International Journal of Advanced Technology in Engineering and Science
Vol. No.4, Issue No. 10, October 2016
www.ijates.com
ijates
ISSN 2348 - 7550

A REVIEW OF IDS TECHNIQUE TO DETECT ATTACK OVER MOBILE ADHOC NETWORK

Sachin Khasdev[1], Prof. (Dr.) Mohit Gangwar[2], Dr. Varsha Namdeo[3]

[1]Resarch Scholar Department of Computer Science, BERI Bhopal, [2]Principal,
[3]Department of Computer Science, BERI Bhopal

ABSTRACT

The wireless Network is an emerging technology in the field of communication. The communication may take place between computers; networking devices etc. the most popular technique is the sensor network. This technology has many advantages but have the loophole called wormhole attack. There are various types of attack can possible in the network. This paper is a brief discussion on Mobile Adhoc network. This paper also throws some light on the various types of attacks like wormhole and its classification.

Keywords: WSN, Attacks, Wormhole, Ids, Mobile ad hoc Networks.

I. INTRODUCTION

The wireless Mobile Adhoc network is an approach to perform the communication using sensor nodes. These sensor nodes are self configured. This type of network is use to control and monitor the environment. A wireless Mobile Adhoc network is a network of cheap and simple processing devices (sensor nodes) that are equipped with environmental sensors for temperature, humidity, etc.

The wormhole attack is dangerous against the security in WSNs in which the nodes that hear a packet transmission directly from some node consider themselves to be in range of (and thus a neighbor of) that node. It is one of the most the powerful attack that are faced by many ad hoc network routing protocols. Since The wormhole attack does not require exploiting the feature of nodes in the network and it can interfere while executing the routing process. Attacker uses these attacks to gain unauthorized access to compromise systems or perform denial-of-service (DoS) attacks. In wormhole, the attacker at one end records the incoming traffic and tunnels packets to the other end. If routing control messages like RREQ are tunneled, this will result in distorted routing tables in the network. If there exist fast transmission path between the two ends of the wormhole that may tunnel the data at higher speed than the normal mode of wireless multi-hop communication. Thus, they will attract more traffic from their neighbors. This will results in rushing attack. In Rushing attack, due to the presence of fast transmission path all the packet will start following that path and this will increase the Average Attack Success Rate. Wormhole attack can also act as the first stage attackers where they can lead to the denial-of-service attacks. In the second stage, this may compromise the security of the global network as that breaks confidentiality and integrity. The wormhole attack is very harmful to the security of network. Due to the placement of the wormhole in the network there will be significant breakdown in communication across a wireless network. A successful wormhole attack may be the reason of disruption and breakdown of a network. Proper balance between these two is necessary to prevent much consumption of resources.

II. WIRELESS MOBILE ADHOC NETWORK

A wireless infrastructure less network having static or dynamic topology is called the Mobile Adhoc network. The basic entity used here is called the sensor. This type of network meets Combine different types of nodes and gateways. Due to the mobility of the nodes in the network supports the dynamic feature. The Mobile Adhoc network can temporal establish instantly. The figure shown below is an example of the Mobile Adhoc network. In this scenario there is a source and destination node is available for communication.

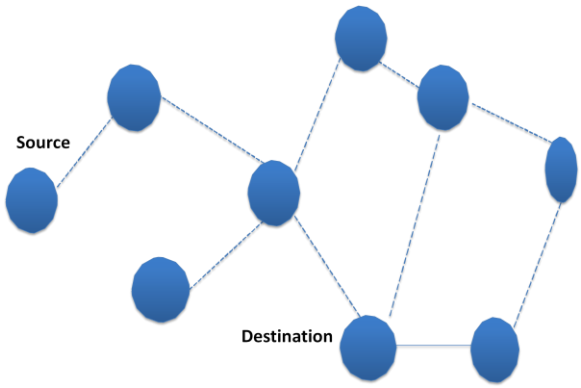

Figure 1 Mobile Adhoc network

2.1 Vulnerabilities OO MANET

- **Wireless Connection:** the wireless links are very helpful to connect the user with the network. The flexibility of this feature is helps the attacker to join the network.
- **Dynamic Topology:** this is a biggest advantage of WSN that nodes can leave and join the network freely. But this approach increased the complexity.
- **Cooperativeness:** Most of the routing approaches believe that the nodes which the moving in the network are not the malicious node. Even these node are cooperative.
- **Bandwidth:** here the bandwidth is limited due to large number of other activities in compare of wired network.

2.2 Applications of WSN

The WSN is very popular because of its properties. It has lots of applications. Some of them are discussed below.

- Collaborative Work
- Disaster Management
- Military and intelligence
- Preserving Historical places
- Personal Area Network (PAN)
- Taxi or Cab Network
- Conference or Meeting room

III. ATTACKS

There are various attacks can possible in the Mobile Adhoc network. But there are two major classifications in this way. Active and Passive attacks are the most common category. In active attack the attacker or the malicious node takes the part actively in the network. Here the attacker will modify or alter the data packet and send this packer into the network. In spite of altering the data packet attacker can also inject and drop the data packet. So that, such type of attacks very harmful for the end users.

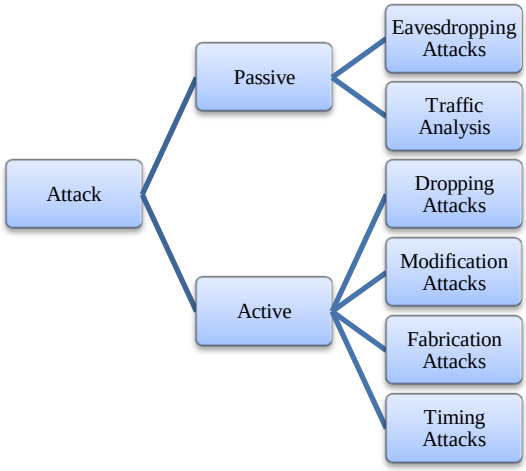

Figure 2 Classifications of Attacks

On other hand the passive attack can happen without the tempering the data packet. In this type of attack the attacker only analyze the data. The main goal of this type of attack is to break the confidentiality. Here the attacker tries to know the activities of the network. It focuses on the pattern to send in the network on the basis of which the attacker will take illegal action. Detection of passive attacks is very difficult since the operation of the network itself does not get affected.

The figure 2 shows the basic classification of the attacking approaches. As it shows the active and passive attack are the first criteria. It is possible to classify this by some other criteria.

3.1 Types of Attacks on Protocol Stack

The characteristics of MANET make them susceptible to many new attacks. These attacks can occur in different layers of the network protocol stack.

Layer	Attacks
Application Layer	Viruses and Worms
Transport Layer	TCP,UDP
Network Layer	Blackhole, Wormhole
Data Link Layer	Traffic Monitoring,
Physical Layer	EavesDropping

3.2 Security Goals in WSN

There are four major constrain on which

Figure 3 Security Goals in WSN

Availability: the service should be in the access of user at any time.

Authentication: it provides the surety that the sender is an authorized person.

Integrity: During Message transmission the message should not be change or modify.

Non-Repudiation: should not need to resend the message in the network

3.3 Attacks on Network Layear

A process in the network for trying to damage or defeat the things using illegal activity in the wireless environment called attack. The person or an object who will do this thing is called the attacker. There are many types of attacks in network layer like

- Black hole Attack
- Rushing Attack
- Wormhole Attack
- Sinkhole Attack
- Link Withholding & Link Spoofing Attacks
- Replay Attacks
- Resource Consumption Attack
- Sybil Attack

In all these attacks the wormhole is a famous and dangers attack. Wormhole attack is a severe attack in which two attackers placed themselves strategically in the network. The attackers then keep on hearing the network, record the wireless data.

IV. RELATED WORK

The author has proposed [8] solution for digital investigation of wormhole attacks in Wireless Mobile Adhoc network. The author gives the name observer to those nodes which are the set of investigator nodes. These nodes are responsible for monitoring the network. Observers gather the information of datagram of the network. They generate and securely forward evidences containing information regarding the monitored datagram, the routing paths they followed, and the identity of the nodes whose behavior is suspicious. The simulation results give the batter results regarding investigation. The authors have presented [9] state-of-the-art research for in order to address the serious problem of wormhole in wireless Mobile Adhoc networks and discuss the relative

strengths and shortcomings of the proposed solutions. The author has concluded by highlighting how such a system can be used for defending against wormhole attackers.

The author [10] has introduces first the concept of wormhole attack and five kinds of this attack and clusters in this work. The author explained the methods used for the IDS sensor network. These approaches are unknown efforts nodes to detect the malicious node. The method has been designed in order to identify the malicious nodes in neighbor nodes where nodes can be pair in the area within its own radio range. On other hand the another technique is implemented in order to get the malicious nodes in the neabure node, in which each pair of nodes may not be in radio range of each other but where there is a node among them which has all the other nodes in its one-hop vicinity. Both techniques use message passing between the nodes. The author has completed these approaches to detect the wormhole attack and isolating them from routing process.

As far as Wireless sensor network [11] is a rising technology which provides the various solution of application areas such as health care, military and industry. Here the sensor devices are used. These sensors which are limited are distributed over the environment and communicate through the wireless media. As sensor devices are limited the network exposed to variety of attacks. Conventional security mechanisms are not suitable for MANET as they are usually heavy and nodes are limited. One of the most severe attacks to detect and defend in wireless sensor network is wormhole attack which data will be forwarded from one part of the network to the other part trough the wormhole tunnel. The author has focused on wormhole attack and proposed distributed network discovery approach to mitigate its effect. The simulation shows that the can mitigated almost 100% of wormhole attack overload in the environment where 54% of nodes are affected with the wormhole.

Security is one of the major concerns in Sensor network[12]. There are many unsolved problems in ad hoc networks. The wormhole attack is one of them. Among all sorts of attack the most threatening and dangerous attacks is wormhole on wireless networks. During the attack a malicious node captures packets from one location in the network, and tunnels them to another distant malicious node, which replays them locally. In this paper, we propose a scheme for the wormhole attack prevention. The scheme relies on the idea that usually the wormhole nodes participate in the routing in a repeated way as they attract most of the traffic. Therefore, each node will be assigned a cost depending in its participation in routing. Besides preventing the network from the wormhole attack, the scheme provides a load balance among nodes to avoid exhausting nodes that are always cooperative in routing.

The author explained that the Wormhole [13] is a kind of attack in Wireless Sensor Network (WSN) that needs not to crack encryption key, which has great harm. Aiming at characteristics of Wormhole attack, the paper presented a kind of wormhole attack defense strategy of WSN based on neighbor nodes verification. Under this strategy, when each normal node received control packet, it will monitor the packet to determine whether it comes from its normal neighbor nodes to avoid Wormhole attack effectively. The simulation has done on OMNeT++ shows that the AODV added neighbor nodes verification successfully implement effective defense.

A wormhole attack [14] is a challenging attack in these days. The wormhole has various security issues in mobile wireless sensor networks. The author has proposed the Statistical Wormhole Apprehension by the Neighbors nodes, called the new approach for getting wormhole in sensor network. . As SWAN utilizes the localized statistical neighborhood information collected by mobile nodes, it apprehends wormholes not only without requiring any Special hardware device but also without causing significant communication and coordination overhead. We performed extensive studies on false positive and detection rates via both analyses

and simulations. The simulation results show that SWAN can detect wormhole attacks with high probabilities and very low false positive rates.

V. CONCLUSION

Securing the Mobile Adhoc network is becoming increasingly important in present scenario. The wireless network is area where there is needs to enhance the security. This paper has analyzed the attacks that WSN can be subjected to. This paper has discussed various types of attack which can happen in WSN. it also shows the protocol which has used in Mobile Adhoc network. The worm hole is a major disadvantage of the WSN. There is a need to overcome this problem. this paper also throws some light on the classification of wormhole and previous work which has been done in this era.

REFERENCES

[1]. Zunnun Narmawala, Sanjay Srivastava, "Survey of Applications of Network Coding in Wired and Wireless Networks" in Proceedings of the 14th National Conference on Communications, pp. 153-157, February 2008.

[2]. Sheikh, R. , Singh Chande, M. and Mishra, D.K., "Security issues in WSN: A review", IEEE 2010, pp 1-4.

[3]. Kannhavong, B., Nakayama, H., Nemoto, Y. and Kato, N., " A survey of routing attacks in mobile ad hoc networks" IEEE 2007, pp 85-91.

[4]. Verma, M.K. and Joshi, S. ; Doohan, N.V. "A survey on: An analysis of secure routing of volatile nodes in WSN", IEEE 2012, pp 1-3.

[5]. P. Papadimitratos and Z. J. Haas, "Secure Routing For Mobile Ad Hoc Networks" in Proc. of CNDS, 2002.

[6]. K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding- Royer, "A Secure Routing Protocol For Ad Hoc Networks" in Proc. of IEEE ICNP, 2002.

[7]. C. E. Perkins, and E. M. Royer, "Ad-hoc on-demand distance vector routing," IEEE 1999, pp 25-26.

[8]. Bayrem Triki, Slim Rekhis and Noureddine Boudriga, "Digital Investigation of Wormhole Attacks in Wireless Sensor Networks", IEEE 2010, pp 179-186.

[9]. Thanassis Giannetsos, Tassos Dimitriou and Neeli R. Prasad, "State of the Art on Defenses against Wormhole Attacks in Wireless Sensor Networks", IEEE 2009, pp 313-318.

[10]. Mahdi Nouri, Somayeh Abazari Aghdam and Sajjad Abazari Aghdam, "Collaborative Techniques for Detecting Wormhole Attack in WSNs", IEEE 2011, pp 1-6.

[11]. Ali Modirkhazeni, Saeedeh Aghamahmoodi, Arsalan Modirkhazeni and Naghmeh Niknejad, "Distributed Approach to Mitigate Wormhole Attack in Wireless Sensor Networks", IEEE 2011, pp 122-128.

[12]. Mariannne. A. Azer, "Wormhole Attacks Mitigation in Ad Hoc Networks", IEEE 2011, pp 561-568.

[13]. Jin Guo, Zhi-yong Lei, "A Kind of Wormhole Attack Defense Strategy of WSN Based on Neighbor Nodes Verification", IEEE 2011, pp 564-568.

[14]. Sejun Song Haijie Wu and Baek-Young Choi, "Statistical wormhole detection for mobile sensor networks", IEEE 2012, pp 322 – 327.