ISSN:0975-9646

A Survey on Intrusion detection System for Mobile Ad-hoc Networks

Ranjit j. Bhosale
Master of Engineering,
Department of Computer Engineering
Sinhgad institute of Technology, Lonavala,
University of Pune, Pune.

Prof. R.K.Ambekar
Dept. of Computer Engineering
Sinhgad institute of Technology, Lonavala,
University of Pune, Pune.

***Abstract*— The mobile ad-hoc networks (MANET) is a new wireless technology, having features like dynamic topology and self-configuring ability of nodes. The self -configuring ability of nods in MANET made it popular among the critical mission such as military use and emergency recovery. But due to the open medium and wide distribution of nodes make MANET vulnerable to malicious attackers. So to protect MANET from various attacks, it is crucial to develop an efficient secure intrusion-detection system for MANET. In this paper, we focus on various intrusion-detection system in MANETs.**

***Keywords*— Intrusion detection system,Malicious nodes, Misbehaviour report, Acknowledement.**

I. INTRODUCTION

Wireless networking is the platform for working with the current technology widely used in several applications. Mobile Ad-hoc Network(MANET) is a collection of wireless mobile node, consists of both wireless transmitters and receivers, which dynamically forming a temporary network and communication between transmitter and receiver is by using bi-directional link. Either directly, if nodes in MANET are within communication range or indirectly means transmitter node rely on intermediate node, for forwarding data to destination node. Various feature of MANET, overcomes the problem in contemporary application of wireless network. such as dynamic topology and decentralized network feature of MANET, means all the nodes are free to move randomly. The self-configuring ability of nodes in MANET, Minimal configuration and quick development, makes MANET ready to be used in emergency condition, where an infrastructure is unavailable, or difficult to install network, in scenarios like natural disasters, military conflicts. Due to these various unique characteristics, MANET is becoming popular among all other wireless application as well as widely implemented in industry.

Network security has vital importance in every wireless network technology. But open medium and remote distribution of nodes make MANET vulnerable to various types of attacks. So it is necessary to develop an efficient secure intrusion-detection system (IDS) to protect MANET from various attacks. IDS is one of the Research field in MANET, mostly researchers are focusing on developing a new detection, prevention and response mechanisms for MANET.

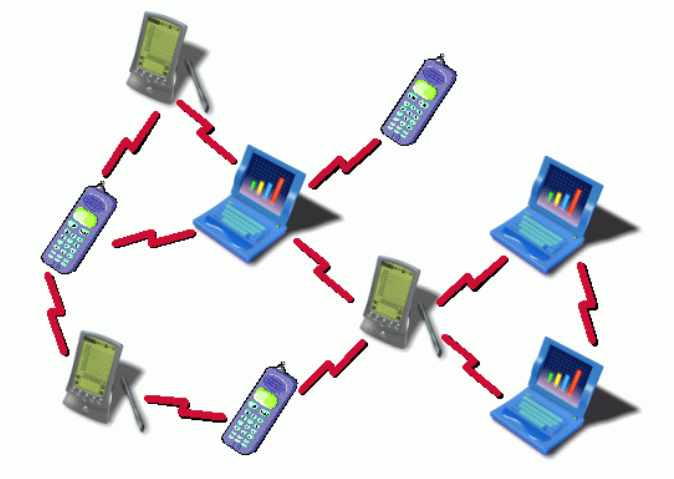

Fig 1. Wireless MANET

1.1 IDS in MANETs:

Intrusion is any set of actions that attempt to comprise the integrity, confidentiality or availability and an intrusion detection system (IDS) is a device or software application that monitors network traffic and if any suspicious activity found then it alerts the system or network administrator. There are three main modules of IDS are Monitoring, Analyses, Response. The Monitoring Module is responsible for controlling the collection of data. Analyses Module is responsible for deciding if the collected data indicated as an intrusion or not. Response Module is responsible for manage and using the response actions to the intrusion.

Due to the limitations of most MANET routing protocols, nodes in MANETs assume that other nodes always cooperate with each other to relay data. This assumption leaves the attackers with the opportunities to achieve significant impact on the network with just one or two compromised nodes. To overcome this problem, intrusion-detection system (IDS) should be added to enhance the security level of MANETs. If MANET knows how to the detect the attackers as soon as they enters in the network, we will able to completely remove the potential damages caused by compromised nodes at the first time. IDS usually acts as the second layers in MANETs. and it is a great complement to exiting proactive approaches. So intrusion detection system is very important aspect of defending the cyber infrastructure from attackers.

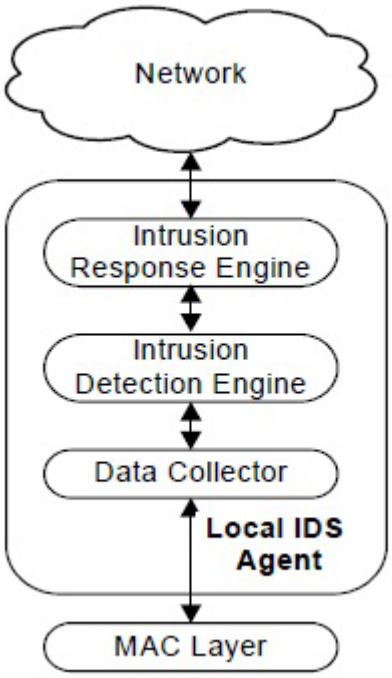

Fig 2.Intrusion detection system

II. RELATED WORK

2.1. Routing misbehavior in mobile Ad-hoc networks (MANET)

Most of the routing protocols in MANET have limitations in transmission. Therefore, nodes in MANET assume that other node always cooperate with each other, to reciprocation of packet this assumption, gives opportunities to attackers, to achieve significant impact on the network with compromising just one or two nodes in the network. To overcome this problem, an intrusion detection system should be introduced, to enhance security level of MANET

In this paper, Marti et al.[] proposed a mechanism called Watchdog. It's aim is to enhance the throughput of network with the presence of malicious nodes. In reality, the watchdog scheme consists of two different parts, namely Watchdog and pathrator.

2.1.1 Watchdog

Watchdog serves as IDS for MANET. It is responsible for detecting malicious node misbehaviors by prominently listing to it's next hop's broadcast. If Watchdog node overhears that, it's next node fails to forward the packet within pre-defined time, it increase it's failure counter. whenever a node's failure counter exceeds a pre-defined threshold, the watchdog node it's as misbehaving node.

2.1.2Pathrator:

Pathrater works as response system. Once Watchdog node identifies malicious node in the network, then the pathrater cooperator with the the routing protocols to avoid the reported node in the future transmission . Many research studies have proved that, watchdog scheme is efficient. Nevertheless, as pointed out by Marti et al[],watchdog scheme fails to detect malicious misbehaviors with presence of following: 1)ambiguous collisions; 2) receiver collisions; 3) limited transmissions; 4) false misbehavior report; 5)collusion; 6) partial dropping.

2.2 Acknowledgement Based Routing Misbehavior Detection in MANET:

To address six weakness of watchdog scheme, various new approaches proposed by many researches.

In this paper Liu et al.[] proposed a novel scheme called TWOACK. TWOACK is one of the most significant approaches among them. This TWOACK scheme is neither an enhancement nor Watchdog based scheme. It's aim is to overcome problems such as Receiver collision an limited transmission power in a watchdog.

TWOACK scheme is proposed to detect routing misbehavior and to reduce mitigate their adversr effect. This scheme scheme is used to detect some selfish nodes nodes, will participate in the route discovery and maintainence processes, but refuse to forward packet.

The TWOACK scheme detect misbehaving link by acknowledging every data packet transmitted over every three consecutive nodes long the path from the source to the destination. After getting packet, by the nodes in a 3-consecutive nodes, each node along the route is required to send back an acknowledgment packet to the node that is two hops aways from it down the route. Source sends the packets to the Receiver after receiving packet by receiver, it generates th 2ack packet back to sender. The retrieval of this 2ack packet within a predefined time period indicates successful transmission, otherwise both intermediates and destination node are reported as malicious.

The 2-ack scheme, successful solves the receiver collision and limited transmission power problems of watchdog scheme. But in 2-ack scheme, the acknowledgement process required in every packet transmission. Due to this acknowledement process, it addes a significant amount of network overhead.

2.3 Video Transmission Enhancement in presence of Misbehaving Nodes in MANETs.

In this paper, sheltami et al. [] proposed a new novel intrusion detection system, called Adaptive-Acknowledgement(AACK). AACK is an acknowledgement-based, scheme, which is considered as combination of TACK (identical to 2-ack) and end-to-end acknowledgement scheme (ACK). It detect misbehavior of malicious node, also avoid them in other transmission. AACK scheme, gives more network throughput and reduces network overhead, as compared to TWO-ACK.

In this AACK System, initially source node sends out packet1 without any overhead except 2b of flag indicating the packet type. Then all the intermediate nodes simply forward this packet. Finally, when the destination node 'D' receives packet 1, it is required to send back an Ack acknowledgement packet to the source node 's' along the reverse order of the same path. If source node receives this ACK acknowledgement packet, within predefined time period, then packet transmission from source to destination is successful. Otherwise, the source node will switch to

TACK scheme by sending out a TACK packet .Hybrid scheme in AACK, significantly reduces RO.

Both the TWO-ACK and AACK schemes are acknowledgment based scheme. For the detection of misbehavior, these two schemes completely depends upon acknowledgement packet from receiver. Misbehaving nodes, that exhibit abnormal behaviors can disrupt the network operation and sends forging acknowledgement packets to the sender. So, it is crucial to guarantee that acknowledgements packets are valid and authentic.

2.4 Detecting forged Acknowledgement in MANETs.

Nodes in MANETs assume that other nodes always cooperate with each other to relay data. This assumption leaves the attacker with the opportunities to drop the packet as well as to generate forge the acknowledgement packet, MANET suffers from the problem is it fails detect malicious node.

In this paper, N. Kang et al [ ] introduce an intrusion detection scheme with digit signature algorithm, to provide secure transmission against false misbehavior report and partial dropping. In MANET, it assumes that misbehaving nodes are lies between source and destination, that is they are intermediate node along with other intermediate node. During the transmission of packet, initially misbehaving node cooperate with other nodes, then they drop the packets instead of forwarding to next node, also they generate forge acknowledgement and send to the source node. When the source node sends out the data packet, it register packet-ID and sent time. After receving packet, destination node need to to send acknowlgement with packet-ID to source noe. Within a predefined time period, if source receives node Acknowledgement packet from destination, then transmission is successful. After getting Acknowledgement packet to source, no more additional ACK packet does not receive by source from destination, otherwise it switch to secure Acknowledgement mode.

In this secure-ACK scheme, the principle is to let every three consecutive node work in group, the third node required to send S-ACK packet to the the first node as well as third node is required to sign packet with it's own digital signature. When the first node receives this s-ack packet, it verifies the third node's signature with the pre-distributed public key. If source node does not receives this S_ACK packet, within predefined time, then both node second and third ar reported as malicious. When the source node receives th e malicious report, instead of trusting the report immediately and it marks the node as malicious, it requires the source node to switch to MRA mode to confirm this malicious report.

The source node switch, to MRA mode, by sending out an MRA packet, to destination node throught different route. If there is no other route exists in cache, source will find alternative route when there are no alternative route to destination node from source node. This detection system, in extreme condition accept this misbehaving report.

2.5 EAACK – A Secure intrusion-detection System for MANETs

As discussed in previous paper, both TWO-ACK and AACK solve two weakness of watchdog scheme, namely receiver collision and limited transmission power. But both of them, still suffer from problem that is to false misbehavior attack.

In this paper, Elhadi M. shakshuki et al [ ] proposed anew IDS called EAACK – Enhanced Adaptive Acknowledgement. It is specially designed for MANET, which solve not only receiver collision and limited transmission power but also the false misbehavior problem. EAACK scheme makes makes use of digital signature, to prevent the attacker from forging Acknowledgment packet. It requires all Acknowledgment packet to be digitally signed. EAACK consists of '3' major parts namely ACK, S-ACK,MRA.

In this first ACK mode, initially sender sends packet to destination, all intermediate node cooperate to forward the packet to destination. After receving packet by destination it is required to send back Acknowledgment packets to receive, it waits for the Ack packet. Within a predefined time interval, if the source node received a acknowledgement from receiver, then the packet transmission is succesful. Otherwise, source node node will switch to S-ACK mode, by sending out an S-ACK data packet.

In this S-ACK mode, the principle is to let every three consecutive node work in a group to detect misbehaving nodes. Every third node, in the group is required to send Acknowledgment to the first node. Within predefined time period, if any node fails to send acknowledgment is marked as malious node. Here, EAACK requires the source node to switch MRA mode and confirm this misbehaving report.

The third step of EAACK scheme, named Misbehavior report Authentications (MRA). In this MRA mode, the main function of MRA scheme, is to authenticate whether the destination node has received the reported missing packet through different packet route. Initially source node first searches it local knowledge base for the altenative path to destination. If there is no other route exist, then source node starts a DSR Routing request to find alternative route. Due to the nature of MANETs, it is possible to find out altenative route between any two node. After receiving an MRA packet by the destination, it searches it's local knowledge base and compares if the reported packet was received. If it is already received, then this is a false misbehavior report and the node which sends that packet marked as malicious. Otherwise, the misbehavior report is trusted and accepted.

This new system uses digital signature to authenticate ACK packet as well as it prevent ACK packet to be forged. In this scheme, sender must sign the packet before sending packet and after receving of the packet reciver will verify the authenticity of the packet . In the case of limited transmission power, receiver collision, false misbehavior rate an EAACK is a preferred intrusion detection system than exiting approaches.

III. CONCLUSION

Malicious attack has always been a major threat to the security in MANETs. In this paper, we have done literature survey for detecting the malicious nodes misbehaviors in Mobile Ad-hoc Network (MANET). Intrusion detection system (IDS) is one of the most active fields of research in MANET. This system usually focused on detecting problem with the routing system to prevent various attack. This paper shows the overview of various intrusion detection system to detect malicious nodes and provide security against the attacks. Packet dropping attack has always been a major threat to the security in MANET. A novel IDS named EAACK protocol specially designed for MANETs. In this system, first send data packet; if it detects any misbehavior in the network it will find misbehaving node and eliminate the node from the route. Otherwise it will select the alternate route from it's local acknowledge base and start sending packet. Compared EAACK scheme against all other popular mechanism in different scenarios through simulations. The results demonstrated positive performances against Watchdog, Two-Ack, AACK in the case of receiver collision, limited transmission power, false misbehavior report. And it reduce packet dropping.

REFERENCES

[1]. Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami, "EAACK- A Secure Intrusion Detection System for MANETs" IEEE trans. Vol.60, no.3, MAR, 2013.

[2]. S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. 6th Annu. Int. Conf. Mobile Comput. Netw., Boston, MA, 2000, pp. 255–265.

[3]. K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007.

[4]. Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in Proc. 4th IEEE Workshop Mobile Comput. Syst. Appl., 2002, pp. 3–13.

[5]. N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowledgements in MANETs," in Proc. IEEE 25th Int. Conf. AINA, Biopolis, Singapore, Mar. 22–25, 2011, pp. 488–494

[6] R. Akbani, T. Korkmaz, and G. V. S. Raju, "Mobile Ad hoc Network Security," in *Lecture Notes in Electrical Engineering*, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666.

[7] R. H. Akbani, S. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hoc networks: A survey," in *Proc. 2nd Int. Meeting ACCT*, Rohtak, Haryana, India, 2012, pp. 535–541.

[8] T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," in *Wireless/Mobile Security*. New York: Springer- Verlag, 2008.

[9] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence ofmisbehaving nodes inMANETs," *Int. J. Multimedia Syst.*, vol. 15, no. 5, pp. 273–282, Oct. 2009.

[10] A. Singh, M. Maheshwari, and N. Kumar, "Security and trust management in MANET," in *Communications in Computer and Information Science*, vol. 147. New York: Springer-Verlag, 2011, pt. 3, pp. 384–387.

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

[12] D. Johnson and D. Maltz, "Dynamic Source Routing in *ad hoc* wireless networks," in *Mobile Computing*. Norwell, MA: Kluwer, 1996, ch. 5, pp. 153–181.