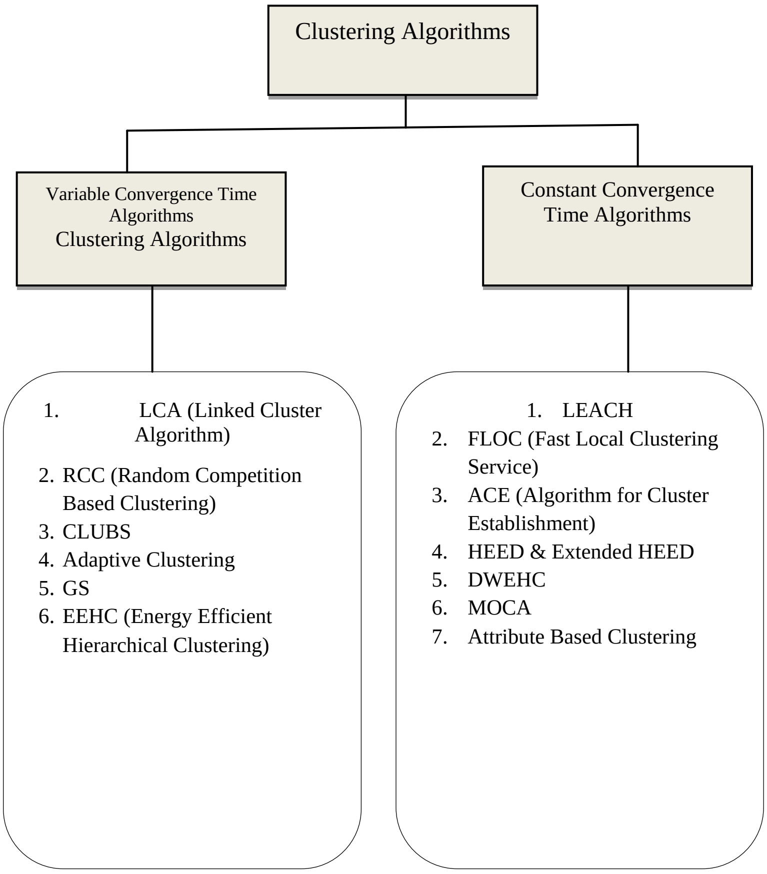
Clustering Algorithms
Variable Convergence Time Algorithms
Clustering Algorithms
Constant Convergence Time Algorithms
1. LCA (Linked Cluster Algorithm)
2. RCC (Random Competition Based Clustering)
3. CLUBS
4. Adaptive Clustering
5. GS
6. EEHC (Energy Efficient Hierarchical Clustering)
1. LEACH
2. FLOC (Fast Local Clustering Service)
3. ACE (Algorithm for Cluster Establishment)
4. HEED & Extended HEED
5. DWEHC
6. MOCA
7. Attribute Based Clustering

Figure 3: Clustering Algorithm Classification

All these factors results in higher energy consumption reducing WSN lifetime. So, to increase network lifetime by reducing energy consumption by removing one or more above mentioned overhead, an efficient MAC protocols must have following characteristics [3]:

- Energy efficiency- because WSN has battery constrained sensor nodes so, they cannot spend their precious energy to transmit and receive many control packets. Thus the MAC protocol should be designed in such a way that it consumes energy efficiently to increase network lifetime.
- Scalability and Adaptability- WSN protocols should be adaptable for the changes such as network size, density of node and network topology because some nodes may stop functioning due to battery drain or link failure or due to any other environmental problems.
- Latency- as Latency determines the network speed& indata processing inside the network, several kinds of delays typically occurs in WSN. In a network, small delay times result in low latency network connection, whereas a high latency connection experience from long delays which is generally not desired.
- Throughput- the total amount of data which flows through the network refers to the network's throughput. Throughput of the WSN should be high.
- Bandwidth utilization- as data rate in networking is known as bandwidth. So, we should not restrict speed of a network with only the network bandwidth, rather, the network should support higher bandwidth utilization.
- Fairness among sensor nodes– since WSN is mostly used for critical applications, so, distribution of resources in a network must be done fairly. Fairness among sensor nodes is also important to increase network lifetime.

According to the literature study [3], we can divide the MAC layer WSN protocols in four major categories- Scheduling/ TDMA Based, Collision Free/ Traffic Adaptive, Contention Based and Hybrid Schemes. Figure 4 shows the classification along with examples of each.

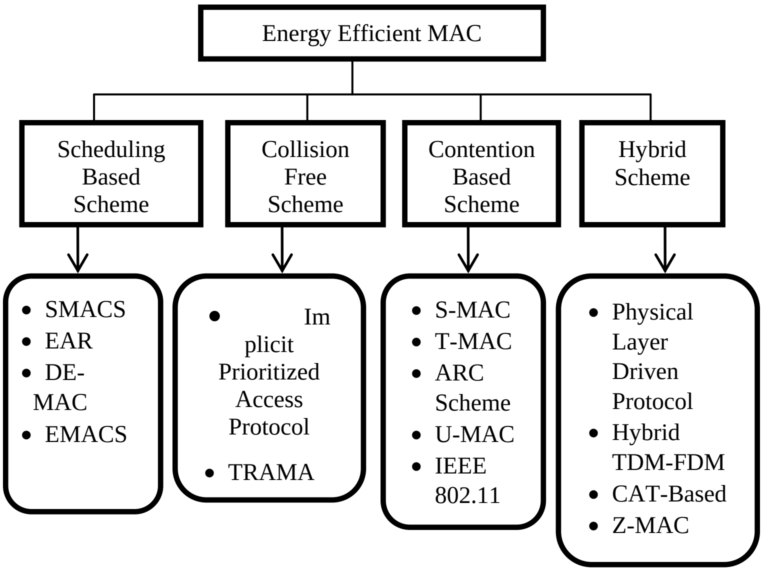

Figure4: MAC Protocols for WSN.

Scheduling Based Scheme- The main idea of this scheme is to decide the time at which a node can transmit the data. This scheme allows multiple nodes to transmit simultaneously without collision/ interference. In this scheme time is divided into number of slots and slots are further grouped into frames. In each frame every node is assigned at least one slot for transmitting its data. The scheduling schemes have two implementations- static & dynamic. In static scheme each station is assigned a fixed slot in frame. This scheme is easy to implement but it result in bandwidth wastage if the node does not want to send data. Another scheme is dynamic, in which slots are assigned randomly to only those stations which needs to send data. This is generally done by a central node which broadcast a request to determine which of the stations wants to send data. This scheme avoids collision and hidden terminal problem efficiently. The various TDMA based protocols in literature are: µ-MAC, SMACS (Self-Organizing Medium Access Control for Sensor Networks), EAR (Eavesdrop-And-Register), DE-MAC (Distributed Energy-Aware MAC), EMACS (Energy Efficient MAC Protocol for Sensor Networks) and SPARE-MAC.

Contention-Based Scheme- This scheme is based on CSMA or CSMA/CA technique. In this scheme there are no central coordinating station but each station simply sense the medium before sending data, and the "sense before sending" principle reduces collision but it never eliminates it. That is, collision can still be there and the performance is directly related with it. So, performance decreases if collisions increases and vice versa. The various protocols using this scheme are S-MAC (Sensor MAC), T-MAC (Timeout MAC), ARC (Adaptive Rate Control), extended IEEE 802.11, Sift, U-MAC (Ultra-Wide Band MAC) etc.

Collision Free Scheme- In this scheme, the medium is divided into sub channels based on time, frequency or orthogonal codes. Further, each node is assigned a unique sub channel which avoids collision and also allows nodes to share medium. The various protocols using this scheme are Implicit Prioritized Access Protocol, TRAMA etc.

Hybrid Scheme- This scheme is the combination of contention-based MAC and TDMA-based MAC. In this, we take all the advantages of both of these methods and make a better solution called hybrid MAC. The hybrid protocols divides the communication channel into two parts, one for control packets and other for data packets. In channel control packets data is sent in the random access and in data packets data are transmitted in the scheduled channel. The hybrid protocols can save much higher energy and support better scalability and flexibility in comparison to above two methods. The various hybrid protocols are CAT Based, A-MAC, IEEE 802.15.4 and Z-MAC

7. ATTACKS &SECURITY PROTOCOLS FOR WSN

Since, wireless network is generally deployed in hostile environment. So, it is very much prone to attack which results in malfunctioning or destruction of network & its services. So, now a day's detecting and protecting WSN is another big research area. Various cryptographic schemes can be used to protect data, but due to constraint resources all such schemes are not always feasible. The goal of security services in WSNs is to protect the information flowing through the network and the critical resources of the system from attacks and misbehavior. The security requirements in WSNs include [4]:

- **Availability**, it ensures that the expected network services are available even in the presence of denial-of-service attacks.
- **Authorization**, it ensures that only the authorized sensors are always involved in providing information to network services& not the unauthorized sensor nodes
- **Authentication**, which ensures that the communication among nodes is genuine, that is, a malicious node cannot masquerade as a trusted network node.
- **Confidentiality**, which ensures that a given message cannot be understood by anyone other than the desired recipients.
- **Integrity**, it ensures that messages sent from one node to another in a network, is not modified by malicious intermediate nodes.
- **Nonrepudiation**, it says that a node in the system cannot deny sending of a message that it has sent earlier.

- **Freshness**, which means that the data is the latest and ensures that no adversary can resend the old messages later in the network.
- **Secrecy**,means, as new sensors are added to the system and old sensor nodes fail, there should be forward and backward secrecy should also be considered:

  Forward secrecy: a sensor should not be able to read any future messages after it left the network.

  Backward secrecy: a joining sensor should not be able to read any previously transmitted message.

The various threats and attacks in WSN can be classified into [4] following three categories as shown in figure-5.

Internal Attacks: these are mainly done due to the compromised nodes. These compromised nodes continuously seek to disrupt or parallelize the network. Based on kind of activity performed by attacker, it can be further classified as:

Outside Attack- in which, an attacker can replace/introduce new malicious node from outside.

Inside Attack- in which, an attacker can capture any node; reprogram it, to act as malicious node.

External Attacks: in these attacks, the attacker node is not an authorized participant of sensor network. Based on the behavior of attacker node, it can be classified as:
Passive Attack- it include eavesdropping on or monitoring packets exchanged within a WSN. It involves only unauthorized listening to the routing packets. Generally, encryption is the standard solution to defend against these attacks.

Active Attack- it involve some modifications of the data steam or the creation of a false stream. Also, itresults in disrupting network functionalities by introducing DOS attacks, Jamming attacks & Power Exhaustion.

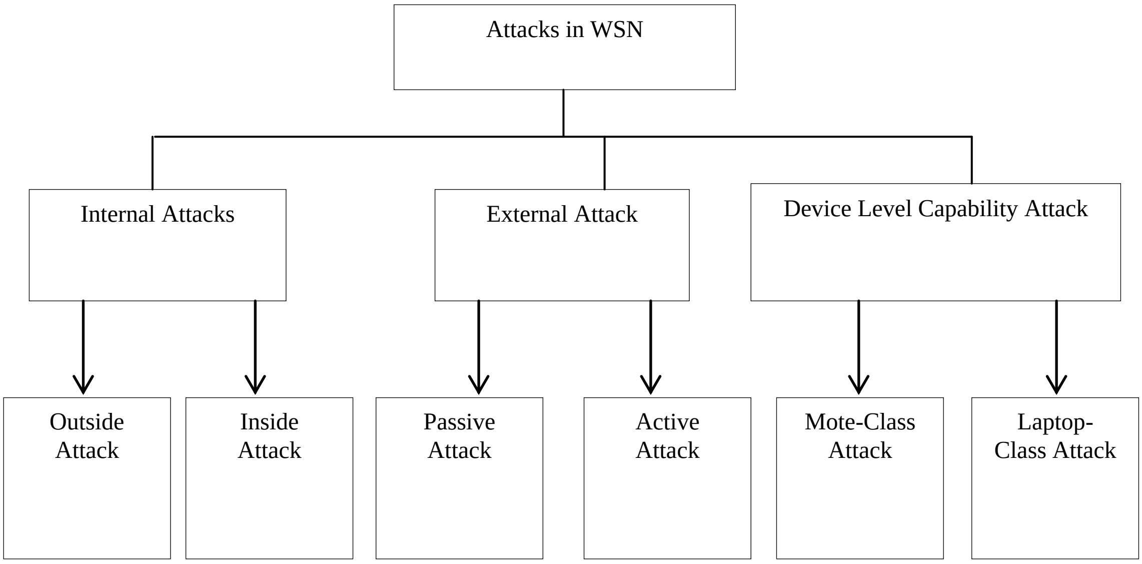

Figure 5: Attack Classifications in WSN

Device Level Capability Attack- this class of attacks is classified based on the capability of the device that is being used for attacking. An attacker may attack the WSN either using a sensor device (Sensor Level) or more powerful laptop device (Laptop Level). An adversary can highly damage the system if he/she uses Laptop Class attack having more powerful computation, storage and battery life.

Beside the above mentioned classifications, an attacker may utilize one or more of the following attack techniquessuch as [5]:

Eavesdropping-in which an attacker silently listen to media for communication between two party and do not modifies the data. It is a passive technique.

Radio jamming- in this attack, the attacker tries to disrupt the communication by sending some radio waves at the same frequency resulting in interference or collisions of packets over network. Jamming can be continuous or intermittent based on the time for which network is kept jammed.

Message's injection- in this the attacker sends many false messages over network in lieu of corrupting the packet data or to simply exhaust network.

Message's replication- in this the attacker capture and resend the same packet many times to same or different sensor and at different times in order to make receiver foolish.

Node compromise (Destruction or theft)- this include physical capturing of a node in order to disrupt network by breaking the communication path or reprogramming a node so that it acts as a spy in network.

Denial of Service (DoS) - in this the attacker will regularly sends packet in order to disrupt services or battery power by using malicious nodes. This is an active type of attack.

HELLO Flooding- we know that HELLO message is used for discovering neighbors. In this type of attack, the attacker uses more powerful nodes to send HELLO messages to far away sensor nodes so that they believe that the malicious node is their neighbor and they will send future packets to it.

Black Hole Attack- in this attack a node tries to become receiver of packets of neighboring nodes by altering their routing table and it will never forward the packets to correct destination.

Selective Forwarding (Gray Hole Attack)- in this attack, the attacker will insert malicious node in the network which tries to change the routing and capture data just like black hole attack but unlike it will selectively forward data (not all) and so difficult to detect.

Wormhole Attack- this kind of attack is done with at least two malicious nodes which have high bandwidth between them either wired or wireless. These malicious nodes will shows other normal nodes that they provide the shorter path to the destination even if they are lying far away in the network. So, the node will forward data to the malicious node which can be captured by attacker easily.

Sinkhole Attack- in this attack the malicious node reside near the base station and it tries to pretend to be closest node to the base station so that other surrounding normal node will update themselves and forward data to the malicious node.

Sybil Attack- in this attack the adversary tries to have multiple identities to other nodes and thus can be in more than one place at single time. Here it tries to be voted as cluster head. A Sybil attack is significant threat to Geographic Routing Protocols.

Infinite Loops- in this attack two or more malicious node tries to circulate packets infinitely in the network in order to exhaust power of the network.

Message Alteration- in this attack the malicious node will capture and change packets on the network. It can add false data or delete data so that packet will become corrupted.

Sleep deprivation torture- in this attack the malicious node will prevent a node from sleeping by sending messages to it or asks for calculation. This is done so that the node will consume its power quickly.

OSI Security Model- OSI is the layered communication model used in WSN. Table-1 shows the various layers, attacks and security mechanism proposed by the model.

Security Mechanisms- beside above OSI Model security methods, various other security techniques are present to secure a WSN from above mentioned attacks. All these security mechanisms and techniques can be categorized as shown in figure-6 below [5]:

Data Partitioning- This is the simplest of security mechanism in which we tries to disguise the attacker by portioning of the whole data into number of packets and sending each packet via different route.Here, the sink node is responsible for joining the received packets to get final data. Here, there are rare chances that the attacker is able to capture all the packets and thus is capable to get only partial information.

The main disadvantage of this technique is that more energy will be consumed in system due to increase in number of communications.

Table-1: OSI Security Model

Layer	Attacks	Countermeasures
Physical	Jamming, Tampering	• Use Spread-Spectrum or frequency Hopping Communication. • Locating jamming and re-routing traffic • Using prioritized transmission schemes to minimize collision. • Using tamper proof locks or coating.
Data Link	Collision, Exhaustion, Interrogation, Unfairness, DoS	• Using TDMA & EC-Codes to minimize collision. • Using Random-Backoffs. • Using rate limiting in MAC admission control. • Using shorter frames to minimize unfairness. • Antireply protection & link layer authentication to mitigate exhaustion/ interrogation. • Jamming identification & mitigating techniques.
Network	Selective forwarding, sinkhole, wormhole, Sybil, HELLO flood attack, routing table alteration	• Encryption & Authentication. • Multipath Routing. • Identity Verification • Bidirectional Link Verification. • Authentication Broadcast.
Transport	Flooding, Desynchro-nization	• Limiting Number of Connections to prevent Flooding. • Authentication of every packet can prevent desynchronization.
Application	Overwhelming Sessions, Path-based DoS, Deluge	-

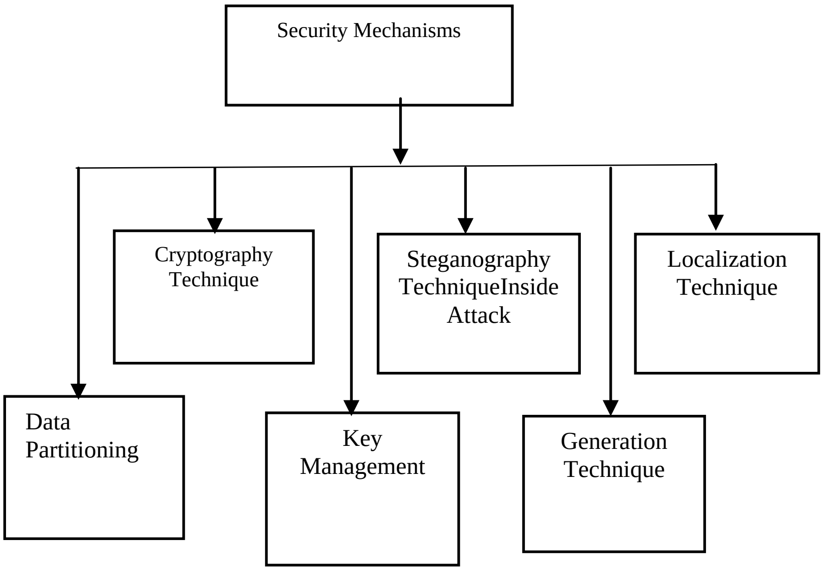

Figure 6: Security Mechanisms in WSN.

Cryptography Technique- It is another security solution available in WSN but only of limited use because of low computing and power resources. The study shows that mostly symmetric key crypto algorithms like AES are used whereas asymmetric key crypto algorithms have limited use and among them ECC shows better performance than RSA in terms of energy consumption.

The main disadvantage of this technique is how we will distribute keys among nodes securely as its success depends upon secrecy of the key only.

Key Management Technique- This technique is related with secure management of key in WSN among nodes. This technique provides more security along with cryptography. As per the literature key can be managed in following four ways:

1. The simplest idea is to have a global key which is preinstalled in nodes before deployment which is used for both encryption & decryption. However, it provides one point failure of the whole system if somehow, attacker able to know the key.
2. Another scheme is to have unique key between each pair of nodes. So, if there has n nodes in system then each node needs to maintain (n-1) unique keys.
3. We can also use keys group wise e.g. we can use unique key per cluster or group. This scheme reduces the total no. of unique keys managed per node.
4. Each node in the network can also be given unique key which it uses for encryption of data and that key is only known to the sink which finally decrypts data.

Steganography Technique- this security mechanism is based on hiding the data in the PHY layer of the 802.15.4 protocol by using the noise of the signal for creating a stenographic channel.

Generation Technique- the main idea of this scheme is that the sink node will generate and distribute unique key in regular intervals during its lifetime and this key acts as a proof of identity that the particular node belongs to the network. Here, if the attacker introduce new node which do not have the generated key than it will not be accepted by network. This is simplest technique to deploy but only provides security against outsider node but not to internal compromised node.

Localization Technique- this scheme is mainly used in network which has GPS enabled nodes& each node is responsible for monitoring a particular area. The idea is that when a new node enter into the network and register itself for particular geographical area to which it can hear by generating beacons than votes for the area will increase & we can identify the intruder node.

8. NODE DEPLOYMENT IN WSN

Node deployment in another important issue in WSN which affects network effectiveness and lifetime. It means placing nodes in actual environment and it is highly application dependent. The node deployment techniques [6] can be broadly divided into two categories: Random Deployment (RD)& Planned Deployment (PD). RD is the simplest deployment technique which involves dropping the sensor nodes by means of Aircraft. Such technique is mostly used for hostile environment, but it can create coverage problems and also results in more energy consumption if nodes need movement after dropping. PD is the most preferable technique in WSN which involves selectively deciding the locations of the sensor nodes to optimize design constraints such as maximizing coverage, minimize power consumption, strong network connectivity etc. The various PD protocols are based on the following four algorithms:

1. **Genetic-based Algorithm-** the aim of these algorithms is to optimize the layout of WSN. Such algorithms make use of GA’s to find position of the nodes such that network has maximum coverage, optimized number of nodes placed to cover whole area and keeping the nodes far away from hostile environment. One such scheme is MOGA (Multi-Objective GA) which assumes that each node has same communication and sensing range. The final position is based on the Deployment Vector (DV), which contains the coordinates of each sensor:

   DV=[x1, y1, ----------, xn, yn]

   After this Rank-based fitness assignment is used in the algorithm to rank each DV according to its area coverage and lifetime. Other such GA based scheme is

Maximum Coverage Sensor Deployment Problem (MCSDP).

2. **Computational Geometry-based Algorithms-** the computational geometry (CG) based algorithms make use of mathematical techniques called Voronoi Diagram (VD) & Delaunay Triangulation (DT) to effectively evaluate coverage area and detection of coverage holes. One example that make use of CG structure is *Bidding Protocol* which consider WSN as combination of both static and mobile nodes. The mobile nodes acts as servers that are used to heal coverage holes detected by static sensors based on their locally constructed Voronoi cells. In each iteration of the protocol, every mobile sensor is assigned a base price, which is proportional to the size of the coverage hole it would leave behind if it moved to another location. Static sensors with detected holes in their Voronoi cells estimate the size of the hole and the candidate position for a mobile sensor to move to in order fill that hole. This information is broadcast by the static sensor in the form of a single parameter called a bid, which is essentially proportional to the size of the coverage hole detected. A mobile sensor node receiving multiple bids chooses the highest one and relocates to heal the biggest coverage hole, provided that the bid is higher than its base price. The protocol terminates when there are no more bids broadcasted in the network higher than the base prices of the mobile sensors.

   Another such scheme is Minimax, Centroid and Dual-Centroid.

3. **Artificial Potential Fields-based Algorithms-** these algorithms make use of mathematical concept called Artificial Potential Field (APF) of Virtual Forces (VF). In these algorithms mostly the nodes are considered as mobile so they are generally called re-deployment algorithms but they can also be used with static sensor with planned deployment. These algorithms have two variations:

   - ***Distributed Algorithms-*** Distributed APF-based deployment approaches are used in de-centralized MWSN architectures, where every sensor uses its local data, such as distances to neighboring sensors and obstacles, to run the deployment algorithm and self-deploy in the optimized positions. In this mobile sensors are treated as virtual free particles that are subject to virtual forces. These forces repel the sensors from each other and from obstacles. This method guarantees that an initial compact configuration of sensors will spread out to maximize the area coverage. In addition to these repulsive forces, sensors are also subject to a viscous friction force. This force is used to ensure that the network will eventually reach a state of static equilibrium. Another such algorithm is VOR, VEC, HEAL (Holes dEtection and healing) etc.

   - ***Centralized Approach-***APF-based centralized deployment algorithms are used in cluster-based WSN architecture, where the cluster head is assumed to have a high computational power to carry out the deployment algorithm for all deployed sensors. To carry out this task, the cluster head has to first localize the sensors in the network after an initial deployment and collect any other data pertinent to the deployment algorithm. After running the algorithm, the cluster head then communicate to each sensor its new target position. The advantage of such algorithms is that not all sensor nodes needs to have sensing or computational abilities. The example of such scheme is Virtual Forces Algorithm (VFA), Target Involved Virtual Force Algorithm (TIVFA).

4. **Particle Swarm Optimization Algorithms-** these algorithms are based on PSO principle. In this technique sensors are assumed to be initially randomly deployed and then a PSO-based algorithm (PSO-Grid) runs on a more powerful base station to calculate optimized positions of sensors and send it to them. Other examples are PSO-Voronoi, PSO with Local Search (PSO-LS), Virtual Force Directed Co-evolutionary Particle Swarm Optimization (VFCPSO), Co-evolutionary PSO (CPSO) technique etc.

9. KEY MANAGEMENT IN WSN

As WSN are generally deployed in hostile environment. So, security is the main issue in most of the networks. Key management is the main part in solving this issue. A key management scheme must satisfy network constraints such as battery life, transmission range, bandwidth, memory and prior deployment knowledge. Any key establishment technique must have evaluation metric such as Resistance, Revocation and Resilience. We can classify [7] key management as: 1) Single network wide key 2) pairwise key establishment 3) Trusted base station 4) public key schemes 5) key predistribution schemes 6) Dynamic key management & 7) Hierarchical key management schemes.

Single network-wide key, pairwise key establishment, Trusted Base Station

These schemes have been discussed earlier in Section- 7. They are also known as symmetric key schemes. Beside these schemes there is a popular protocol suite called SPINS which make use of two widely known protocols called SNEP & µTESLA.

Public-key Schemes

We know that public-key/ asymmetric schemes are more secure but also involves more computation and power consumption. So, such schemes are not widely accepted in WSN. Two well-known public-key schemes are RSA & ECC. The research shows that ECC is more efficient in terms of energy than RSA.

Key Predistribution Schemes

In this scheme some keys are preloaded into each node before deployment and later the network undergoes a discovery process to setup shared keys used for future communications. There are following key predistribution schemes available:

1. ***Random-key predistribution Scheme-*** this is also known as Basic-Scheme & consist of three steps: key predistribution (KP), shared-key discovery (SKD) and path-key establishment (PKE). In KP stage large key pool along with their identifiers is generated. From this pool keys are randomly picked and pre-installed into every node. In SKD stage comes into play when the nodes are deployed in actual environment. In this each node broadcast the key identifier list to find out the node pairs which share common key and use those keys for communication with those nodes. In PKE stage actual communication occurs & if two communicating nodes do not share key among them then communication takes place via intermediate shared key nodes.

To make this scheme more secure we can implement the concept of *key-revocation* in which a controller node will delete all previous keys of a node and assign fresh keys in its ring. This makes intruder hard to identify keys. Also this scheme has two variants known as *Q-Composite Random key predistribution Scheme & multi-path reinforcement.* The Q-Composite Scheme provides security under small scale attack but is vulnerable under large scale attack. In this variant we put a check that two shard key nodes must have at least q matching keys among them. This make intruder harder to break the communication.The multipath scheme makes the path established more secure by generating more secure communication key using disjoined path and exchanging information which finally helps in generating key.

2. ***Polynomial pool-based key predistribution-*** it is more secure scheme & in this during initialization phase the setup server first of all generates a bivariate t-degree polynomial f(x, y). The setup server then generates a polynomial share of the equation for every node in the sensor network. If two nodes i& j wants to generate common key used for communication then they evaluate their respective polynomial shares. Two variations of this scheme are Random Subset Scheme and Grid based key predistribution.

3. ***Hypercube key distribution scheme-*** this scheme guarantees that two nodes in the network will keep on using shared key until one of them is not compromised & provides higher probability of working. This scheme aims at computing n-dimensional hypercube with m^{n-1} polynomials. The setup server first of all assign each node an exclusive coordinate in matrix & also assign a set of polynomials which are used to compute pairwise key for communications.

Dynamic key Management
These schemes allows improved network sustainability & better network extension. The basic key management technique is called exclusion-based system (EBS) in which each node is assigned k keys from a pool of size k+m. And if any compromised node is detected then the whole key is rekeyed. This scheme is having collision problems so there are two variants of this scheme namely SHELL & LOCK.

Hierarchical key Management
These key management schemes provides reliable security to large scale WSNs and employ in-network processing & passive participating which was not considered in previous schemes. One such scheme is called LEAP. It is energy efficient and support various communication patterns like unicast, broadcast & global broadcast. It also maintain four types of keys in the network: individual key, pairwise shared key, cluster key & group key. *Individual Key* is uniquely shared among node and base station. This key is used to send alert signals to base station. *Pairwise Shared Key* is the unique key between a node & its neighboring node. A node use this key to share cluster key or sending data to the aggregator node. *Cluster Key* is shared among a node and its neighboring nodes. With this key a node can decide whether to send message or not. *Group Key* is the key shared among base station and all the nodes. This key is used for querying in the network. Efficient rekeying mechanism must be used to make system more secure.

10. DATA AGGREGATION IN WSN

This is another major research field of WSN which deals with minimizing network traffic & thus saving precious energy and bandwidth of network. In WSN there may be more than one sensor node sensing a particular region. So, each will send its sensed data to base station & it results in redundant data packets received at base station. Data aggregation is the process in which some intermediate nodes receiving multiple packets will aggregate and produce single packet by removing duplicity. The aggregation protocol must achieve five goals: energy efficiency, reducing data propagation latency, data accuracy, aggregation freshness and avoiding collisions.The literature [8] shows that there are four data aggregation strategies as shown in figure-7:

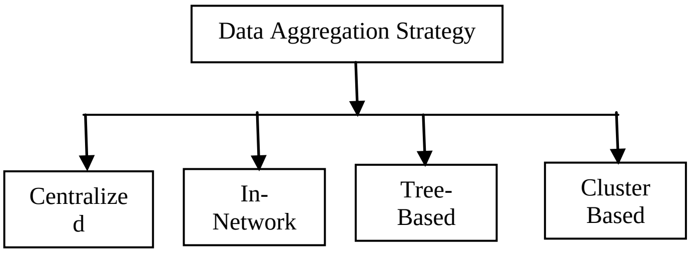

Figure 7: Data Aggregation Strategies.

Centralized Data Aggregation- the idea is to have a more powerful central node called header node to which all sensing node will forward data and finally it will aggregate and send data to base station. Here, each sensor node will send data to this header node via possible shortest path.

In-Network Aggregation- as WSN are generally multi-hop networks so in this scheme some intermediately nodes acts as the aggregator node rather than a centralized node. These aggregator nodes will work in two ways: with size reduction, without size reduction.With size reduction the aggregator node will combine and compress the received packets to reduce the packet length and finally forward it to the sink. Without size reduction, the aggregator nodes will simply merge data packets into single packet without processing the values of data and forward it to sink. The various algorithms are DAG based In-Network aggregation, OPAG (Opportunistic Data Aggregation) etc.

Tree-Based Aggregation- in this scheme first of all a Data Aggregation Tree (DAT) is created by using spanning tree. In this tree, each sensor node are present at leaves and every node only forward to its parent node which will perform aggregation of packets. The various examples of this strategy are shortest path tree algorithm, center at nearest source algorithm, Greedy Incremental Tree algorithm, Ant Colony Algorithm, DBST (Dynamically Balanced Spanning Tree), SDRE (SVM based Data Redundancy Elimination), DEDA (Delay Efficient Distributed Data Aggregation) etc.

Cluster-Based Aggregation- this strategy is based on clustering of the network and giving the cluster head the responsibility of data aggregation. The various examples are DRINA (data routing in network aggregation), REDD (Redundancy Eliminated Data Dissemination), BHCDA (Bandwidth efficient Heterogeneity aware Cluster based Data Aggregation), AEERDAT, EEBCDA etc.

11. RELIABILITY IN WSN

In WSN the traffic is generally converging in nature toward sink node & it results in congestion/blockage at sink. This results in loss of packets along with packets lost due to transmission errors, packet collision, interference, node failure and other unforeseeable reasons. It directly affects the QoS also.So, reliability is another major research topic in

WSN which aims at minimizing packet loss due to above mentioned reasons. Figure 8 shows the classification of reliability strategies/methods [9]:

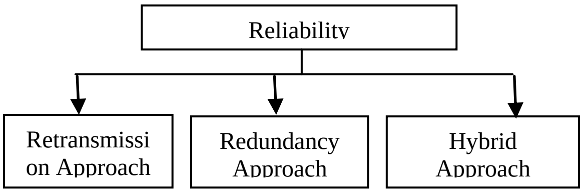

Figure 8: Reliability Strategies in WSN.

Retransmission Approach- it is the most simper technique to achieve reliability in WSN which involve waiting for the acknowledgement after sending packets. This approach make use of two kinds of acknowledgements namely explicit acknowledgement (eACK) & implicit acknowledgement (iACK). eACK mechanism make use of special control message which the receiving node of packet sends back to the sender. In this the sender keeps on storing the packet until it receives the acknowledgement. This mechanism results in extra overhead on network in term of bandwidth and more energy consumption due to extra control messages. iACK mechanism, on the other hand, tries to minimize the control overheads by listening to the channel & interpreting the forwarding of the packet by next hop node as a receipt of acknowledgement. Retransmission based reliability can be implemented by following two methods:

1. *End-to-End Method*-it is a connection-oriented approach to ensure reliable transmission of data. The example of one such protocol is STCP (Sensor Transmission Control Protocol) which is a sink centric end to end reliability protocol with congestion control mechanism. This protocol make use of eACK&the sink node handles congestion by informing the congested sender about choosing some alternate links for sending data. The other such protocol is DTSN (Distributed Transport for Sensor Network) which is non-sink centric end to end reliability protocol.

2. *Hop-by-Hop Method)* -it is a link-oriented method which guarantee reliability in transmitting packets between two neighboring nodes. One such protocol is DFRF (Directed Flood Routing Framework), which make use of iACK based scheme called SWIA (Stop & Wait iACK). Other examples are RTMC (Reliable Transport with Memory Consideration), RBC (Reliable Brusty Convergecast), ERTP, TRCCIT, RMST, PSFQ, GARUDA etc.

Redundancy Based Approach- this technique forbid retransmission of whole packets after some bits are lost, instead, it tries to recover by making use of some error detection and correcting codes such as FFC (Forward Error Correction) & OREC (Optimum Reed-Solomon Erasure Coding). This significantly reduce re-transmission overhead of the packet. This approach can also be implemented using following two methods:

1. *End-to-End Method-* it is a connection-oriented approach which make use of OREC coding for reliable data transmission. In this scheme, the encoding/ decoding operations are only performed by sender and receiver nodes while the intermediate nodes simply relay the packets. This scheme make use of GA to determine the total no. of fragments done by sender. This scheme also assume network as query-based.

2. *Hop*-by-Hop Method- it is a link-oriented approach and encoding/decoding operations are performed at every intermediate node. The example is TRSN, RDTS, MVSA, ARM etc.

Hybrid Approach- we know that retransmission ensure reliability at the transmission overhead cost & the success of redundancy approach depends on the ability to reconstruct the lost data at receiving node based on total no. of fragments received. So, in this approach we combine the better of two approaches and use retransmission along with redundancy in case it fails to recover when the no. of received fragments are less than the original fragments.

12. Congestion Control In WSN

Congestion control is another research issue which directly affects Quality of Service (QoS) parameters such as packet delivery ratio (PDR), end to end delay and energy consumption [10]. Congestion in WSN can be at two levels: node level & link level congestion. Node level/ buffer overflow congestion occurs when packet arrival rate is higher than the packet service rate. This type of congestion increases packet loss & power waste. In link level congestion, the PDR at sink node is reduced due to factors such as collision, competition & bit error.

Congestion control [10] in WSN is done in three steps: congestion detection, congestion notification & congestion control.

Congestion Detection- it is the process of detecting & finding the presence of congestion in network. Congestion detection in WSN depends on following parameters:

1. *Buffer Occupancy-* it is the queue length of the node and when it is filled it indicates congestion.

2. *Channel load-* it is another parameter which helps in detecting congestion as it results in increase in time frame for the transmission of data packets than predefined threshold.

3. Packet *Service Time-* it is defined as the time difference between packet arrival at MAC layer & its transmission time.

Congestion Notification- it is the process of informing the upstream nodes about collision situation in network. There are following two methods of congestion notification:

1. *Explicit Congestion Notification-* this technique involves making use of sending special control messages to upstream sensor nodes. This mechanism results in further increase in link load due to more control messages.

2. *Implicit Congestion Notification-* in this technique the congested node will inform about congestion by piggybacking the congestion information in a payload packet header.

Congestion Control- the various congestion control techniques [10] can be broadly divided into four categories as shown in figure-9 below.

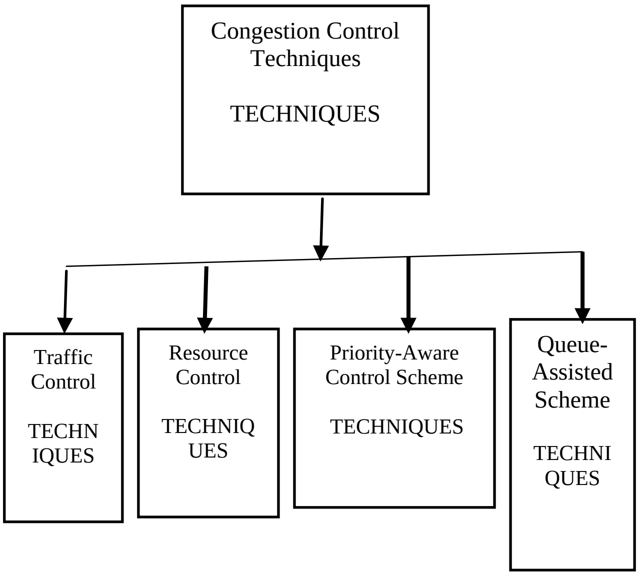

Figure 9: Congestion Control Techniques

1. ***Traffic Control Scheme:*** in this mechanism, the congestion is removed by reducing the traffic i.e. generating less number of packets over WSN. In these techniques, only the source node can mitigate the congestion & no other node. It can be done either by decreasing the congestion window size in case of congestion, or, by explicitly calculation of sending rate mathematically based on the available network bandwidth. Since, only the source is involved in congestion control, so, this technique is inefficient to handle real-time applications.

   The various such protocols are ARC (Adaptive Rate Control), CODA (Congestion Detection & Avoidance), CCF (Congestion Control & Fairness), FUSION, CONSISE, FACC, CADA, ECODA etc.

2. ***Resource Control Scheme:*** in this mechanism, the congestion is handled by managing the hardware resource available i.e. increasing network bandwidth or using idle or uncongested path for transmitting packets. This technique improves packet delivery rate significantly.

   The various such protocols are TARA (Topology Aware Resource Adaptation), LACAS (Learning Automata based on Congestion Avoidance Scheme), HTAP, flock-CC, WCCP, CRRT, DAIPAS etc.

3. ***Priority-Aware Control Scheme:*** in this mechanism, we use prioritized transmission i.e. the congested node is given higher priority so that its packets are transmitted faster to remove congestion.

   The various such protocols are IFRC (Interference Aware Fair Rate Control), DPCC (Decentralized Predictive Congestion Control), CCTF, GMCAR, HOCA, QCCP-Ps etc.

4. ***Queue-Assisted Scheme:*** in this mechanism, we use rate adjustment techniques to keep the transmission queue of a node as low as possible.

   The various such protocols are PCCP (Priority-aware upstream Congestion Control Protocol), TLP, ACT, CL-APCC, DPCC, FLC, ESRT, PSFQ (Pump Slowly Fetch Quickly) etc.

The various congestion control metrics are goodput, fairness, throughput, packet delivery ratio, end-to-end delay, average node energy consumption, packet loss rate, and network lifetime.

13. QOS IN WSN

As we know that the WSN's structure is highly dependent on the particular application under consideration. Some application require higher QoS (Quality of Service) for data than others. The QoS is directly affected by various parameters such as: deployment, coverage, lifetime and connectivity. The QoS also helps in achieving energy efficiency and lifetime improvement for the network & thus improves reliability of the WSN.

The QoS is a challenge for WSN due to its specific characteristics such as resource constraints, unbalanced traffic, data redundancy, network dynamics, energy imbalance, scalability and reliability requirements, packet delivery performance, data delivery delay and reliable connections [11] under failures.

Coverage- coverage may be defined as an ability to sense the environment under consideration such that maximum area is covered along with minimizing the multiple sensors sensing the same area thus resulting data redundancy. It is highly related with connectivity and communication of system. There are roughly three coverage strategies categorized as: area coverage, point coverage, and path coverage.

Deployment and Connectivity- the aim of various deployment strategies is to maximize the coverage thus increasing QoS or to minimize energy consumption. Various such strategies have been discussed earlier in this paper.

Lifetime- lifetime is another parameter for QoS and is defined as the time for which the WSN keeps on sensing & collecting data from the environment concerned. As, the nodes are power constrained so with time they fails resulting in coverage & connectivity. The various strategies used to increase network lifetime can be categorized as: Sensor relocation, Cover sets, Data gathering strategies, multiple moving base stations, by unequal clustering or scheduling the selection of cluster heads, Adaptive data propagation, Optimal routing and Optimizing the energy consumption.

14. CONCLUSION& FUTURE DIRECTIONS

Overall we can conclude that WSN is a vast research field having lot of possibilities & opportunities to be still carried out. This paper can be very useful for a newbie in the field of WSN. In this paper we have tried out best to cover WSN field fully but a more detailed description can be there for each protocol specified in future.

The future is very dynamic for wireless sensor network due to large demand of WSN for various application and both hardware and software fields are wide opened for it.

15. REFERENCES

[1] G S Sara, D Sridharan, "Routing in mobile wireless sensor network: a survey", Springer TelecommunSyst 57, pp. 51-79, 2014.

[2] A.A Abbasi, M. Younis, "A Survey on Clustering Algorithms for wireless sensor network", Elsevier Computer Comm. 30, pp. 2836-2841, 2007.

[3] R Lin, Z Wang & Y Sun, “Energy Efficient Medium Access Control Protocols for Wireless Sensor Networks and Its State-of-Art”, IEEE, 2004.

[4] X Chen, K Makki, et al., “Sensor Network Security: A Survey”, IEEE Communications Surveys & Tutorials, Vol. 11, No. 2, pp. 52-73, Second Quarter 2009.

[5] D Martins, H Guyennet, “Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey”, IEEE International Conference on Network-Based Information Systems, pp. 313-320, 2010.

[6] D S Deif, Y Gadallah, “Classification of Wireless Sensor Networks Deployment Techniques”, IEEE Communications Surveys & Tutorials, Vol. 16, No. 2, pp. 834-855, Second Quarter 2014.

[7] Y Xiao, V K Rayi et al., “A Survey of key management schemes in wireless sensor networks”, Elsevier Computer Commun. 30, pp. 2314-2341, 2007.

[8] S Sirsikar, S Anavatti, “Issues of Data Aggregation Methods in Wireless Sensor Network: A Survey”, Elsevier Procedia Computer Science 49, pp. 194-201, 2015.

[9] M A Mahmood et al., “Reliability in wireless sensor network: a survey & challenges ahead”, Elsevier Computer Networks 79, pp. 166-187, 2015.

[10] A Ghaffari, “Congestion control mechanisms in wireless sensor networks: A survey”, Elsevier Journal of Network and Computer Applications 52, pp. 101-115, 2015.

[11] I Snigdh, N Gupta, “Quality of Service Metrics in Wireless Sensor Networks: A Survey”, Springer J. Inst. Eng. India Ser. B, December 2014.

[12] Akyildiz I, Su W, Sankarasubramaniam Y, Cayirci E, “A survey on sensor networks”, IEEE Communication Magazine 40(8), pp. 102–114, 2002.

[13] Karl H, Willig A (2007) Protocols and architectures for wireless sensor networks. Wiley Interscience, New York.

[14] Ehsan S, Hamdaoui B, ”A survey on energy-efficient routing techniques with QoS assurances for wireless multimedia sensor networks”, IEEE Communication Survey Tutor 14(2), pp. 265–278, 2012.

[15] DiFrancescoM,DasSK,AnastasiG, “Data Collectionin Wireless Sensor Networkswithmobile elements: a survey”, ACM Trans Sens Network 8(1):7, 2011.

[16] Wang F, Liu J,”Networked wireless sensor data collection: issues, challenges, and approaches”, IEEE Communication Survey Tutor 13(4), pp. 673–687, 2011.

[17] Zeng Y, Cao J, Hong J, Zhang S, Xie L, “Secure localization and location verification in wireless sensor networks: a survey”, J Super comput 64(3), pp. 685–701, 2013.

[18] Kavitha T, Sridharan D, “Security vulnerabilities in wireless sensor networks: a survey”, J Inf Assur Secur 5(1), pp. 31–44, 2010.

[19] Kausar F et al, “Scalable and efficient key management for heterogeneous sensor networks”, J Super comput 45(1):44–65, 2008.

[20] La Malfa S (2010) Wireless sensor networks. Available online: http://www.dees.unict.it/users/bando/ files/wsn.pd..

[21] EnOcean. http://www.enocean.com/en/enocean-wireless-standard/.

[22] ANT technology. http://www.thisisant.com/technology.

[23] ZigBee Alliance. Available online: http://www.zigbee.org/

[24] Buratti C, Conti A, Dardari D, Verdone R, “An overview on wireless sensor networks technology and evolution”, Sensors 9(9), pp. 6869, 2009.

[25] L. Shi et al., “DDRP: An Efficient Data-Driven Routing Protocols for Wireless Sensor Networks with Mobile Sinks,” Int’l. J. Commun. Systems, vol. 26, no. 10, pp. 1341–55, Oct. 2013.

[26] K. Tian et al. a, “Data Gathering Protocols for Wireless Sensor Networks with Mobile Sinks,” Proc. IEEE GLOBECOM 2010, pp. 1–6, Dec. 2010.

[27] F. Yu et al., “Elastic Routing: A Novel Geographic Routing for Mobile Sinks in Wireless Sensor Networks,” IET Commun., vol. 4, no. 6, pp. 716–27, June 2010.

[28] Flora J, “A survey on congestion control techniques in wireless sensor networks”, In: Paper presented at the 2011 international conference on emerging trends in electrical and computer technology, p. 1146–9, 2011.

[29] Gowthaman P, Chakravarthi R, “Survey on various congestion detection and control protocols in wireless sensor networks”, Int J AdvComputEngCommunTechnol, 2(4):15–9, 2013.

[30] Heikalabad SR, Ghaffari A, Hadian MA, Rasouli H, “DPCC: dynamic predictive congestion control in wireless sensor networks”, IJCSI Int J ComputSci Issues 8(1), pp. 472–7, 2011.

[31] Sergiou C, Vassiliou V, Paphitis A, ”Congestion control in Wireless Sensor Networks through dynamic alternative path selection”, ComputNetw, 75(Part A), pp. 226–38, 2014.

[32] Wang C, Sohraby K, Lawrence V, Li B, Hu, Y, “Priority-based congestion control in wireless sensor networks”, In: Paper presented at the IEEE international conference on sensor networks, ubiquitous, and trustworthy computing, 2006 (SUTC’06), pp. 8, 2006.

[33] Wang C, Sohraby K, Li B. Sen, “TCP: a hop-by-hop congestion control protocol for wireless sensor networks”, Paper presented at the IEEE INFOCOM, pp.107– 14, 2005.

[34] Zhao J, Wang L, Li S, Liu X, Yuan Z, Gao Z, “A survey of congestion control mechanisms in wireless sensor networks”, In: Paper presented at the 2010 sixth IEEE international conference on intelligent information hiding and multimedia signal processing (IIH-MSP), pp. 719–22, 2010.

[35] Antoniou P, Pitsillides A, Blackwell T, Engelbrecht A, Michael L, “Congestion control in wireless sensor networks based on bird flocking behavior”, ComputNetw. 57(5), pp. 1167–91, 2013.

[36] Chen J, Díaz M, Llopis L, Rubio B, Troya JM, "A survey on quality of service support in wireless sensor and actor networks: requirements and challenges in the context of critical infrastructure protection", J NetwComputAppl, 34 (4), pp. 1225–39, 2011.

[37] P Rawat et al.," Wireless sensor networks: a survey on recent developments and potential synergies", Springer J Supercomput 68, pp. 1-48, 2014.

[38] A. Ghaffari, "Congestion control mechanisms in wireless sensor networks: A survey", J NetwComputAppl, 52, pp. 101-115, 2015.

[39] S. Sirsikar, S. Anavatti, "Issues of Data Aggregation Methods in Wireless Sensor Network: A Survey", Procedia Computer Science, 49, pp. 194-201, ScienceDirect, 2015.

[40] L. Mainetti, L. Patrono, and A. Vilei, "Evolution of wireless sensor networks towards the internet ofthings: A survey," in Proc.International Conference on Software, Telecommunications and Computer Networks (SoftCOM), pp. 1–6, 2011.

[41] V. Potdar, A. Sharif, and E. Chang, "Wireless sensor networks: A survey," in Proc. International Conference on Advanced Information Networking and Applications Workshops (WAINA'09), pp. 636– 641, 2009.

[42] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," vol. 52, no. 12. Elsevier, pp. 2292–2330, 2008.

[43] P. Huang, L. Xiao, S. Soltani, M. Mutka, and N. Xi, "The evolution of mac protocols in wireless sensor networks: A survey," IEEE Commun. Surveys & Tutorials, 2012, to be published.

[44] Y.-h. Kim, C.-M. Kim, D.-S. Yang, Y.-j. Oh, and Y.-H. Han, "Regular sensor deployment patterns forp-coverage andq-connectivity inwireless sensor networks," in Proc. International Conference on Information Networking (ICOIN), pp. 290–295, 2012.

[45] M. R. Ingle and N. Bawane, "An energy efficient deployment of nodes in wireless sensor network using voronoi diagram," in Proc. 3rd International Conference on Electronics Computer Technology (ICECT), vol. 6, pp. 307–311, 2011.

[46] X. Yu, W. Huang, J. Lan, and X. Qian, "A novel virtual force approach for node deployment in wireless sensor network," in Proc. IEEE 8th International Conference on Distributed Computing in Sensor Systems (DCOSS), pp. 359–363, 2012.

[47] Al-Karaki, J. N., & Kamal, A. E,"Routing techniques in wirelesssensornetworks:asurvey", IEEE Wirel.Commun., pp. 6–28, December 2004.

[48] Al-Karaki,J. N., & Al-Malkawi,I. T,"On energyefficient routing for wireless sensor networks", In Proceedings of international conference on innovations in information technology, December 2008.

[49] O. D. Incel, A. Ghosh, B. Krishnamachari, and K. Chintalapudi, "Fast data collection in tree-based wireless sensor networks," IEEE Trans. Mob. Comput., vol. 11, no. 1, pp. 86–99, 2012.

[50] A. A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks," Elsevier Computer Communications, vol. 30, no. 14-15, pp. 2826 – 2841, 2007.

[51] K. Romer and F.Mattern,"The design space of wireless sensor networks," IEEE Wireless Commun., vol. 11, no. 6, pp. 54–61, Dec. 2004.

[52] T. Haenselmann, "Sensor networks," in Free (GNU) Textbook on Wireless Sensor Networks, Apr. 2005.

[53] P. Antoniou and A. Pitsillides, "A bio-inspired approach for streaming applications in wireless sensor networks based on the Lotka-Volterra competition model," Comput. Commun., vol. 33, no. 17, pp. 2039–2047, Nov. 2010.

[54] L. Cobo, A. Quintero, and S. Pierre, "Ant-based routing for wireless multimedia sensor networks using multiple QoS metrics," Comput. Netw., vol. 54, no. 17, pp. 2991–3010, Dec. 2010.

[55] C. Sergiou, P. Antoniou and V. Vassiliou, "A Comprehensive Survey of Congestion Control Protocols in Wireless Sensor Networks", IEEE Communication Surveys & Tutorials, Vol. 16, No. 4, Fourth Quarter 2014.

[56] K. Henry and Douglas R. Stinson, "Secure network discovery in wireless sensor networks using combinatorial key predistribution", In Proceedings of the Workshop on Lightweight Security and Privacy: Devices, Protocols and Applications (LightSec'11). IEEE, Los Alamitos, CA, 34–43, 2011.

[57] Keith M. Martin, Maura B. Paterson, and Douglas R Stinson, "Key predistribution for homogeneous wireless sensor networks with group deployment of nodes", ACM Transactions on Sensor Networks7,2,1–19,2010. http://dl.acm.org/citation.cfm?id=1824767.

[58] A. Sangwan and R. Pal Singh, "Survey on Coverage Problems in Wireless Sensor Networks", Wireless PersCommun, 80, pp. 1475–1500, 2015.

[59] Ammari, H. M., &Giudici, J, "On the connected k-coverage problem in heterogeneous sensor nets: The curse of randomness and heterogeneity", In 29th IEEE international conference on distributed computing systems, pp. 265–272, 2009.

[60] Ammari, H. M., & Das, S. K, "Scheduling protocols for Homogeneous and Heterogeneous k-Covered Wireless Sensor Networks", Journal of Network and Computer Applications, 7(1), 79–97, 2011.

[61] Balaganesh, S., &Periyasamy, S, "Load balanced connection aware clustering algorithm for wireless sensor networks", International Journal of Innovative Research in Computer and Communication Engineering, 2(1), 3781–3787, 2014.

[62] I. Snigdh, N. Gupta, "Quality of Service Metrics in Wireless Sensor Networks: A Survey", J. Inst. Eng. India Ser. B, November 2014.

[63] D. Chen, P.K. Varshney, "QoS support in wireless sensor networks: a survey", Int. Conf. Wirel. Netw. 233, pp. 1–7, 2004.

[64] M.Z. Hasan, T. Wan, "Optimized quality of service for real-time wireless sensor networks using a partitioning multipath routing approach", J. Comput. Netw. Commun. 2013, 18 (2013). doi: 10.1155/2013/497157.

[65] N. Aitsaadi, N. Achir, K. Boussetta, G. Pujolle, “Multi-objective WSN deployment: quality of monitoring, connectivity and lifetime”, in Communications IEEE International Conference on (ICC’10), pp. 1–6 (2010). doi:10.1109/ICC.2010.5502276.

[66] eleniKlaoudatou, ElisavetKonstatinou and Georgios Kambourakis," A survey on Cluster-Based Group Key Agreement protocols for WSNs", IEEE Communications surveys & Tutorials, voLI3, No.3, pp.429-442, 2011.

[67] Xueli Yan and Xiaohui Ye, "A novel key predistribution scheme for wireless sensor networks based on hexagon deployment model", In proceedings of ELSEVIER, pp. 8018-8026, 2011.

[68] Yiying Zhang, Xiangzhen Li, Yuanan Liu and Dequan Gao, “A Hierarchy-based dynamic key management for c1ustered wireless sensor network", In proceedings of ELESEVIER, pp.7967-7974, 2011.

[69] Sun Qian, "A novel key pre-distribution for wireless sensor networks", ELESEVIER international conference on solid state devices and materials science, pp.2183-2189. 2012.