ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

A Survey on Secure Intrusion Detection using Routing Protocols against Malicious Attacks in MANETs

C.Logeshwari[1], S.Priyadarshini[2], C.Priyanka[3]

PG Scholar, Department of Computer Science and Engineering, Kalaignar Karunanidhi Institute of Technology, Coimbatore, India[1]

PG Scholar, Department of Computer Science and Engineering, Kalaignar Karunanidhi Institute of Technology, Coimbatore, India[2]

PG Scholar, Department of Computer Science and Engineering, Kalaignar Karunanidhi Institute of Technology, Coimbatore, India[3]

Abstract- Mobile ad hoc network is a wireless network with a group of mobile nodes. It consists of independent mobile nodes within the same transmission range. In this, during the data transmission some nodes are attacked by the malicious attackers. In recent years, security has grown to be a most essential service in Mobile Ad hoc Network. Compared to other networks, MANETs are more susceptible to various types of attacks. To detect the malicious attackers in the network some routing protocols such as, DSR, AODV and ZRP are used. Also, these secure routing protocols consist of two messages: the routing messages and the data messages. The two messages require different security and different route. In this paper, a survey on Secure Intrusion Detection Systems for detecting malicious attackers in MANETs is presented. Due to some particular characteristics of MANETs, prevention mechanisms alone are not sufficient to control the secure networks. First this paper gives an overview of IDS architecture for improving security level of MANETs and then a hybrid cryptography IDS to reduce the network overhead caused by digital signature is specified.

Keywords: Mobile ad hoc network, Attacks, Defense Mechanisms, Routing Protocol

1. INTRODUCTION

A mobile ad hoc network (MANET) is a self configuring network created without human intervention by a collection of mobile nodes. Each node is prepared with a wireless transmitter and receiver, and it allows communicating with other nodes in its same radio range. In the network each node must act as both a host and a router at the same time. The network topology often changes due to the mobility of mobile nodes and it moves in the network independently. There are two types of attacks in MANETs such as passive and active attacks. In passive attacks, packets including secret information might be overheard something, and it violates confidentiality. In active attacks, the problems that occur are the packets may be introduced to unacceptable destinations in the network, deleting packets, modifying the contents of packets, and masquerading as other nodes violate availability, integrity, authentication, and non-repudiation.

The communication between various nodes can be achieved using multi hop wireless links since the base stations are absent. The mobile nodes can be turned on or off at any time without reporting other nodes as they move randomly. Nodes maintain routing information in the routing table for data forwarding. In order to preserve the routing information available, the nodes need to know the topological changes that take place in the network. The applications of MANET are military operations, emergency rescue operations, disaster recovery etc. Several protocols have been developed for MANETs such as (Destination Sequenced Distance Vector) DSDV, (Dynamic Source Routing) DSR, (Ad hoc On Demand Routing) AODV, (Optimized Link State Routing) OLSR, (Greedy Perimeter Stateless Routing) GPSR, (Location Aided Routing) LAR. These protocols offer varying degrees of efficiency.

Intrusion detection system can be defined as the process of examining activities in system, which can be a computer or network system. Due to the restrictions of most MANET routing protocols, nodes in MANETs believe that other nodes always assist with each other to transmit data. This supposition disappear the attackers with the opportunities to achieve major force on the network with just one or two compromised nodes. To tackle this problem, Intrusion Detection System (IDS) should be added to develop the security level of MANETs [1]. Intrusion detection can be used as a second wall of defense to defend the network from such problems. If the intrusion is found, a response can be started to avoid or reduce scratch to the system. Intrusion detection can be

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

divided based on audit data as either host-based or network-based. A network-based IDS captures and examines packets from network traffic while a host based IDS uses operating system in its analysis. In this paper, we discussed about different types of routing protocols to avoid malicious attacks in the MANET.

2. LITERATURE REVIEW

In this section, since the IDS for traditional wired systems are not compatible to MANETs, many researchers have proposed several IDS particularly for MANETs.

2.1 Local Intrusion Detection System (LIDS)

Albers *et al.* [3] proposed a disseminated and collaborative architecture of IDS by using mobile agents. A Local Intrusion Detection System (LIDS) is implemented on every node for local concern, which can be extended for global concern by cooperating with other LIDS. In order to investigate the possible intrusion, data must be obtained from what the LIDS detect, along with other information from other nodes. Other LIDS may be run on dissimilar operating systems or use data from unlike activities such as system, application, or network activities; consequently, the format of this raw data might be different, which makes it hard for LIDS to analyze. Though, such complexities can be solved by using SNMP (Simple Network Management Protocol) data located in MIBs (Management Information Base) as an audit data source.

2.2 Dynamic Hierarchical Intrusion Detection

Sterne *et al.* [4] proposed a dynamic intrusion detection hierarchy that is probably scalable to huge networks by using clustering. Nodes labeled \1" are the first level cluster heads while nodes labeled \2" are the second level cluster heads and so on. The first level of the clusters is called leaf nodes. Each node has the responsibilities of supervising, sorting, analyzing (i.e., attack signature are similar or examining on packet headers and payloads), responding to intrusions detected if there is enough verification, and alerting or exposure to cluster heads. Normally used in MANETs to build routes, to self-organize into local neighborhoods (first level clusters) and then select neighborhood representatives (cluster heads). These representatives then use clustering to manage themselves into the second level and select the representatives. This process will be continued until all nodes in the network are part of the hierarchy.

2.3 Distributed Intrusion Detection System Using Multiple Sensors

O. Kachirski and R.Guha, [5] proposed a multi-sensor intrusion detection system based on mobile agent technology. The system can be divided into three main modules, each of which represents a mobile agent with certain functionality: monitoring, decision-making or initiating a response. By separating functional tasks into categories and assigning each task to a different agent, the workload is distributed which is suitable for the characteristics of MANETs. In addition, the hierarchical structure of agents is also developed in this intrusion detection system.

Monitoring agent: Two functions are carried out at this class of agent: network monitoring and host monitoring. A host-based monitor agent hosting system-level sensors and user-activity sensors is run on each node to monitor within the node.

Action agent: Every node also hosts this action agent. Since every node hosts a host based monitoring agent, it can determine if the any distrustful or abnormal activities on the host node based on anomaly detection. When there is strong substantiation sustaining the anomaly detected, this action agent can commence a response, such as terminating the process.

Decision agent: The decision agent is run only on certain nodes, mostly those nodes that run network monitoring agents. These nodes collect all packets within its radio range and analyze them to establish whether the network is under attack. The network is rationally separated into clusters with a single cluster head for each cluster. This cluster head will monitor the packets within the cluster and only packets whose originators are in the same cluster are captured and investigated. In this mechanism, the decision agent performs the decision-making based on its own collected information from its network-monitoring sensor.

2.4 Co-operative Intrusion Detection System

A cluster-based cooperative intrusion detection system has been presented by Huang and Lee [6]. In this system, an intrusion system is not only able to identify an intruder, but also to recognize the type of attack and the attackers, through anomaly detection. A variety of types of statistics, which are anticipated in their prior work, are estimated from a sampling period by detaining the basic view of network topology and routing operations. Therefore, attacks could be recognized if the statistics move away from the pre-computed ones (anomaly detection). Statistics can be categorized into two types, non traffic-related and traffic-related. Non traffic-related statistics are calculated based on the mobility and the trace log files, which can be done independently on every node. Traffic-related statistics are concerned in routing and packet forwarding and can be designed by counting packets going inside and outside, e.g. the number of packet received, the number of packet forwarded, the number of route reply messages, etc.

3. CLASSIFICATION OF ATTACKS

Nodes in MANET can be broken down, and it may be malicious or selfish. Broken nodes develop into non functional due to some link failure so cannot forward the traffic that they prior agree to forward. Malicious nodes intended at distracting the network by dropping the

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

packets or initiating denial of service attacks. Selfish nodes delay the routing by dropping packets in order to preserve their energy and bandwidth. To facilitate encourage it use in expectation, it is significant to make certain secure and reliable routing in MANET. So this paper focuses on attacks and security mechanisms employed to safeguard beside these attacks [7][2]. Attacks can be classified into two broad categories.

3.1 Passive Attacks

The attacker just interfere the network without disturbing the network operation. These attacks negotiation the confidentiality of the data and tell which nodes are working in immoral mode.

3.1.1 Eavesdropping

It is reading or snooping of messages by an unintended receiver. In MANET, the nodes share a wireless medium thus nodes can easily eavesdrop communication of the nodes within its transmission range. This attack can be prohibited by using encryption.

3.1.2 Selfishness

A selfish node with the intention of save its battery life and resources does not participate in routing either by reducing the packets or not forwarding them.

3.2 Active Attacks

Attacks in which attacker disordered the normal operation of the network by manufacturing messages, sinking or transforming packets, replaying packets or tunneling them to other part of the network. These can be internal attacks (caused by compromised nodes within the network) and external attacks (caused by the nodes outside the network).

Active attacks can be supplementary confidential corresponding to different layers in MANET:

3.2.1 Data Link Layer Attacks

Denial of service: There is a single wireless channel mutual by all the nodes so a malicious node remains this channel busy by sending false packets to consume node‘s battery power.

3.2.2 Physical Layer Attacks

Device Tampering: Nodes in ad hoc wireless networks are small, dense and hand-held dissimilar wired devices so can be easily stolen or damaged.

3.2.3 Multilayer attacks

These attacks can be commenced from several layers as a substitute of a single layer. Examples of multi-layer attacks are jamming, denial of service attacks, impersonation attacks and man-in-the-middle attack.

4. DEFENSE MECHANISM

In this section, discuss about defense mechanism for detecting malicious nodes and malicious attackers [2] [7]. There are three different types of mechanisms are used to find which is malicious nodes in the network.

4.1 Proactive Mechanism

It contains security-aware routing protocols that avoids amount of attacks. These protocols should be required to take the environment features and form first line of defense as prevention is better than cure. It comprises cryptographic algorithms and trust based mechanism to make certain integrity, authentication and confidentiality of the messages.

4.2 Conviction Based Mechanism

In this, secure routing protocols use belief as security metric to keep away from inclusion of malicious or selfish nodes while creating routes. Every node verifies the trust, it is directly communicating with neighboring nodes and also combining other nodes recommendations. A node can make a decision whether to exchange routing information with it or not. Generally, trust based schemes use IDS for monitoring neighborhood traffic but need buffering of packets which may use computational resources.

4.3 Hybrid Mechanisms

Cryptographic mechanisms being more exclusive and conviction based being few secured, so hybrid protocol must be produced that merges the advantages of both mechanisms. To facilitate secure trust metric in the routing packets, a lightweight security mechanism must be integrated to get hybrid protocol which is a smaller amount expensive than cryptographic mechanism and more secure than conviction based. Future protocol designs should focus on using combination of conviction-based metrics and lightweight security mechanisms

5. ROUTING PROTOCOLS

In this section, a routing protocol is needed when a packet wants to be transmitted to a destination through number of nodes. Routing is the process of finding a routing from a source to destination in the network. These protocols find a route for packet delivery from source to destination. The various Proactive and Reactive protocol like DSR, AODV, and ZRP [8].

5.1 Dynamic Source Routing (DSR)

The Dynamic Source Routing (DSR) protocol is an on-demand routing protocol. In the source routing, a sender establishes the exact sequence of nodes through which to transmit a packet. In DSR, every node in the network wants to preserve a route cache. When a node wants to send a packet to some other node, first checks its route cache for a source route to the destination. In the case a route is found, the sender uses this route to transmit the packet. Otherwise, source node initiates the route discovery to find a different path between two nodes. Initially, source node sends the route request to the

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

destination node then after receiving the request the destination node sent the acknowledgement with the route reply. Likewise, it finds an alternative path to sends the packets to other nodes. This path will not be visible to attackers. So, malicious attackers cannot find the path in this routing protocol.

5.2 Ad hoc On-demand Distance Vector (AODV)

The Ad Hoc On-Demand Distance Vector routing protocol (AODV) is an improvement of the Destination-Sequenced Distance Vector routing protocol (DSDV). It generates the routes on an on-demand basis, as different to retain a complete list of routes for each destination. In route discovery process, the source node sends the route request to the destination and also sent to the neighbor nodes. Until the intermediate node knows the route it sends packet continuously. After receiving the packet the destination node sends back acknowledgement to the source node. In maintaining routes, intermediate node beside the forward path moves, its upstream neighbor perceives the move and propels a link failure notification message to each of its active upstream neighbors to inform them of the removal of that part of the route.

5.3 Zone Routing Protocol (ZRP)

In MANET, most of the communication takes place between nodes close to each other. Each node defines its own zone size, and the zone size is defined as number of hops to the zone perimeter. For example, the zone size may depend on signal strength, available power, reliability of different nodes. ZRP is not very dissimilar while providing framework for other protocols.

6. CONCLUSION

In this paper, almost all the intrusion detection has discussed and which was used in MANETs. To secure intrusion detection system, the different types of defense mechanisms were used. Intrusion detection system for mobile ad hoc networks has concerned much awareness newly due to increased usage of mobile ad hoc networks. With the nature of mobile ad hoc networks, almost all of the intrusion detection systems (IDSs) are prearranged to be disseminated and have a cooperative architecture. An intrusion detection system aims to perceive attacks on mobile nodes or intrusions into the networks. Though, attackers may endeavor to attack the IDS system itself. Consequently, the study of the defense mechanisms to such attacks should be investigated as well. The security solution must include wider outlook involving both known and unknown attacks. There is an exchange between security and network performance. So, conclude that using the defense mechanism intrusion detection of MANETs was secured.

REFERENCES

[1]. Y. Zhang, W. Lee, and Y. Huang, “Intrusion Detection Techniques for Mobile Wireless Networks,” *ACM/Kluwer Wireless Networks Journal (ACM WINET)*, Vol. 9, No. 5, September 2003.

[2]. H. Yih-Chun Hu; Perrig, A.; Johnson, D.B., Wormhole attacks in wireless networks, *Selected Areas in Communications, IEEE Journal on* , vol. 24, no. 2, pp. 370- 380, 2006

[3]. P. Albers, O. Camp, J. Percher, B. Jouga, L. M, and R. Puttini, “Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches," *Proceedings of the 1st International Workshop on Wireless Information Systems (WIS-2002)*, pp. 1-12, April 2002.

[4]. D. Sterne, P. Balasubramanyam, D. Carman, B. Wilson, R. Talpade, C. Ko, R. Balupari, C.-Y. Tseng, T. Bowen, K. Levitt, and J. Rowe, “AGeneral Cooperative Intrusion Detection Architecture for MANETs," *Proceedings of the 3rd IEEE International Workshop on Information Assurance (IWIA'05)*, pp. 57-70, March 2005.

[5]. O. Kachirski and R. Guha, “Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks," *Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS'03)*,p. 57.1, January 2003.

[6]. Y. Huang and W. Lee, “A Cooperative Intrusion Detection System for Ad Hoc Networks,” *Proceedings of the ACM Workshop on Security in Ad Hoc and Sensor Networks (SASN’03)*, pp. 135-147, October 2003.

[7]. A.J. Menezes, S.A. Vanstone, P.C. Van Oorschot, “Handbook of Applied Cryptography”. CRC Press, Inc., USA, 2001.

[8]. D.B. Johnson, D.A. Maltz, et.al. “The dynamic Source Routing Protocol for Mobile Ad hoc Networks (DSR)”. Internet Draft, draft-ietf-manet-dsr-07.txt, work in progress, 2002.