ISSN:0975-9646

Survey on Intrusion Detection Mechanisms for MANETS

Shwetha M[1]
Student of MTech IV sem, CSE
East west Institute of Technology
Bangalore, India

Mamatha A[2]
Assistant professor, CSE
East west Institute of Technology
Bangalore, India

Abstract - **Security is a most important service in Mobile Adhoc Network from past few years. MANETs are more vulnerable to various kinds of security attacks and hence secure routing is very important. MANETs communicate in a dynamically built network that lacks centralized access and fixed infrastructure. Nodes in the network communicate directly with each other when they are within the same communication range. Otherwise, they rely on their neighbors to relay messages. The reputation of a node increases if it transfers the message properly and decreases otherwise. Because of this dynamically changing topologies, wireless medium and absence of centralized controlling points, security is of at most importance. But MANETs are more viable because of the minimum computation and communication overhead.**

Index terms — **Ad hoc networks, Authentication, Confidentiality, Mobile Adhoc Networks (MANETs), malicious nodes, Time-To-Live (TTL).**

I. Introduction

The widespread adoption of wireless technologies has caused the computer networks concept to be re-shaped. Wireless networks are mostly preferred due to their scalability, mobility, improved technology and reduced costs. The implementation of the wireless network takes place at the physical layer of the OSI Model using the radio communication for administering it.

Mobile Ad Hoc Networks (MANETs) is a collection of mobile nodes, which includes both a transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or by relying on other nodes as routers. The operation on these nodes does not depend on preexisting infrastructure or a base station [1].

Due to the mobility of the nodes in MANETs, the network topology keeps changing rapidly and unpredictably. All network activities have to be executed by the nodes themselves, either individually or collectively. However, this communication is limited to the range of transmitters, i.e, two nodes cannot communicate with each other when the distance between them is beyond the communication range of their own. MANET relay on intermediate nodes to overcum this problem to transmit the data. MANET is divided into two types of networks: single-hop and multihop to achieve this. All nodes within the same radio range communicate directly with each other to transmit the data in a single-hop network, where as in a multihop network, nodes rely on other intermediate nodes to transmit the data if the destination node is out of their radio range.

MANETs are capable of creating a self-configuring and self-maintaining network with a decentralized network infrastructure. MANET can be readily used in emergency circumstances where an infrastructure is unavailable or unfeasible to install, because of its minimal configuration and quick deployment nature. Depending on its application, the structure of a MANET may vary from a small, static network that is highly power-constrained to a large-scale, mobile, highly dynamic network [2].

Because of these unique characteristics, open medium and remote distribution, MANETs are vulnerable to various types of attacks. Routing protocols in MANETs assume that every node in the network behaves cooperatively with each other and presumably not malicious [3], thus attackers can easily compromise MANETs by inserting malicious or noncooperative nodes into the network. Because of this distributed architecture and changing topology of MANETs, a traditional centralized monitoring technique is no longer feasible, and it is crucial to develop an intrusion-detection system (IDS) specially designed for MANETs.

II. Related Work

As discussed before, the assumption that the nodes in MANETs always cooperate with each other to relay data, provides the attackers with the opportunities to achieve significant impact on the network with just one or two compromised nodes. Hence an IDS is needed to enhance the security level of MANETs. If the attackers are detected as soon as they enter the network, then the potential damages caused by compromised nodes can be completely eliminated. Else IDSs can be used at the second layer in MANETs to identify the attackers and the compromised nodes.

Anantvalee and Wu [4] presented a very thorough survey on contemporary IDSs in MANETs. In this section, we describe some of the existing approaches.

1) Intrusion Detection in MANETs: In traditional wired networks all the traffic must go through switches, routers, or gateways. Hence, IDS can be added to and implemented in these devices easily. Whereas, MANETs do not have such devices. Moreover, the medium is wide open, so both legitimate and malicious users can access it. Furthermore, there is no clear separation between normal and unusual activities in a mobile environment. Since nodes can move arbitrarily, false routing information could be from a compromised node or a node that has outdated information. Thus, the current IDS techniques on wired networks cannot be applied directly to MANETs. Many intrusion detection systems have been proposed to suit the characteristics of MANETs [4].

2) *Watchdog:* This scheme proposed by Marti *et al.* [5] aims to improve the throughput of network with the presence of malicious nodes. The Watchdog scheme is consisted of two parts: the Watchdog and the Pathrater. Watchdog serves as an IDS for MANETs and is responsible for detecting malicious node misbehaviors in the network. It detects malicious misbehaviors by promiscuously listening to its next hop's transmission. If a Watchdog node overhears that its next node fails to forward the packet within a certain period of time, it increases its failure counter. Whenever a node's failure counter exceeds a predefined threshold, the Watchdog node reports it as misbehaving. In this case, the Pathrater cooperates with the routing protocols to avoid the reported nodes in future transmission. Many following research studies and implementations have proved that the Watchdog scheme is efficient. Furthermore, compared to some other schemes, Watchdog is capable of detecting malicious nodes rather than links. These advantages have made the Watchdog scheme a popular choice in the field. Many MANET IDSs are either based on or developed as an improvement to the Watchdog scheme.

As said by Marti *et al.* [5], the Watchdog scheme fails to detect malicious misbehaviors with the presence of the following: 1) ambiguous collisions; 2) receiver collisions; 3) limited transmission power; 4) false misbehavior report; 5) collusion; and 6) partial dropping.

3) End-to-End Acknowledgment Schemes: There are several schemes that use end-to-end acknowledgments (ACKs), proposed by K. Liu *et al.*[1], to detect routing misbehavior or malicious nodes in wireless networks. These acknowledgments are sent by the end receiver to notify the sender about the reception of data packets up to some locations of the continuous data stream. In order to identify malicious routers that draw traffic toward themselves but fail to correctly forward the traffic, secure traceroute protocol was proposed which allows sender to simply send packets with increasing Time-To-Live (TTL) values and wait for a warning message from the router at which time the packet's TTL value expires. The secure traceroute protocol authenticates the traceroute packets and disguises them as regular data packets. To adaptively probe faulty links on the route being used, binary search is initiated on faulty routes. This technique only works with static misbehaviors and needs to disguise the probing messages as regular routing control packets. Once a link is identified as faulty, the link weight is increased so that future link selections will avoid this link.

4) The TWOACK and S-TWOACK Schemes: In [6], J. Deng *et al.* proposed an early version of the 2ACK scheme, termed TWOACK. The 2ACK and the TWOACK schemes have the following major differences: 1) The receiving node in the 2ACK scheme only sends 2ACK packets for a fraction of received data packets, while, in the TWOACK scheme, TWOACK packets are sent for every data packet received. Acknowledging a fraction of received data packets gives the 2ACK scheme better performance with respect to routing overhead. 2) The 2ACK scheme has an authentication mechanism to make sure that the 2ACK packets are genuine.

The Selective TWOACK (S-TWOACK) scheme proposed in [6] is different from 2ACK as well. Mainly, each TWOACK packet in the S-TWOACK scheme acknowledges the receipt of a number of data packets, but a 2ACK packet in the 2ACK scheme only acknowledges one data packet. With such a subtle change, the 2ACK scheme has easier control over the trade-off between the performance of the network and the cost as compared to the S-TWOACK scheme.

5) Adaptive Acknowledgement (AACK): Based on TWOACK, Sheltami et al. [7] proposed a new scheme that is called AACK. Similar to TWOACK, AACK is an acknowledgment-based network layer scheme which can be measured as a combination of a scheme called TACK (identical to TWOACK) and an end-to-end acknowledgment scheme called ACKnowledge (ACK). Compared to TWOACK, AACK considerably reduces network overhead while still capable of maintaining or even surpassing the same network throughput during data transmission. The end-to-end acknowledgment scheme in ACK is shown in Fig. 1. In the ACK scheme the sender node sends out Packet 1 without any overhead except 2 b of flag indicating the packet type. In this network all the intermediate nodes simply forward this packet to the next nodes. When the destination node i.e the receiver receives Packet 1, it is vital to send back an ACK acknowledgment packet to the sender node down the reverse order of the same route. Within a predefined time, if the sender node receives this ACK acknowledgment packet from the destination node, then the packet transmission from sender to receiver is successful. Or else, the sender will switch to TACK scheme by sending out a TACK packet. The concept of adopting a hybrid scheme in AACK greatly reduces the network overhead, but both TWOACK and AACK still suffer from the problem that they fail to detect malicious nodes with the presence of false misbehavior report and forged acknowledgment packets.

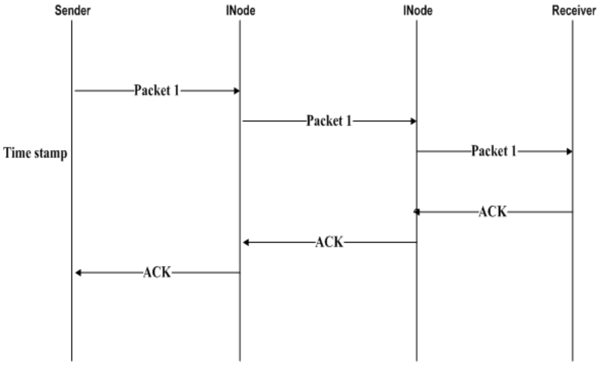

Fig. 1 AACK scheme: The reciever node is required to send acknowledgment packets to the source node.

6) IIDS: It is important to guarantee that the data packets are valid and authenticated. To ensure this integrity of IDS, Anusha.K *et al.* [8], proposed IIDS, which requires data packets to be encrypted before they are sent out and verified until they are accepted. Improved IDS (IIDS) is mainly proposed to address the problem of extra resources required due to the introduction of security in MANETs. IIDS uses AODV routing protocol to find the shortest path in the network to reach destination. Then it encrypts the data packet with hash key and send to the destination. The destination decrypts the data and check the hash value for data integrity. If the route has attacker nodes and if the sender does not receive acknowledgement packets then the packets will be sent in the new route. If any node wants to send packet to neighboring node then first source node generate the packet and send to the neighboring node. The sent packet is sent to acknowledge system in which we AACK with security. After that it send packet according to mode and detect the intruder in the system, If intruder or misbehaving node is detected then alert will be triggered by the same node that detect the misbehaving node. When a node detect malicious node it will inform the source node by sending an acknowledgement, which is a small packet that is generated by the routing protocol and extract the route from source route of corresponding data packet and the packet will be sent in a new route.

III. CONCLUSION

Mobile Ad Hoc Networks (MANETs) have been an area for active research over the past few years due to their potentially widespread applications. Security is a major threat in MANETs by the attackers from the malicious nodes, a best IDS is needed to detect a malicious node in the network and avoid it. This paper surveys some of the existing mechanisms of intrusion detection which helps in understanding them better. And is beneficial for the researchers who are into the development of novel IDS for MANETs to provide better security among the mobile nodes.

ACKNOWLEDGMENT

We express our gratitude to all those who gave their valuable guidance and times to help us understand. Also we thank Department of Computer science and Engineering, East West Institute of Technology, Bangalore for giving us permission to continue my research on this topic.

REFERENCES

[1] 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.

[2] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami, “EAACK—A Secure Intrusion-Detection System for MANETs,” *IEEE Trans. Industrial Electronics*, vol. 60, no. 3,pp 1089- 1098, March 2013.

[3] L. Buttyan and J. P. Hubaux, *Security and Cooperation in Wireless Networks*. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.

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

[5] 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.

[6] 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.

[7] 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.

[8] Anusha.K, Rajyalakshmi G.V, “*Secure Adaptive Acknowledgment Algorithm for Intrusion Detection System“,* Int. J. Emerging Research in Management &Technology ,Vol 2, Issue-7,July 2013.