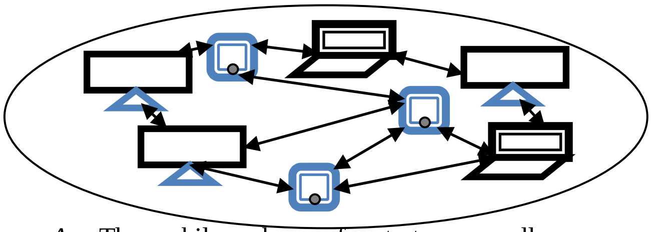
Security attacks in MANET: A Survey

Gagandeep Singh[1], Arshdeep Singh[2]
[1]*Pursuing M.Tech, Computer Science and Engineering*
[2]*Assistant Professor, Bhai Gurdas Institute of Engineering and Technology, Sangrur*

Abstract-The MANET that is Mobile Ad-hoc Network are forming a group of many nodes they can interact with each other in limited area. All the malicious nodes present in the MANET always disturb the usual performance of routing and that cause the degradation of dynamic performance of the network. The intermediate nodes work is very responsible in Routing procedure with continue movement. During the work we have recommended one security scheme against the attack of packet dropping by the malicious node in the network. The scheme which is recommended here will work to find attackers by using the concept of detection to link to forward the data or information between sender and receiver. The packet dropping on link through node is detected and prevented by IDS security system. The network performance measures in the presence of attack and secure IDS with the help of performance metrics PDR throughput etc.

I. INTRODUCTION

A mobile ad hoc network (MANET) is a collection of mobile nodes which establish a network spontaneously and communicate over a shared wireless channel without any infrastructure. In MANET [1], collection of mobile nodes may dynamically vary the topological structure. The nodes are inconstantly connected with each other and formed an arbitrary topology.



- *A.* The mobile nodes are free to turn casually.
- *B.* Each node can act as both router and host.
- *C.* There is no existence of fixed infrastructure.
- *D.* Quickly installation with least possible user intervention.

II. MANETCHALLENGES

Mobile nodes have the ability to sense, compute and communicate like static nodes. The dynamic nature of MANET leads to their benefits, but also creates technical challenges due to some factors as given:

- *A.* Potentially frequent network partitions.
- *B.* Security mechanisms.
- *C.* Routing.
- *D.* Restricted wireless transmission range.
- *E.* Resource availability.
- *F.* Mobility-induced route changes.
- *G.* Internet access mechanisms.
- *H.* Self-configuring networks requires an address allocation mechanism.
- *I.* Resource availability.
- *J.* No predefined boundary.

III. SECURITY ATTACKS IN MANET

Security attacks and detection schemes in MANET. Attacks can be classified as

- *A.* Passive Attacks.
- *B.* Active Attacks.

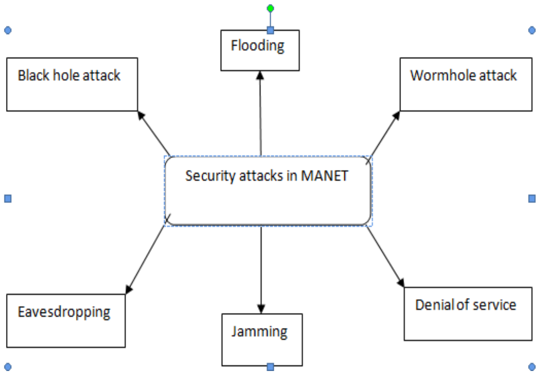


Fig. 2 Security attack in Manet

1) *Eavesdropping*-An eavesdropping attack, which are also known as a sniffing or snooping attack, is an incursion where someone tries to steal information that computer, smart phones or other devices transmit over a network. A passive type of attack in which the malicious nodes sniff within the traffic of network is known as eavesdropping.

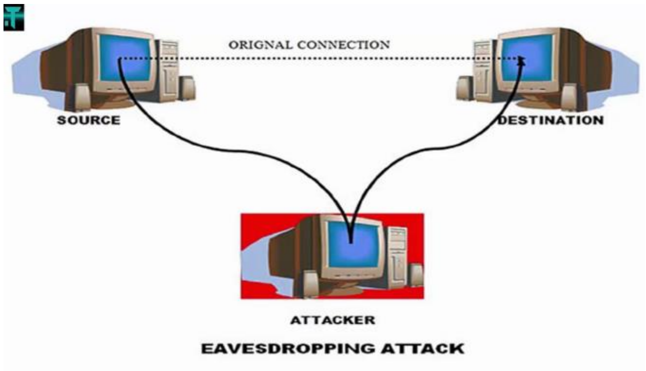
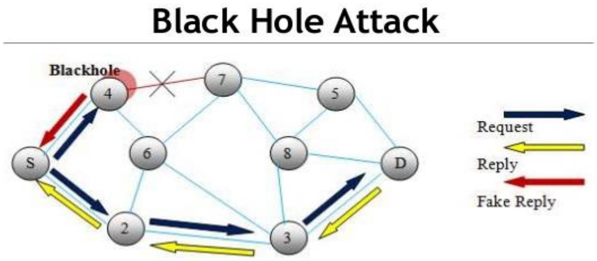


Fig.3 Eavesdropping attack

2) *Black hole Attack*- In this type of attack a malicious node send a path reply packet to the source node in reply packet to the source node in reply of path request for root discovery. The malicious nodes present within the network are responsible for triggering this type of active attack. The selection of path from source to destination is to be done by the reactive routing protocols.



3) *Wormhole attack*- An attack that can be caused within or outside the network by the malicious node is known as a wormhole attack. Wormhole attack is a critical attack in which the attacker records the packets bits at one location in the network and tunnels those to another location. Either the retransmitting or tunneling of the bits could be done selectively. The path which is used for information passing is usually not part of the actual network this make it difficult to detect the wormhole attack.

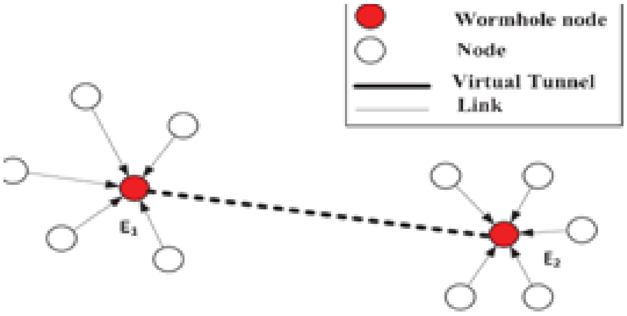


Fig.4 Wormhole attack

4) *Jamming Attack*- It is an active type of attack. In jamming attack number of packets is sent to specific node by the malicious node. The node is not able to handle a large number of packets. Due to which there will be blocking in the network. This attack is also taken place in network by other way. In this the attacker will find out the frequency at which destination node is receiving the signal from sender. There are different channels to deliver the signal.

5) *Denial-of-Service Attack*- Attack to disrupt the authorized use of networks, systems, or applications. The required services cannot be accessed by the legitimate nodes in the denial-of-service attack. The elimination of the allowed access to resources or the delaying of time on the critical operations. The network performance measurement parameters such as throughput and bandwidth get depleted which degrade the overall performance of the network. Dos attack, is an explicit attempt which have to made a computer resource that is unavailable by either injecting a computer virus or flooding the network with useless traffic signals. When a denial of service attack occurs, a computer or a network user is unable to access resources like e-mail and the internet. An attack that may be directed at an operating system or at the network.

6) *Flooding attack*- It is a type of active attack. The bandwidth, consumption of node resources network resources are exhausted by attacker. The flooding attack is an attack that attempts to cause a failure in a computer system or other data processing entity by providing more input entry can process properly. The attack attempts to exhaust a server's resources by sending a large amount of legitimate requests.

IV. SELECTIVE PACKET DROP ATTACK

Selective Packet drop attack is the type of denial of service attack. Packet dropping attack is launched in the forward phase. So it is very complex and difficult to isolate. This attack is very easy to perform but very difficult to detect it. A Selfish node also drops packet in their different ways. They drop some packets for save their resources not to damage any other nodes. In these types of attacks, malicious nodes act as normal nodes every time but selectively drop sensitive packets.

A. Performed if jamming is not successful.

B. Packet header is inspected-forwarded or dropped.

C. If attacker interrupts- gets access to drop packets randomly.

D. Less Flexible approach.

E. Why – Based on routes through which packets are transmitted.

F. Selective Packet drop is only possible when a jamming attack is unsuccessful.

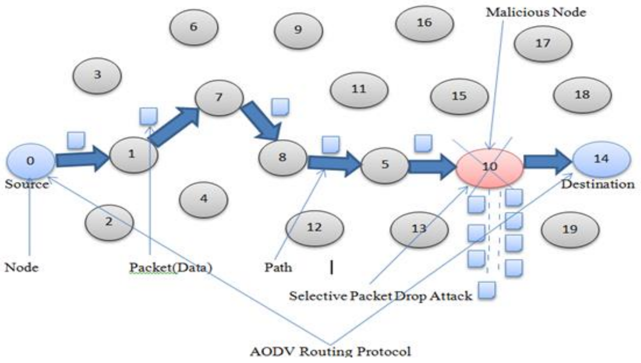


Fig.5 Selective packet drop attack

V. LITERATURE SURVEY

Rohit Chourasia, et.al, (2017), have proposed that the packet dropping on link, through node is detected and prevented by IDS security system. The scheme not only works to identify the nodes performing malicious activity however, prevent them also. The identification of attacker noticed by dropping of data packets in excessive quantity. The prevention of it can be done via choosing the alternate root somewhere the attacker performing malicious activity not available among the senders to receivers.

Sourabh Singh Verma, et.al, (2015), have analyzed that MANET can be affected by various kinds of attacks. In this number of mobile nodes is present that are decentralized and needs cooperation to transfer traffic. In this network number of nodes are present and any nodes can be malicious that can participate or lead to denial of service (DOS) attacks. The network QOS parameters get affected by these attacks one of them is flooding attack. In this paper different flooding nodes in network have been given by authors by considering different interval of times. The hello flooding consists of two request and data flood attacks that are classified by flooding. The authors have considered request flooding under multi facets conditions and parameters.

Swagata Singha, et.al (2014), in paper proposed the plan that has work in two phases. In the first phase a secure algorithm based on cryptography is used which checked the authenticity of a new arrived node in the network. This phase authorized to some of the network related jobs in spite of granting full authorization. In the second phase maliciousness of newly joined node is checked. For this purpose entire data set divided into some smaller parts. After execution of above phase node is able to construct an entire data getting lowest number of those data parts if it is non-malicious.

Raquel Lacuesta, et.al (2013), identified the problem related to protocol which manages creation and organization of spontaneous and dynamic wireless ad hoc network. In this paper a framework is proposed which helps nodes to reasonable by the use of their IP addresses. This framework deploys secure protocol and IP address assignment mechanism.

VI. PROPOSED WORK

Following are the various objectives of this research work:

1. To study and analyze various intrusion detection systems for mobile Ad-hoc network.
2. To Apply various different types of attacks i.e Black hole Attack, Eavesdropping etc.
3. To propose technique for isolation of selective forwarding attack that is based on mutual authentication technique.

VII. CONCLUSION

In this work, it has been concluded that mobile Ad-hoc network is decentralized type of network due to which malicious nodes enter the network and leave whenever they want. Due to decentralized nature of the network, many malicious nodes enter which are responsible to trigger various active and passive attacks. This research is based on detecting malicious nodes from the network which are responsible to trigger flooding attack. The proposed technique will be based on authentication technique in the network. To drop the packets is the only intention of packet dropping attackers'. During this work reliable and novel IDS (Intrusion Detection System recognized the activity performed by attacker nodes. The data dropping activity decreases the MANET performance. The packet dropping is reduced and enhance receiving of data packets.

REFERENCES

[1]. Rohit Chourasia and Rajesh kumar Boghey," Novel IDS security against Attacker routing misbehaviour of packet dropping in MANET". IEEEvol.6, pp.1-5, 2017.

[2]. Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester, "An Overview of Mobile Ad-hoc Networks: Applications and Challenges", IJSER, vol. 3, pp. 132-138,2005.

[3]. Y. Khamayesh, R.Salah and M.B. Yassein. "Malicious Nodes Detection in MANETs: Behavioral Analysis Approach", Journal of Networks, Vol.7, No.1, January 2012.

[4]. Raquel Lacuesta, Jaime Lloret, Miguel Garcia, and Lourdes, "A Secure Protocol for Spontaneous Wireless Ad Hoc Networks Creation", IEEE Transactions on Parallel And Distributed Systems, Vol. 24, No. 4, April2013.[10]

[5]. Swagata Singha, Abhijit Das, "Detection and Elimination of the Topological Threats in Mobile Ad Hoc Network: A New Approach", IEEE International Conference on

Advances in Computer Engineering and Applications (ICACEA), 2015.

[6]. Mahsa Seyyedtaj, Mohammad Ali Jabraeil Jamali, “Different Types of Attacks and Detection Techniques in Mobile Ad-hoc Network”, International Journal of Computer Applications Technology and Research vol.3, pp. 541 – 546, 2014.

[7]. Priyanka Goyal, Sahil Batra, Ajit Singh, “A Literature Review of Security Attack in Mobile Ad-hoc Networks”, International Journal of Computer Applications, vol.9, pp.11-15, 2010.

[8]. C.M. Nalayini, Dr. Jeevaa Katiravan, Arvind Prasad. V, “Flooding Attack on MANET – A Survey”, Special Issue Published in International Journal of Trend in Research and Development (IJTRD), vol. 5, pp. 20-28, 2017

[9]. Meenakshi Patel, Sanjay Sharma, Divya Sharan, “Detection and Prevention of Flooding Attack Using SVM”, 2013 International Conference on Communication Systems and Network Technologies, vol. 12, pp. 533-537, 2013.