Intrusion detection System for Attack Prevention in Mobile Ad-hoc Network

Tapan p.Gondaliya[1], Maninder Singh[2]
[1] Research Scholar, Lovely University, Phagwara.,
[2] Associate Professor, Dept of Computer Science, Lovely University, Phagwara

Abstract:
Mobile Ad-hoc Networks prove to be the best fit for various applications like Military operations, Flood affected areas, Remote area etc. Ad-hoc Networks are limited with energy and generally more venerable to various attacks as compared to other types of networks. Insider attacks are one of the active attacks occurred in Ad-hoc network. These attack are very common in case of Reactive Protocols like Ad-hoc On Demand Distance Vector Protocol. In this research, an intrusion detection system will be developed for detection and isolation of attacks. In this Research, mac layer applications will be used for detecting malicious activities and will focus on the finding of attack sequences in the Network. This Research will provide stable and effective attack observations which can be directly applicable to the Real environment for Mobile Ad-hoc Devices.

Keywords: *Mobile Ad-hoc Network, Insider Attack, Ad-hoc On Demand Distance Vector Protocol, Intrusion Detection System, Routing Protocols, Route Request, Route Reply.*

1. Ad-hoc Networks

Centralized networks, such as GSM, don't have capability to use everywhere in all situations. Some popular examples of these types of networks include establishing survivable monitoring, reliable with efficiency, dynamically adaptive communication for rescue operations in emergency, disaster relief efforts and different type of unique/ non-unique military networks. These types of network scenarios cannot be a centralized and organized connectivity and it can be act as applications of MANETs. The huge chunk of applications for MANETs is widely ranging from small to largely diversify, ranging from small to big, static to dynamic networks that are constrained by very limited power sources, mobility terms comes in scene always, and highly movable or dynamic networks.

To use or enable multi-hop communication in a widely driven and distributed environment, all nodes should be capable of acting as small transferring router/ switch according to demand (see Figure 1.1). Intermediate path (Routes) has been created and maintained by some routing protocol. MANET routing protocol designed in a complexity of having capability to handle the dynamically changing environment as discussed earlier so that rapidly changing topologies and environments can be covered by these protocols. For route maintenance one has two main approaches in MANETs, reactive and proactive. Reactive routing protocols create on demand routes which saves huge resources. On the other hand proactive protocols have to maintain whole table of topology in timely dynamic environment.

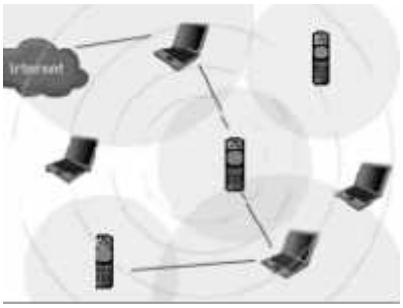

Figure.1.1. A A typical MANET [4]

Mobility varies according to the network behavior and each node act as a router for next node for the communication. Traffic is only transmitted to nearby neighbors within the radio range when these network working in the ad-hoc manner, which in turns required manet routing protocols to set up and maintain traffic paths.

2. Routing in MANET

Routing means to choose a path. Routing in MANET means to choose a right and suitable path from source to destination. Routing terminology is used in different kinds of networks such as in telephony technology, electronic data networks and in the internet network. Here work is more concern about routing in mobile ad hoc networks [4]. Routing protocols in mobile ad hoc network means that the mobile nodes will search for a route or path to connect to each other and share the data packets [2]. Protocols are the set of rules through which two or more devices (mobile nodes, computers or electronic devices) can communicate to each other. In mobile ad hoc networks the routing is mostly done with the help of routing tables. These tables are kept in the memory cache of these mobile nodes [4]. When routing process is going on, it route the data packets in different mechanisms. The first is unicast, in which the source directly sends the data packets to the destination. The sec is multicast, in this the source node sends data packet to the specified multiple nodes in the network [4].

The third is broadcast; it means the source node sends messages to all the near and far nodes in the network.
Routing has two basic types, which are as under.

Static Routing: is done by the administrator manually to forward the data packets in the network and it is permanent. No any administrator can change this setting [3]. These static routers are configured by the administrator, which means there is no need to make routing tables by the router itself.

Dynamic Routing: is automatically done by the choice of router. It can route the traffic on any route depend on the routing table. Dynamic routing allows the routers to know about the networks and the interesting thing is to add this information in their routing tables. In dynamic routing the routers exchange the routing information if there is some change in the topology [4]. Exchanging information between these dynamic routers learn to know about the new routes and networks. Dynamic routing is more flexible than static routing. In dynamic routing it have the capability to overcome the overload traffic. Dynamic routing uses different paths to forward the data packets. Dynamic routing is better than static routing [4].

3. AODV (Ad hoc On-demand Distance Vector)

AODV is an on-demand routing protocol. The AODV algorithm gives an easy way to get change in the link situation. For example if a link fails notifications are sent only to the affected nodes in the network. This notification cancels all the routes through this affected node. [6] It builds unicast routes from source to destination and that's why the network usage is least. Since the routes are build on demand so the network traffic is minimum. AODV uses Destination Sequence Numbers (DSN) to avoid counting to infinity that is why it is loop free. This is the characteristic of this algorithm. When a node send request to a destination, it sends its DSNs together with all routing information. It also selects the most favorable route based on the sequence number [8]. There are three AODV messages i.e. Route Request (RREQs), Route Replies (RREPs), and Route Errors (RERRs) [4]. By using UDP (user datagram protocol) packets, the source to destination route is discovered and maintain by these messages. For example the node which request, will use its IP address as Originator IP address for the message for broadcast. It simply means that the AODV not blindly forwarded every message. The number of hops of routing messages in ad hoc network is determined by Time-To-Live (TTL) in the IP header. [9]

Fig.1.2. RREQ and RREP messages in MANET using AODV [6]

When the source node wants to create a new route to the destination, the requesting node broadcast an RREQ message in the network [9]. In the figure 1.2 the RREQ message is broadcasted from source node A to the destination node B. The RREQ message is shown by the black line from source node A to many directions. The source node A broadcasts the RREQ message in the neighbor nodes [4]. When the neighbor nodes receive the RREQ message it creates a reverse route to the source node A. This neighbor node is the next hop to the source node A. The hop count of the RREQ is incremented by one. The neighbor node will check if it has an active route to the destination or not. If it has a route so it will forward a RREP to the source node A. If it does not have an active route to the destination it will broadcast the RREQ message in the network again with an incremented hop count value. The figure 1.2 shows the procedure for finding the destination node B [4]. The RREQ message is flooded in the network in searching for finding the destination node B. The intermediate nodes can reply to the RREQ message only if they have the destination sequence number (DSN) equal to or greater than the number contained in the packet header of RREQ.

4. Insider/ Jamming Attacks in MANET Network

The open nature of the wireless medium leaves it vulnerable to jamming attacks. Jamming in wireless networks has been primarily analyzed under an external adversarial model, as a severe form of denial of service (DoS) against the PHY layer. [2] Existing anti-jamming strategies employ some form of spread spectrum (SS) communication, in which the signal is spread across a large bandwidth according to a pseudo-noise (PN) code. However, SS can protect wireless communications only to the extent that the PN codes remain secret. Insiders with knowledge of the commonly shared PN codes can still launch jamming attacks. [2] Using their knowledge of the protocols specifics, they can selectively target particular channels/layers/protocols/packets. We will describe two types of selective jamming attacks against WMNs, which employ channel and data selectivity.

5. Problem Definition

MANET is a mobile ad-hoc network which dynamically set up temporary paths between mobile nodes which acts both as router and hosts to send and receive packets so it is more vulnerable to attacks and one of them is Wormhole Attack. In insider attacks it is very difficult to deal with inside information preservation due to full privilege to all nodes. These attacks can be easily implemented in AODV during the routing discovery process due to on demand discovery nature of reactive protocol. An attacker can create a safe attack sequence and can launch attack after sequence is on full control and flow can be controlled by attacker. To avoid these attacks we will provide a mac layer monitoring through an intrusion detection system.

6. Proposed Work

This research will focus on providing solution for said problem by implementing a mac layer monitoring through intrusion detection system resulting in regaining of the normal state of the network.

This research will be focused on the providing header information of all the nodes which are connected in the single mobile ad-hoc network and will monitor the activities of the nodes. If any node found to be produces uneven behavior or providing extra utilization of resources then normal then intrusion system will consider it as suspected node for any attack sequence observation. Regular monitoring will be fetched and frequent updates by suspected node will be judged. Multicasting solutions will be opted to find the multiple nodes misbehavior. In our basic study, we have implemented a basic structure for mobile networks by implementing it in Network simulator. Ad-hoc on demand and Multicast on demand protocols have been implemented.

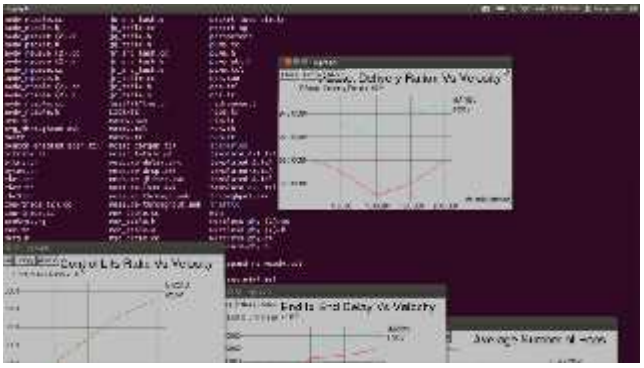

Figure 4: Packet delivery ratio of both protocols.

7. Conclusion

This Research will prove to be a good solution for saving resources while finding the malicious nodes in Mobile Ad-hoc Network and also will be effective in finding insider attack perfectly. This Research is still in process and experimentation in running phase to test the developed algorithm on Mobile Ad-hoc Networks. A new concept has been developed which can detect attacks with limited energy used.

References

[1] Bo Sun, Kui Wu, Udo W. Pooch, "Zone-Based Intrusion Detection for Mobile Ad Hoc Networks", Journal on Adhoc Networks in gurd conference, Vol.10, No. 7, pp 1179-1190, March 2010.

[2] Loukas Lazos, and Marwan Krunz, "Selective Jamming/Dropping Insider Attacks in Wireless Mesh Networks" An International Journal on Engineering Science and Technology Arizona edu, Vol.2, No. 2, pp 265-269, April 2010.

[3] Ajay Prakash Rai, Vineet Srivastava, Rinkoo Bhatia, "Wormhole Attack Detection in Mobile Ad Hoc Networks", International Journal of Engineering and Innovative Technology, Vol.2, No. 2, pp 384-389, August 2012.

[4] Routing protocols and concepts, CCNA exploration companion guide. ''Introduction to dynamic routing protocols''. Chapter three, pp 148-177.

[5] R.Vidhya, G. P. Ramesh Kumar, "Securing Data in Ad hoc Networks using Multipath routing", International Journal of Advances in Engineering & Technology, Vol.1, No. 5, pp 337-341, November 2011.

[6] K.Kiruthika Devi, M.Ravichandran, "Detecting Sinking Behavior at MAC and Network Layer Using SVM in Wireless Ad hoc Networks, International Journal of Computer Science and Network (IJCSN), Vol. 1, Issue. 3, pp. 12-16,June 2012.

[7] Turgay Korkmaz, "Verifying Physical Presence of Neighbors against Replay-based Attacks in Wireless Ad Hoc Networks", Information Technology: Coding and Computing, International Journal of Information Technology , Vol. 2, No. 2, pp 704-709, April 2005.

[8] Van Phuong T., Ngo Trong Canh, Young-Koo Lee, Sungyoung Lee, Heejo Lee, " Transmission Time-based Mechanism to Detect Wormhole Attacks", IEEE Conference on Asia-Pacific Service Computing Conference, pp 172- 178, December 2007.

[9] Ma Hongwei, "The Study on Ad hoc Networks Security Strategy based on Routing Protocols", IEEE International Conference on Computer Science and Network Technology, Vol.1, No.4, pp 445-449, December 2011.

[10] E.A.Mary Anita, V.Thulasi Bai, E.L.Kiran Raj, B.Prabhu, "Defending against Worm Hole Attacks in

Multicast Routing Protocols for Mobile Ad hoc Networks" IEEE International Conference on Information Theory and Aerospace & Electronics Systems Technology, pp 1–5, March 2011.