A Review Paper on Intrusion Detection System in MANETs

Farhin Shaikh[1], Chandresh Parekh[2]
[1]M.Tech, Raksha Shakti University, Ahmedabad, Gujarat, India
[2]Assistant Professor, Raksha Shakti University, Ahmedabad, Gujarat, India

ABSTRACT

The MANETs is one type of Ad Hoc network that is used for mobile communication. The Mobile Ad Hoc NETworks (MANETS) are used when the user is moving. Because MANET does not depend on fixed infrastructure. In MANETs Wireless networks are used to connect with different networks. surrounded by all the contemporary wireless networks, Mobile Ad hoc NETwork (MANET) is one of the most important and unique applications. The self-configuring ability of nodes in MANET absolutes it admired among essential mission applications like military use or emergency recovery. The mobility and scalability carried by wireless network ended it possible in many applications. Surrounded by all the contemporary wireless net- works Mobile Ad hoc NETwork (MANET) is one of the most significant and exclusive applications. In this review paper a qualified learns of Secure Intrusion- Detection Systems for determining malicious nodes and attacks on MANETs are presented. One of the main advantages of wireless networks is its capability to permit data communication between different parties and still maintain their mobility.

Keywords: Mobile Ad Hoc NETworks, Attacks on MANETs, Intrusion Detection System

I. INTRODUCTION

Mobile Ad hoc NETwork (MANET) is a collection of mobile nodes assembled with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly. MANET does not need a fixed infrastructure; thus, all nodes are free to move randomly. MANET is able to creating a self-configuring and self-maintaining network without the help of a centralized infrastructure. MANET is becoming more and more extensively implemented in the industry.

One of the major advantages of wireless networks is its capability to allow data communication between different parties and still manage their mobility. However, this communication is limited to the area of transmitters. This means that two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication area of their own. In contradictory to the traditional wireless network, MANET has a decentralized network infrastructure. MANET does not need a fixed infrastructure; thus, all nodes are free to move randomly. MANET is able to creating a self-configuring and self-maintaining network without the help of a centralized infrastructure, which is often inaccessible in critical mission applications like military conflict or emergency recovery. MANET ready to be used in emergency circumstances where an infrastructure is unavailable or impossible to install in scenarios like natural or human-induced disasters, military conflicts, and medical emergency conditions [3].

MANETs have many applications in various fields. For example, they have been used in a military context since the 1970s to ensure the timely flow of information and command in battle, contributing to the success of a mission. MANETs are also ideal for stabilizing communication networks and providing rescue services following natural disasters such as earthquakes or floods [6].

II. Background

Attacks in MANETs

CSEIT1172692 | Received : 20 Nov 2017 | Accepted : 12 Dec 2017 | November-December-2017 [(2)6: 715-719]

Many types of attacks can be performed over a MANET.

Classification of Attacks in MANETs

MANETs can be divided into two main categories, namely passive attacks and active attacks. The passive attacks typically involve only eaves dropping of data, whereas the active attacks involve actions performed by adversaries such as replication, modification and deletion of exchanged data.

1) **Passive Attacks:** MANETs are more vulnerable to passive attacks. A passive attack is a network attack in which a system is observed and sometimes scanned for open ports and vulnerabilities. passive attacks include the unauthorized "listening" to the network traffic or accumulates data from it. Passive attacks are floated to steal valuable information in the targeted networks. Examples of passive attacks in ad hoc network are eavesdropping attacks and traffic analysis attacks. Detecting this kind of attack is crucial because neither the system resources nor the critical network functions are physically damaged to prove the intrusions [8].

Eavesdropping

An incursion where someone tries to steal information that computers, smartphones, or other devices transmit over a network. An eavesdropping attack takes advantage of unsecured network communications in order to gain the data being sent and received.

Location Disclosure Attack

In this attack, the privacy requirements of a node are compromised. Through the use of traffic analysis technique or with simpler probing and monitoring approaches an attacker is capable to discover a location of the node, and the structure of the network [9].

Traffic Analysis

In MANETs the data packets as well as traffic pattern both are important for attackers. For example, confidential information about network topology can be derived by analysing traffic patterns. Traffic analysis can also be conducted as active attack by destroying nodes, which stimulates self-organization in the network, and valuable data about the topology can be gathered.

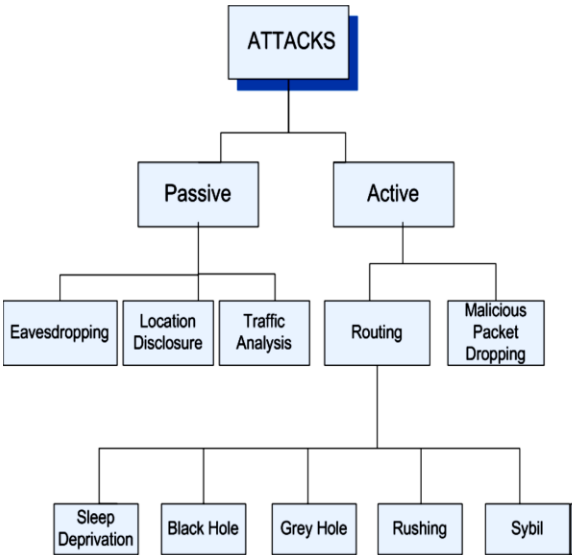

Figure1. Classification of Attacks

2) **Active Attacks:** Active attacks are very severe attacks on the network that stop message flow between the nodes. These attacks make unauthorized access to network that helps the attacker to make changes such as modification of packets, modification and deletion of exchanged data, message replays, message fabrications and the denial of service attacks, replication [8].

Blackhole Attack

Blackhole attack is the solemn problematic for the MANET, in which a malicious node sends false routing info, stating that it offers the shortest path for the destination node whose packets it wants to interrupt and then constraint them without promoting to the destination.

Grey hole Attack

Grey hole attack is the type of active attack that leads to the dropping of the data packets. The malicious node firstly permits to transmit the packets and then fails to do so [7]. Grey hole attacks make the intruder node to broadcast the similar action as a genuine node during discovery of route, which leads to dropping of packets from particular nodes. It is a major concern since it is tough to identify this attack [10].

Sinkhole Attack

The sinkhole attack is the severe attack in the mobile ad-hoc network. In the sinkhole attack, the main aim is that the malicious node or compromised node attract close by all the traffic from its intermediary nodes by telling that it has the shortest part for the destination node. Once received all the traffic from the intermediary nodes it makes changes in the secret info, like modification in the packets or drop the data packets [7].

Sleep deprivation attacks

This kind of attack is actually more specific to the mobile ad hoc networks. The aim is to drain off limited resources in the mobile ad hoc nodes (e.g. the battery powers), by constantly makes them busy processing unnecessary packets. In a routing protocol, sleep deprivation attacks might be launched by flooding the targeted node with unnecessary routing packets. For instance, attackers could flood any node in the networks by sending a huge number of route request (RREQ), route replies (RREP) or route error (RERR) packets to the targeted node. As a result, that particular node is unable to participate in the routing mechanisms and rendered unreachable by the other nodes in the networks [8].

Rushing Attack

It uses forged suppression during the route discovery process are prone to this attack. An attacker which could transmit further route request rapidly than genuine nodes can enlarge the chance that the routes include the attacker will be found instead of authentic route, rushing attack prevention provides the defensive process against the attack.

Sybil Attack

Each node in a mobile ad hoc network seeks a significant address to participate in routing, and nodes are identified through address in the network. There is no central authority to verify these identities in MANETs. An attacker can exploit this property and send control packet, for example RREQ or RREP, using different identities this is known as a Sybil attack [10].

Malicious Packet Dropping

In this type of attack packets are discarded without any reason. This Packet dropping at a malicious intermediate node can lead to interruption of communication or generation of wrong information between the source and destination which is an undesirable situation.

3) **External attacks:** External attacks are attacks launched by enemies who are not initially authorized to participate in the network operations. These attacks usually desire to cause network congestion, denying access to specific network function or to disrupt the whole network operations. Bogus packets injection, denial of service, and impersonation are some of the attacks that are usually instituted by the external attackers.

4) **Internal attacks:** Internal attacks are instituted by the authorized nodes in the networks, and might come from both compromised and misbehaving nodes. Internal nodes are determined as compromised nodes if the external attackers hijacked the authorized internal nodes and are then using them to launch attacks against the ad hoc networks. Security requirements such as authentication, confidentiality and integrity are severely vulnerable in the ad hoc networks with the compromised internal nodes because communication keys used by these nodes might be stolen and passed to the other colluding attackers [8].

III. IDS IN MANETS

Because of the limitations of most MANET routing protocols, nodes in MANETs assume that other nodes always cooperate with each other to relay data. This conclusion leaves the attackers with the opportunities to achieve significant impact on the network with just one or two compromised nodes. To overcome this problem, an IDS should be added to enhance the security level of MANETs. IDSs usually act as the second layer in MANETs, and they are a great companion to existing proactive approaches.

In this section, we mainly describe three existing approaches, namely, Watchdog, TWOACK, and Adaptive Acknowledgment (AACK).

1) Watchdog:

Watchdog is capable to detecting malicious nodes rather than links. These advantages have made the Watchdog scheme accepted choice in the field. the Watchdog scheme is contained in two parts, namely, Watchdog and Path rater. Watchdog produced as IDS for MANETs. It is liable for detecting malicious node in the network. Watchdog detects malicious misbehaviors by promiscuously listening to its next hop's transportation. If a Watchdog node listen that its next node fails to forward the packet within a certain period of time, it increases its failure counter. The Watchdog scheme fails to detect malicious misbehaviors with the incidence of the ambiguous collisions, receiver collisions, limited transmission power, false misbehavior report collusion and partial dropping.

2) TWOACK:

TWOACK is neither an improvement nor a Watchdog-based scheme. To overcome the receiver collision and limited transmission power problems acknowledging every data packet transmitted over every three successive nodes along the path from the source to the destination. Upon retrieval of a packet, each node along the route is necessary to send back an acknowledgment packet to the node that is two hops away from it down the route. TWOACK is recommended to work on routing protocols such as Dynamic Source Routing (DSR) [5].

The TWOACK scheme successfully deal with the receiver collision and limited transmission power problems posed by Watchdog. However, the acknowledgment process recommended in every packet transmission process added a significant amount of unwanted network overhead. Because of the limited battery power nature of MANETs, such redundant transmission process can easily degrade the life span of the entire network [3].

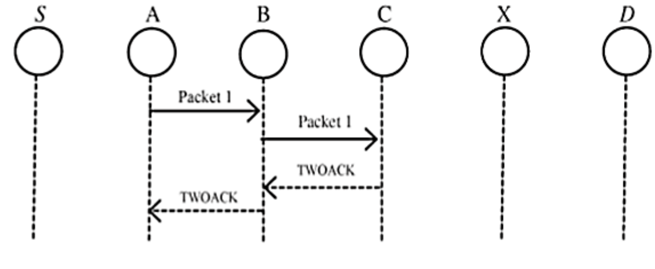

Figure2.

TWOACK scheme: Each node is required to send back an acknowledgment packet to the node that is two hops away from it.

3) AACK:

Similar to TWOACK, AACK is an acknowledgment-based network layer scheme which can be treated as a combination of a scheme called TACK(TWOACK) and an end-to-end acknowledgment scheme called ACKnowledge (ACK). Compared to TWOACK, AACK significantly decreased network overhead while still capable of maintaining or even surpassing the same network throughput. The end-to-end acknowledgment scheme in ACK is shown in Fig. 2. The concept of adopting a hybrid scheme in AACK significantly reduces the network overhead, but both TWOACK and AACK still go through the problem that they fail to detect malicious nodes with the presence of false misbehavior report and forged acknowledgment packets.

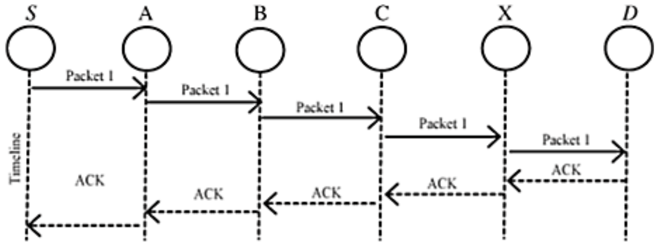

Figure3.

ACK scheme: The destination node is required to send acknowledgment packets to the source node.

In fact, many of the existing IDSs in MANETs adopt an acknowledgment-based scheme, including TWOACK and AACK. The functions of such detection schemes all largely depend on the acknowledgment packets. Hence, it is crucial to guarantee that the acknowledgment packets are valid and authentic [3].

IV. CONCLUSION

MANETs have been an area of active research over the past few years due to their potentially widespread application in military and civilian communication. However, MANETs are extremely vulnerable to attacks due to their dynamically changing topology, absence of conventional security, open medium of communication. Mobile Ad-hoc Network is facing many problems related to the security. In this review paper, one can see that there are several attack characteristics that must be considered in designing any security measure for the ad hoc network. In a future work, several security solutions that have been proposed to secure mobile ad hoc network will be investigated and classified based on this classification. The investigation will include various techniques that might be employed in protecting, detecting, and responding to the attacks against MANETs.

V. ACKNOWLEDGMENT

I would first like to thank prof. Chandresh D. Parekh for his mentorship and guidance on my experiment. I would like to extend a special thanks to My family members for their affection, care and encouragement. Above all I am thankful to almighty God for everything.

VI. REFERENCES

[1]. D. Mudzingwa and R. Agrawal, “A study of methodologies used in intrusion detection and prevention systems (IDPS)," IEEE, pp. 1-6, March 2012.

[2]. 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.

[3]. Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang, and Tarek R. Sheltami, Member, IEEE “EAACK—A Secure Intrusion-Detection System for MANETs”, IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 60, NO. 3, MARCH 2013.

[4]. B. Sindhu1 M.E, Karpagam University, “A Survey on Intrusion Detection in Mobile Ad Hoc Networks Using Enhanced Adaptive Acknowledgment”, International Journal of Innovative Research in Computer and Communication Engineering, Vol.2, Special Issue 1, March 2014.

[5]. S.Rajeswari, Dr. A.Ramamurthy, K.T.V Subbarao, “An Efficient Intrusion-Detection Mechanisms To Protect Manet From Attacks” , International Journal of Science Engineering and Advance Technology, IJSEAT, Vol 2, Issue 12, December – 2014.

[6]. Adnan Nadeem, Member, IEEE and Michael P. Howarth, “A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks”, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, ACCEPTED FOR PUBLICATION.

[7]. Ram Kishore Singh, Parma Nand, “Literature Review of Routing Attacks in MANET”, international Conference on Computing, Communication and Automation (ICCCA2016).

[8]. Dr Sanjeev Yadav, Rachna Jain, Mohd Faisal, “Attacks in MANET”, International Journal of Latest Trends in Engineering and Technology (IJLTET), ISSN: 2278-621X, Vol. 1 Issue 3 September 2012.

[9]. P. Narendra Reddy, CH. Vishnuvardhan, V. Ramesh, “ROUTING ATTACKS IN MOBILE AD HOC NETWORKS”, IJCSMC, Vol. 2, Issue. 5, May 2013, pg.360 – 367.

[10]. I. Meenatchi , K. Palanivel, “Intrusion Detection System in MANETS: A Survey”, International Journal of Recent Development in Engineering and Technology, ISSN 2347 – 6435, Volume 3, Issue 4, October 2014. José Helano Matos Nogueira The International Journal of FORENSIC COMPUTER SCIENCE IJoFCS (2006) 1, 28-32.