Middle-East Journal of Scientific Research 24 (2): 398-403, 2016
ISSN 1990-9233
© IDOSI Publications, 2016
DOI: 10.5829/idosi.mejsr.2016.24.02.23032

An Effective Method for Reliable Data Delivery in Highly Dynamic Mobile Ad Hoc Networks

[1]K. Vinodh Kumar and [2]S. PadmaPriya

[1]Research Scholar, Department of Information Technology, St Peter's University, India
[2]Professor, Prathyusha Engineering College, Department of Computer Science and Engineering,

Abstract: To prevent vulnerable virtual machines from being compromised in the cloud, a multi-phase distributed vulnerability detection, measurement and countermeasure selection mechanism called NICE is been proposed, which is built on attack graph-based analytical models and reconfigurable virtual network-based countermeasures. The proposed framework leverages Open flow network programming APIs to build a monitor and control plane over distributed programmable virtual switches to significantly improve attack detection and mitigate attack consequences. The greatest advantage of using the DSR over the AODV based protocols is that we do not have to use the beacon transmission, i.e. the periodic hello packet. In the previous research techniques the dynamic anomaly based detection schemes for the AODV based protocols have been studied and presented. Anomaly detection can be done in DSR based MANETs by sampling a section of the path and comparison with the general activity of the network determined by a baseline. This is achieved by first classifying the possible attacks in DSR. A training database is maintained and compared with a sample at any random area of the network. Using weighted co-efficient, it is possible to detect any anomaly behavior inside the network.

Key words: Training database · Open flow network · Graph-based analytical models · Counter measure selection

INTRODUCTION

A Mobile Ad-hoc Network is a kind of wireless ad-hoc network and it is a self-configuring network of mobile outers connected by wireless links. It is a wireless network without infrastructure. One of the important research areas in MANET is establishing and maintaining the adhoc network through the use of routing protocols.

The security is one of the essential requirements in mobile adhoc network. When the Mobile adhoc network is compared to wired network, MANET is more vulnerable to security attacks due to the lack of the trusted centralized authority and limited resources. Normally, attacks on adhoc networks are classified as passive and active attacks. A MANET is referred to as an infrastructure less network because the mobile nodes in the network dramatically set up paths among themselves to transmit packets temporarily. In the MANET, nodes within each other's wireless transmission ranges can communicate directly. However nodes outside each other's range have to rely on some other nodes to relay messages. Any routing protocol must encapsulate an essential set of security mechanisms. These mechanisms are used to prevent, detect and respond to security attacks.

In the existing paper uses the routing protocol named as Ad-hoc On Demand Distance Vector (AODV) which is a route discovery process. It is very different to maintain the routing information. It can maintain multiple route cache entries for each destination. Without source routing, AODV relies on routing table entries to propagate a route request back to a source and subsequently to route data packets to the destination. It uses a sequence number maintained at each destination to determine freshness of routing information and to prevent routing loops. These sequence numbers are carried by all routing packets. It is not suitable for all types of packets. To overcome this drawback design another routing process this is named as Dynamic Source Routing (DSR).

Corresponding Author: K. Vinodh Kumar, Research Scholar, Department of Information Technology, St Peter's University, India.

The key distinguishing feature of DSR is the use of source routing. The source routing describes that the sender knows the complete hop-by-hop route to the destination. These routes are stored in a route cache. The data packets carry the source route in the packet header. When a node in the adhoc network attempts to send a data packet to the destination for which it does not already know the route, it uses a route discovery process to dynamically determine such a route. Route discovery works by flooding the network with route request packet. Each node receiving a route request and rebroadcast it, unless it is the destination or it has a route to the destination in its route cache. Such a node replies to the route request with a route reply packet that is routed back to an original source.

Related Works: In [2] the dependability of the routing system in adhoc networks inherently relies on node behavior. In order to support multihop operation in the network, most ad hoc routing algorithms assume well-behaving nodes. However, in reality there may exist constrained, selfish or malicious nodes. We discuss the influence of node misbehavior on the routing process. In particular, we derive a classification for misbehaving nodes and extend an analytical model of the route acquisition process executed by the adhoc on-demand distance vector (AODV) routing protocol to cover different classes of misbehavior. The validation of the behavior model and the clarification of the impact misbehaving nodes impose onto the routing process, was completed using an experimental analysis.

In [3] mobile ad hoc networks pose new kinds of security problems, caused by their nature of collaborative and open systems and by limited availability of resources. Wi-Fi connectivity was considered as data link layer as a basis and focus on routing security. Implementation of the secure AODV protocol extension was discussed, which includes tuning strategies aimed at improving its performance. Namely, an adaptive mechanism was proposed that tunes SAODV behavior. Moreover, adaptive strategy and another techniquewere analyzed and that delays the verification of digital signatures.

In [6] initial work in ad hoc routing has considered only the problem of providing efficient mechanisms for finding paths in very dynamic networks, without considering security. Because of this, there are a number of attacks that can be used to manipulate the routing in an adhoc network. The threats were discussed, specifically showing their effects on ad hoc on-demand distance vector and dynamic source routing. Our protocol, named authenticated routing for ad hoc networks (ARAN), uses public-key cryptographic mechanisms to defeat all identified attacks. ARAN can secure routing in environments where nodes are authorized to participate but untrusted to cooperate, as well as environments where participants do not need to be authorized to participate. Through both simulation and experimentation with our publicly available implementation, characterize and evaluate of ARAN was done and show that it is able to effectively and efficiently discover secure routes within an ad hoc network.

In [7] one of the main challenges in budding instruction detection systems (IDSs) for mobile ad hoc networks(MANETs) was to integrate the mobility impact and adjust the behavior of IDSs dynamically. They focus on the protection of MANET routing protocols and first demonstrate that nodes' moving speed, a commonly used parameter in tuning IDS performance, was not an effective metric for the performance measurement of IDSs for MANETs. The link change rate was proposed, which can not only act as a unified metric in measuring MANET IDS performance, but also be used to facilitate local MANET IDSs to select normal profiles adaptively. Different mobility models were utilized to study the performance of our proposed adaptive mechanisms at different mobility levels. Simulation results show that our proposed adaptive mechanisms were effective and less dependent on mobility models. Detailed analysis of simulation results was also provided.

In [8] the increasing use of intrusion detection system gives rise to a huge volume of alert logs, making it hard for security administrators to uncover hidden attack scenarios. Four-layer semantic scheme were proposed and designed to allow inferring attack scenario and enabling attack semanticqueries. The modified case grammar, PCTCG, was used to convert the raw alerts into machine understandable uniform alert streams. The 2-atom alerts semantic network, 2-AASN was used to generate attack scenario classes. Afterwards, based on the alert context, attackscenario instances were extracted and attack semantic query results on attack scenario instance using spreading activation technique were forwarded to the security administrator.

Existing System

AODV Routing Protocol Overview: The AODV is a reactive routing protocol in which it can generate a route. Before communication the network generates a route from ource to destination. Each node present in the network

has its own sequence number. The number is changed for every link is added. Based on the sequence number, the information present in the channel should be rested. In order to make geographical routing protocol to be triumphant, it is supposed to be supplemented by a positionservice which is capable enough to provide position information for all possible destinationnodes. There existsa considerable corpse of research which treats position services formobile ad hoc networks. The theoretically troublefree protocols preserve no knowledge about how the nodes move, where they are, or the nodes they have previously encountered. Two suchtheoretically simpleprotocols are: 1) randomized routing [4], where a packet randomly jumps around between nodes until it reaches the destination and 2) epidemic routing [5], where every node in the network receives a copy of a packet. Another conceptually simple scheme, but one that actively uses node mobility and limits its overhead, is spray and wait. In spray and wait, a packet is distributed to a limited number of nodes that hold on to the packet until they (potentially) meet the destination.Cerf *et al*., have portrayedarchitecture for DTNs, in which a large and heterogeneous system transports data bundles between custodians that temporarily store the bundles until they can be forwarded again.

The key difference between the authors view of a DTN and the proposedview of an IC-MANET is in the size and diversity of the systems. It can be notified that an IC.

- MANET as a relatively homogeneous system with a relatively modest spatial distribution. This difference in system properties leads to the proposal that the routing should be done on the network. In common mostof the proposed MANET routing protocols transfer packets between nodes using a linklayer unicast transfer mode.

This condition enables error correction at the link layer, but it does not exploit the broadcast nature of wireless transmissions. In opportunistic routing (OR), a packet is sent in a broadcast mode to several eligible forwarders and the best forwarder that received the packet will continue to forward it. The challenge in OR is how knowledge about the best forwarder can be distributed. One way of doing the selection of the forwarder is by geographical selection, which is an approach taken in contentionbased forwarding (CBF) and beaconless routing (BLR).

The protocol builds on these principles and extends them to meet the requirements of an IC-MANET. Because of the disconnected nature of the network, there will be similar problems with delays as for the mapping-based location services. One protocol that attempts to limit the cost of a location request by having a proactive component is Brownian gossip. In Brownian gossip, nodes exchange information on previous encounters when two nodes meet. This information is used to guide a location request toward the destination node's position.

Working Principle of AODV Routing Protocol: AODV routing protocol works by using two messages named as Route Request Message (RREQ) and Route Reply Message (RREP). If a communication node is not in range then send a RREQ message to its neighbours. The RREQ message contains source IP address and sequence number as well as destination IP address and sequence number. If the neighbour knows the destination it sends the RREP message back to the source. If the neighbour is not known then it rebroadcast the RREQ to source. Route Error Message (RERR) is mainly usedwhen the node gets removed around and connection is lost. If any node receives RERR message, it deletes all the routes associated with that node. Error messages also send when the route becomes invalid.

AODV routing protocol works with two phases. They are route discovery and route maintenance.

Route Discovery: Fig. 1 illustrates the route discovery process. Every node broadcast a RREQ to its neighbours. If a neighbour has no path then forwards the RREQ to the source. If the neighbour has a route then it changes the routing table. This process is continued until it reaches its destination. After it reaches, it sends the reply message to the source then the route is discovered communication starts successfully.

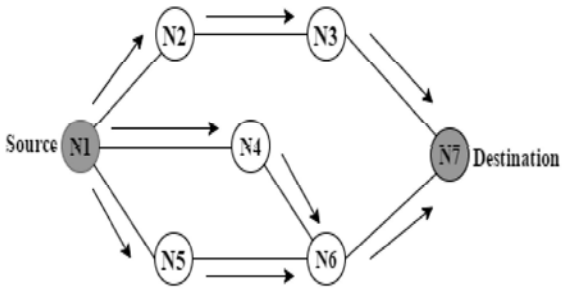


Fig. 1: Route discovery process

The longest distance between two points within these shapes must be the preceptor radio range of the node(s). If overhearing is not a critical property and we want to maximize the probability of finding a new curator node, then the forwarding area should include all nodes that guarantee progress toward the destinationnode. To avoid very small hops and to supplyfor inaccuracies in the locationservice, e.g., the Global Positioning System (GPS), a minimum forward distance may be discreet.

All these forwarding areas can be used inAPBRRPas a parameterized input. In this research work, we have chosen thepacket progress forwarding area and we will return to the basis.The delay timer for each mobile node can be set based on many principles, where two natural ones are to favourshort hops or long hops toward the destinationnode.Short hops are beneficialwhenmuch data will be exchanged between the nodes, because the transfer probability is higher with a shorter distance. The snagof APBRRPis that more hopsmay be created resulting in higher overhead. Long hops will reduce the number of hops, by which resulting the snag of the transfer reliability between distant nodes is lesser.

MOBILE ad hoc networks (MANETs) have gained a great deal of attention because of its significant advantages carried about by multihop, infrastructure-less transmission. On the other hand, due to the error prone wireless channel and the dynamic network topology, reliable data delivery in MANETs, especially in challenged environments with high mobility residue an issue. MANET is used to communicate between hosts in the absence of dedicated routing infrastructure, when messages are forwarded by intermediate hosts if the sender and receiver are out of communication range. The quality of such a routing algorithm can be measured by its delivery ratio that be supposed to maximum; that is, the ratio of the number of data packets received at the destination to the number of data packets sent by the source. Traditional topology-based MANET routing protocols (e.g., DSDV, AODV, DSR [1]) are relatively liable to node mobility. The main cause is due to the end-to-end route discovery is before data transmission. Owing to the constantly and even fast changing network topology, it is very difficult to maintain a deterministic route. The discovery and recovery procedures are also time and energy consuming. Once the path shatters, data packets will get lost or be delayed for a long time in anticipation of the renewal of the route, causing transmission disruption.

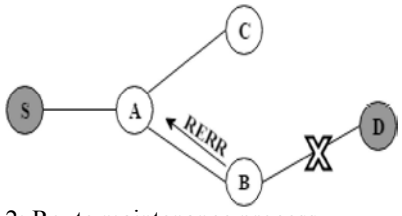


Fig. 2: Route maintenance process

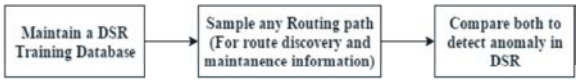
Route Maintenance: After finding the path then it should be maintained. A path being used is called as an active path. There is no communication along the active path then the source node discover new path for transmission. It sends the RERR message to all the intermediate nodes. This RERR message is denoted as the failed link for this route. There is no communication along this route.

In the Fig 2 discover a path from source to destination. Suppose the connection from the node B to node D disconnect then the node B sends the RERR message to source. After this the communication is not transferred through the same path.

Attacks on AODV: The black hole attack is one of the active DoS attacks possible in MANETS. In this attack a malicious node sends a false reply response packet to a source node that initiated the route discovery, in order to pose itself as a destination node or an immediate neighbor to the actual destination node. In such a case the source node would forward all of its data packets to the malicious node, which originally were intended for the genuine destination. The malicious node eventually may never forward any of the data packets to the genuine destination. As a result, the source and the destination node becomes unable to communicate with each other.

Proposed System

System Design:



Algorithm

Step 1: check Dynamic source routing is possible

Step 2: Maintain a training database in dynamic source routing.

Step 3: Transmitted data can be available in the database

Step 4: Create a sample routing path

Step 5: Complete the routing path by route discovery and maintenance.

Step 6: Detect the path and compare for anomaly in DSR.

Initially the dynamic source routing they maintain a training database. The database contains the information about the data which are transmitted between the nodes. After the database is created create a sample routing path. This routing path contains both the route discovery and maintenance process. After the path is discovered then compare both to detect anomaly in DSR.

Training Database: The training database is calculated at consecutive intervals of time and updated dynamically after every sampling process if the normal activity is observed from the traffic analysis.

From a large network area, a small sample of Δx is considered. The mean and projection distance from the mean are calculated.

The training database is given by,

$$Di = \{x\}$$

The DSR packet types (RREQ and RREP) are considered for sampling in the area of DSR in the MANETs traffic for two phases:

- Route Discovery
- Route Maintenance

The variable parameters and the weighted coefficients are calculated and hence simulation of the proposed method is done in NS2.

RESULTS

A node which is going to take care of all other nodes by managing the traffic. It is going to check whether the reply's sending by the nodes are appropriate or not in regular intervals, whenever any new node enter in to the network it will check whether the node is hacking node or not by the reply it sending and inform to all other nodes about the new node for the secure data transmission.

If any node is not responding properly then the certificate authority checks the threshold value for that node. If the threshold value is in out of range then it mark the node is malicious node. The data transmission is not done through this node. If the threshold value is in range then the node is a trust node. The data transmission is done through this node. If the threshold value is not justified then the node is moved in to the warning list until the threshold value is justified. The certificate authority work properly and secure efficiently.

Certificate Authority is used to handle the security process which is important node in the network. It is going to take care of the entire network i.e., it monitors all the nodes and checks which are giving good response based on that it will allow other nodes to communicate with each other.Networks users are assigned aggregation privileges by the trusted authority in a public key infrastructure on behalf of the network owner. However, the network owner may, for various reasons, impersonate network users to aggregate data items.

The compromised entities are regarded as insiders because they are members of the network until they are identified. The adversary controls these entities to attack the network in arbitrary ways. For instance, they could be instructed to aggregate false or harmful data, launch attacks such as Sybil attacks or Denial of Service attacks and be non-cooperative with other nodes.

Data gathered by the individual nodes ultimately routed to the base station. A rate monitoring attack simply makes use of the idea that nodes closest to the base station tend to forward more packets than those farther away from the base station. An attacker need only monitor which nodes are sending packets and follow those nodes that are sending the most packets. Thus the node nearer to the base station is monitored continuously and transmits the data after finding that the node is a trust node.

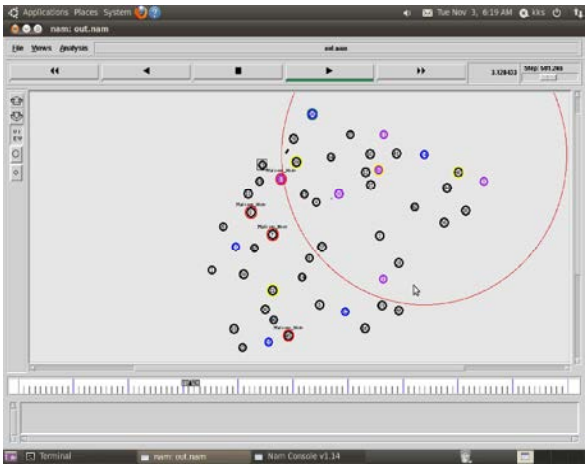


Fig. 5.1: Certificate Authority

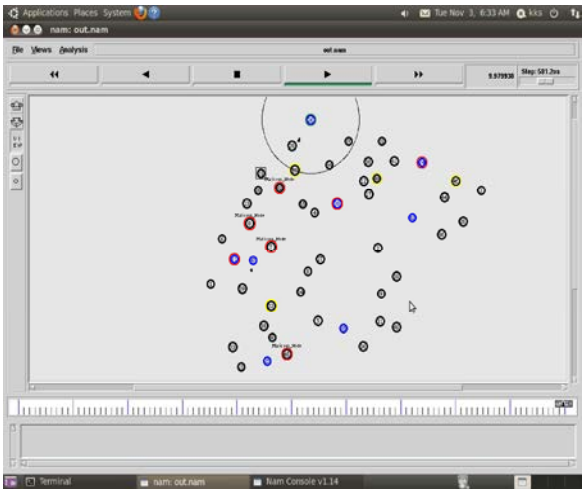


Fig. 5.2: Route Discovery Process

CONCLUSION

In this paper, we address the problem of reliable data delivery in highly dynamic mobile ad hoc networks. Continually changing network topology makes conservative ad hoc routing protocols incapable of providing satisfactory. performance. In spite of frequent link break due to node mobility, substantial data packets would either go astray. Stimulated by opportunistic routing, we propose a MANET routing protocol DPBR which takes advantage of the stateless property of geographic routing and broadcast nature of wireless medium. In addition selecting the next hop, several forwarding candidates are also explicitly specified in case of link break. Leveraging on such natural backup in the air, broken route can be recovered in a timely manner. The efficiency of the involvement of forwarding candidates against node mobility is analyzed. Through simulation, the effectiveness and efficiency of proposed routing method has confirmed. In addition, the metric high packet delivery ratio is achieved while the delay and duplication are the lowest.

REFERENCES

1. Mishra, K. Nadkarni and A. Patcha, 2004. "Intrusion detection in wireless ad hoc networks," IEEE Wireless Commun., 11(1): 48-60, Feb. 2004.
2. Hollick, M., J. Schmitt, C. Seipl and R. Steinmetz, 2004. "On the effect of node misbehavior in ad hoc networks," in Proc. IEEE Global Telecommun. Conf. GLOBECOM, Jun. 2004, pp: 3759-3763.
3. Cerri, D. and A. Ghioni, 2008. "Securing AODV: the A-SAODV secure routing prototype," IEEE Commun. Mag., 46(2): 120-125, Feb. 2008.
4. Yih-Chun, H. and A. Perrig, 2004. "A survey of secure wireless ad hoc routing," IEEE Security Privacy, 2(3): 28-39, May/Jun. 2004.
5. Ramkumar, M. and N. Memon, "An efficient key predistribution scheme for ad hoc network.
6. Sanzgiri, K., D. LaFlamme, B. Dahill, B.N. Levine, C. Shields and E.M. Belding-Royer, 2005. "Authenticated routing for ad hoc networks," IEEE J. Sel. Areas Commun., 23(3): 598-610, Mar. 2005.
7. Sun, B., K. Wu and U. Pooch, 2004. "Towards adaptive intrusion detection in mobile ad hoc networks," in Proc. IEEE Global Telecommun. Conf. GLOBECOM, Nov./Dec. 2004, pp: 3551-3555.
8. Yan, W., E. Hou and N. Ansari, 2005. "Extracting and querying network attack scenarios knowledge in IDS using PCTCG and alert semantic networks," in Proc. IEEE ICC, May 2005, pp: 1512-1517.