International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 2 257– 260

Survey on Hybrid IDS for Mobile Ad-hoc Networks

Mangesh Bhusari
CSE Department, P.I.E.T
Nagpur, India
bhusarimangesh@gmail.com

Ashish Sambare
Asst. Prof., P.I.E.T
Nagpur, India
ashishsambare@hotmail.com

Sachin Jain
Asst. Prof., P.I.E.T
Nagpur, India
Sacchinjain98440@rediffmail.com

Abstract— Due to its special capability of creating self configuring and self maintaining network without taking help of centralized or fixed network infrastructure, MANET is becoming increasingly popular and widely accepted wireless network. Minimum configuration, easy and quick deployment makes MANET an obvious choice for military and emergency applications. Many of the routing protocols used for MANET assumes that all the nodes in the network are cooperative to each other and are not malicious. Such assumptions and some of its unique characteristics make MANET susceptible for variety of passive as well as active attacks. Thus it is vital to have an intrusion detection system (IDS) designed especially for MANET. An overview of such intrusion detection systems is given in this paper. Many of these systems are dependent on acknowledgment packets for detection of intrusions. Digital signature and hybrid cryptography can be used to address such dependency.

Keywords- *Acknowledgment packets, Intrusion Detection System (IDS), Mobile Ad-hoc Network (MANET), Malicious node.*

*****

I. INTRODUCTION

Many historical studies have shown that intrusion prevention techniques alone, such as encryption and authentication are not sufficient. As the system become more complex it becomes vulnerable to more weaknesses which causes security problems. Intrusion detection can be used as a mechanism for defense in such scenarios to protect the network from such potential security threats. When intrusion is detected, certain activity can be carried out to prevent or minimize damage to the system. Intrusion can be any activity or action that is carried out by attackers to disrupt the normal operation of the network and intrusion detection system is nothing but the system that is designed specially to detect such activity or action [9].

MANET is a collection of mobile nodes that cooperates with one another for data and resources. MANET has many interesting characteristics that makes it a bit different compared to other wireless networks. Mobile nodes in MANET are equipped with both a wireless transmitter and a receiver. By making use of which nodes communicate with each other via bidirectional wireless links either directly or indirectly. Unlike traditional wired systems wireless networks allow data communication between different nodes and still maintain their mobility. Nodes that are in each other's radio range can communicate while maintaining their mobility .MANET makes it possible for nodes that are not in range of one another to communicate by making use of intermediate nodes as relay nodes. This means that nodes have to forward packets for other nodes [10] ,[11].

Basically MANET is of two kinds, Single hop MANET and Multi hop MANET. In single hop network the nodes that are in the range of each other can directly communicate via bidirectional wireless link between them. This kind of MANET does not use relays to transmit data packets. The multi hop network requires the intermediate nodes to forward packet from source to destination when they are not in the radio range of one another.

Unlike traditional wireless networks, MANETs do not need expensive or wired infrastructure to support mobility. In some scenarios such as military missions, disaster recovery or temporary networks, conventional wireless networks are not suitable for usage. In such scenarios we need a fast deployment and self organized network that will be used just for a specific purpose in a predetermined period of time. MANETs are decentralized, self-configuring, self-organizing networks, and are capable of forming a network without any fixed infrastructure. Minimal configuration and quick deployment make MANET ready to be used in emergency circumstances.

Since it has these unique characteristics, MANET is becoming more and more widely implemented wireless network in industry [12],[13]. However, considering the fact that MANET is popular among critical applications, network security in MANET is susceptible because of the open medium and remote distribution of MANET environment. Hence it is vital to have an intrusion detection system (IDS) designed especially for MANET that will address the problem of detecting the correct intrusions while tackling the unique characteristics of MANET environment.

II. LITERATURE SURVEY

Marti et al. [1] proposed a technique that is efficient in detecting misbehaving nodes in MANETs. This technique works in accordance with the routing protocol and has two parts namely Watchdog and Pathrater. Watchdog detects the nodes which are misbehaving and marks them as malicious nodes. Pathrater then coordinate with routing protocol to avoid use of these malicious nodes while finding routes.

Watchdog identifies misbehavior by listening to the transmission of node which is at one hop distance from it further on the route towards destination. This is possible because of the characteristics of wireless networks. If the next node does not forward the given packet in a predefined amount of time, its failure counter is incremented by one. When failure count of any node crosses the predefined threshold then it is marked a malicious.

Fig 2.1 shows the working of watchdog. Assume S and D are the source and destination respectively of the ongoing transmission. Similarly X, Y and Z are the intermediate nodes on the route from S to D. Node X receives packet from node S and forwards it to node Y. It keeps a copy of this packet in its buffer.

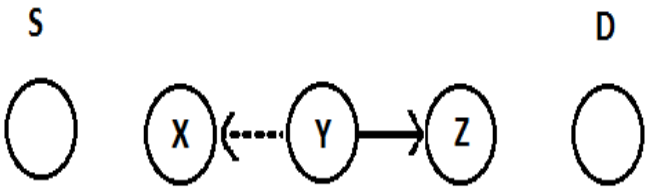

Figure 2.1 Working of Watchdog

Node X then starts listening to the transmission of Y. If the packet overheard form node Y is same as the one in its buffer then node X concludes that Y has successfully forwarded the packet to next node. Otherwise if node Y fails to forward the packet in some predefined amount of time, node X increments the failure counter of node Y and it is marked as malicious node when its failure count exceeds the threshold.

A MANET with watchdog and pathrater is efficient in detecting the malicious nodes and selecting routes which does not have misbehaving nodes. Many of the intrusion detection systems that are designed for mobile ad-hoc networks are either based on watchdog or developed as an enhancement of it. Watchdog technique fails to identify misbehavior under presence of certain scenarios like ambiguous collisions, receiver collisions, limited transmission power, false misbehavior report, collusion and partial dropping.

In [2] Nasser and Chen proposed a method to especially tackle the false misbehavior report problem to find out misbehaving nodes in MANETs. This scheme is called as ExWatchdog which signifies extension of original Watchdog scheme. In false misbehavior report problem malicious nodes deliberately reports an innocent node as a misbehaving node while they are in fact the intruders. In ExWatchdog scheme each node needs to maintain information regarding the number of packet it receives, forwards and sends. This information is recorded in tabular form. Each node maintains three tables namely for received, sent and forwarded packets.

Whenever the source node receives a misbehavior report, instead of directly trusting the report the source node find out another path to the same destination and send a query packet to it. In this query packet source node asks the destination nodes about the number of data packets received by destination. If the destination node receives the same number of packets as send by the source then the node which sends the misbehavior report is in fact the malicious node. Otherwise the misbehavior report is trusted and nodes that are reported malicious in it are the real intruders. A major drawback of this scheme is when there is no path from the given source to the destination that does not contain the real misbehaving node in it then it is impossible to check the number of packets received by destination node.

In [3] Patcha and Mishra extended the Watchdog mechanism and proposed a scheme designed to address the collusion attacks. In this scheme the nodes which initially form the MANET are assumed to be the trusted nodes while the nodes that would join the MANET later are assumed as ordinary nodes. This assumption is made to detect malicious nodes when multiple nodes collaborate to carry out misbehavior. One of the trusted nodes is selected as watchdog node which eliminates the possibility of false misbehavior reporting. A watchdog node in this scheme maintains couple of thresholds namely, suspect threshold and acceptance threshold, for all the ordinary nodes that are its neighbors. The suspect threshold gives the count of total number of misbehaving nodes and the acceptance threshold gives the count of total number of nodes that are behaving properly. Based on these two threshold values the watchdog node makes the decision that whether its neighboring node is malicious node or trusted node.

Parker *et al.* [4] proposed an enhancement over the watchdog technique. Unlike original watchdog technique that is designed to be used only with DSR protocol, this new scheme can be used with all the routing protocols used in MANETs. In the original watchdog scheme the watchdog node only listens to the next node's transmission which is on the forward route. But in this new scheme the watchdog node listens to transmission of all the neighboring nodes that are in its radio range. Every node gives response in two ways namely passive and active. In passive response mechanism each node has the liberty to act independent of others. Thus ultimately the malicious node is blocked from using the resources provided by network. In the other response mechanism the misbehavior is detected by using a voting process. The node is identified as malicious if majority of the nodes votes against it and when this happen, an alert is broadcasted throughout the network. As a result the malicious node will not be able to use the network resources from this point onwards.

All the above mentioned schemes are either watchdog based schemes or an enhancement to original watchdog scheme. Many other researchers have worked on acknowledgment based systems for detecting intrusion in MANETs; some of the most efficient acknowledgment based schemes are given below.

A scheme called TWOACK proposed by Deng et al. in [5] is one of the most promising schemes that aimed at overcoming the problematic scenarios experienced by watchdog. TWOACK is an entirely new approach and is not based on watchdog technique. In TWOACK scheme, nodes on the route from a given source to intended destination works in coordination with each other. Specifically, every three consecutive nodes logically work as a group. Every third node in the group of three has to send back a TWOACK acknowledgement packet to the first node of the group. This acknowledgement indicates that third node has successfully received a data packet from second node which simply relays the packets from first node to third node. When the first node receives TWOACK packet in a predefined amount of time it concludes that transmission of data packet up to the third node is successful otherwise it marks both, the second and third node as malicious nodes. In general each node on the route has to send a TWOACK acknowledgment packet to a node which is at two hop distance from it in the backward direction on the same route. TWOACK scheme successfully resolves limited

transmission and receiver collision problems.

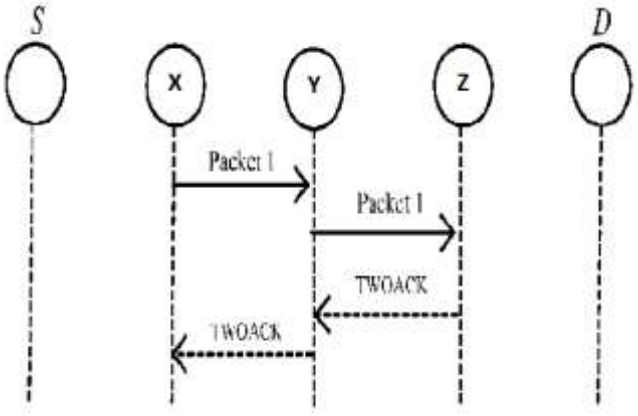

Figure 2.2 Working of TWOACK

compared to TWOACK scheme. The routing overhead caused

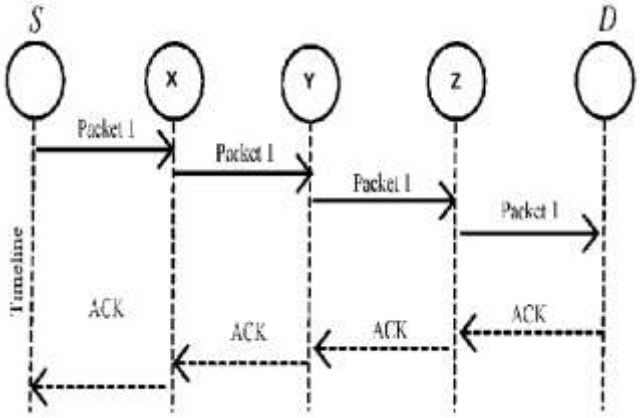

Figure 2.3 Working of End to End acknowledgment

Fig, 2.2 shows working of TWOACK nodes S and D are assumed as source and destination respectively whereas X.Y and Z are intermediate nodes. X, Y and Z are consecutive three nodes thus node Z must send back TWOACK acknowledgment packet for every data packet received by it. As shown in fig. node X receives packet 1 and send it to node Y which simply forwards it to node Z. Upon receiving packet 1 node Z creates a TWOACK packet and send it to node X via node Y.

TWOACK schemes runs on top of routing protocols like DSR. Since every node in the network needs to send an acknowledgement packet for every single data packet it receives, this scheme induces processing overhead in the network. Processing so many acknowledgement packets also consumes a lot of battery of the nodes which is very vital resource in MANET. Thus this scheme eventually degrades the life span of the network.

An enhancement over the basic TWOACK scheme was proposed by Liu *et al.* in [6] named as 2ACK. The major difference in the working process of 2ACK is that unlike TWOACK, 2ACK does not require an acknowledgement packet to be sent for every data packet received. In 2ACK scheme each node in the route for given source and destination pair, sends acknowledgment packet called 2ACK for a fraction of total number of data packets received. This allows 2ACK to address the performance issues in much better way as compared to TWOACK. Another improvement over TWOACK scheme is, in 2ACK the acknowledgment packets are guaranteed to be genuine as 2ACK scheme makes use of authentication mechanism.

Sheltami *et al.* in [7] developed a method that is based on TWOACK scheme. This is an acknowledgment based network layer scheme built on top of DSR protocol. The technique is named as adaptive acknowledgment (AACK) and can be considered as a hybrid system having combination of two schemes. The first scheme is an end to end acknowledgment scheme called ACKnowledge (ACK) and the other scheme is an enhanced version of basic TWOACK scheme called TACK. AACK scheme reduces the network overhead as by TWOACK scheme is also reduced to great extent by AACK. This scheme improves the overall efficiency of the TWOACK scheme.

Fig. 2.3 shows working of end to end acknowledgment scheme. Nodes S and D are the source and destination of the ongoing transmission respectively. Nodes X, Y and Z are intermediate nodes. Node S sends the data packet to node X which simply forwards it to next intermediate node Y which in turn forwards it to destination D. In end to end acknowledgment scheme intermediate nodes simply relays the data packet unlike TWOACK where intermediate nodes also needs to create acknowledgment packets. When node D receives the packet sent from node S, it sends back an acknowledgment packet to source node S. If node S receives this acknowledgment in predefined amount of time then communication is considered to be successful otherwise not.

The source node in AACK schemes basically works in two modes, TACK mode and ACK mode which is the default mode. When source node does not receives the acknowledgment in the predefined time then the mode is switched to TACK mode. One bit in the reserved field of DSR header used to identify the type of packet. Depending on this bit the intermediate nodes decides whether it should simply relay the packet or create TACK acknowledgment packet in TACK mode. In addition AACK scheme maintains two timeout thresholds one for each mode.

Though it reduces the overhead to great extent, AACK still fails in presence of false misbehavior report and forged acknowledgment packets.

One of the best acknowledgment based schemes for intrusion detection in MANETs is proposed by Shakshuki *et al.* in [8].The scheme is called as Enhanced Adaptive Acknowledgment (EAACK). This technique overcomes from three drawbacks of watchdog scheme namely limited transmission power, receiver collision and false misbehavior reports. In addition to that EAACK makes use of digital signature in order to prevent malicious nodes from forging the acknowledgment packets.

The EAACK scheme is a hybrid intrusion detection system

consisting four major parts as ACK, S-ACK, MRA and Digital signature. ACK is an end to end acknowledgment system as discussed before. S-ACK is a secure acknowledgment scheme which work on the similar basis as that of TWOACK. MRA stands for misbehavior report authentication and it is used to detect false misbehavior reporting of innocent nodes by malicious nodes. MRA focuses on verifying whether the destination node has received the allegedly missing packet. To do this MRA makes use of an alternate path to the same destination. Whenever the source node encounters a misbehavior report, it searches another path to the destination in its knowledge repository. On this new path it sends a packet to the destination node asking whether it has received the missing packet in the last transmission. When destination node receives this packet it checks for the missing packet and if it has received the packet then it is evident that the misbehavior report is false and hence this report must be discarded. Thus the node which has generated this report is marked as malicious node. If this is not the case the report is trusted and nodes that are marked malicious in it are blocked in the network. EAACK is an acknowledgment based hybrid system. To detect the intrusion this scheme heavily relies on acknowledgment packets. Sometimes it is possible that the attacker may send an acknowledgment packet that appears to be sent by legitimate node. This type of forged acknowledgment packet may hamper the performance of the system hence EAACK scheme makes use of digital signatures to provide authenticity. Due to this EAACK is capable of overcoming another drawback of watchdog called forged acknowledgment packets.

To differentiate between the types of packet two bits in the reserved bits of DSR header are utilized. EAACK is considered to be one of the best acknowledgment based approach designed for intrusion detection in MANETs. It provides high number of correct intrusion detection while still maintaining considerably efficient performance. However use of digital signature introduces additional network overhead.

III. CONCLUSION

The survey shows that it is vital to have especially designed intrusion detection system for MANETs that addresses its special and unique characteristics. Many researchers have worked on the specific security attacks while others have worked on providing a system that can resolve number of security and performance related issues. Making use of acknowledgment based intrusion detection schemes in MANET provides correct intrusion detections while maintaining good performance. Watchdog based techniques suffers from performance issues and fails to detect intrusion in presence of certain scenarios that are often seen in MANET environment.

. REFERENCES

[1] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad-hoc Networks," Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom'00), PP. 255-265, August 2000.

[2] N. Nasse and Y. Chen, "Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad-hoc Networks," IEEE International Conference,vol., no., pp.1154-1159, 24-28 June 2007.

[3] A. Patcha and A. Mishra, "Collaborative security architecture for black hole attack prevention in mobile ad-hoc networks," Radio and Wireless Conference, RAWCON '03. Proceedings, vol., no., pp. 75-78, 10-13 Aug. 2003.

[4] J. Parker, J. Undercoffer, J. Pinkston and A. Joshi, "On intrusion detection and response for mobile ad-hoc networks," Performance, Computing, and Communications, 2004 IEEE International Conference, vol., no., pp. 747-752, 2004.

[5] K. Balakrishnan, J. Deng, and P.K. Varshney, "TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks," Proc. IEEE Wireless Comm. and Networking Conf. (WCNC '05), Mar. 2005.

[6] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An Acknowledgment-based Approach for the Detection of Routing Misbehavior in MANETs," IEEE Transactions on Mobile Computing, vol. 6, no. 5, pp. 536-550, May 2007.

[7] Al-Roubaiey, T. Sheltami, A.Mahamoud, E. Shakshuki and H. Mouftah, "AACK: Adaptive Acknowledgment Intrusion Detection for MANET with Node Detection Enhancement", 24th IEEE International Conference on Advanced Information Networking and Applications,pp. 634-640,2010.

[8] E. Shakshuki, Nan Kang and T.M. Sheltami, "EAACK- A secure intrusion detection system for MANETs",IEEE trans. Industrial electronics, vol. 60, no. 3,pp. 1089-1098,March 2013.

[9] T. Anantvalee and J, Wu, " A Survey on intrusion detection in mobile ad-hoc networks", in Wireless/Mobile security, New York springer Verlag 2008.

[10] G. Jayakumar and G. Gopinath, "Ad hoc mobile wireless network routing protocol-A review ," J.Comput. Sci.,vol.3, no. 8,pp.574-582,2007.

[11] B. Sun, "Intrusion detection in mobile ad-hoc networks," Ph.D dissertation,Texas A&M Univ,. Collage Station, TX 2004.

[12] K. Kuladinith, A. S. Thimm-Giel and C. Gorg, "Mobile ad-hoc communications in AEC industry," J. Inf. Tecnol. Const.,vol.9, pp.313-323,2004.

[13] K. Stanoevska-Slabeva and M. Heitmann, "Impact of mobile ad-hoc networks on the mobile value system," in Proc. 2nd Conf. m-Bus., Vienna, Austria, Jun. 2003.