International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No. (01), January 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

SURVEY OF NETWORK LAYER ATTACKS IN MOBILE AD HOC NETWORK

M.Bobby[1] ,S.Sharmila[2]

[1]Assistant professor,Department of computer science,
Sri Adi Chunchanagiri Women's College,(India)
[2]M.Phil Scholar,Department of computer Science,
Sri Adi Chunchanagiri Women's College,(India)

ABSTRACT

There are vast improvement in wireless technology over the past few decades.As wireless usage is greatly increasing it has both its pros and cons besides.Mobile adhoc network also known as wireless adhoc network or ad hoc wireless network is considerably infrastructure less network of mobile devices connected wirelessly. Each device in a MANET is free to move independently in any direction. Each must forward traffic through router. Different protocols are then evaluated based on measures such as pocket drop rate,end to end packet delays,ability to scale etc.The challenges are no fixed access point,dynamic snetwork topology,contrary environment and irregular connectivity and no centralized authority.Taking this challenges as advantage there are various attacks to degrade the performance of network.This paper focuses on various type of malicious attacks with their effect on the Mobile ad hoc network networks.

Keywords:Mobile Adhoc Network,Malicious nodes,wormhole attack,blackhole attack,greyhole attack.

I.INTRODUCTION

As the importance of computer increases it also build up the connectivity demand. Wired solutions are used from a very long time, but the demands for wireless solution are increasing for connecting to the Internet, exchanging information, send and receive E-mail messages etc. Mobile Ad-hoc network (MANET) becomes one of the most capable fields for research. MANET is a wireless adhoc network. A MANET can be connected to internet or external network and can be a standalone network. MANET is a Latin word which means "for this," or "for this purpose only". A MANET is a group of self-governing wireless mobile nodes which can interchange data in dynamic manner. Due to the mobile behavior of nodes the network structure is dynamic. The network is self-deploying and decentralized. The nodes in MANET act as both router and as a host and network topology changes rapidly and decision taken in a distributed manner. Due to dynamic behavior of network, routing for MANET is a daring task and wireless link become highly error prone in MANET. Security, reliability, availability, scalability, quality of service is some of the requirements of MANET.

As the demand for wireless networking greatly increasing it leads to growth of technique called ad hoc network.Adhoc networking has application in various fields[2] such as at the time of natural disasters or example during flooding,fire accident etc,in military sector it is very much useful in communicating information between soldiers,information headquarters,vehicle The other possible applications include personal area and

home networking, location-based services, and sensor networks. civilian environments like taxicab, sports stadium, boat and small aircraft, mobile ad hoc communications will have many application.

II. LITERATURE REVIEW

D.Helen and D.Arivazhagan[1] focused greatly on the applications,advantages and challenges of MANET.L.Raja and S.Santhosh [2] reviewed the various types of attacks and their challenges.G.S.Mamatha and Dr.S.C.Sharma[3] focused only on network layer attacks and also proposed the defence mechanism for such attack..Pooja Jaiswal and Dr.Rakesh Kumar[4] simulated the methods to prevent black hole attack in MANET.P.Narendra Reddi et al[5] concentrated on routing attacks by exposing all routing protocols and found out how routing process are being affected by various attacks. Ashish kumar Pandey and Anurag Srivastava[6] focused on evolution,challenges and uses of MANET.Pooja chachal et al[7] performed the compararive ananlysis of various attacks in MANET and also suggested the preventive techniques for those attacks.

III. ATTACKS IN MANET

Securing the mobile adhoc network is one of the challenging work and finding the attacks on the network is one of the important aspect regarding securing the network. Mobile adhoc network is vulnureble to many types of attacks as it has various possibilities such as dynamically changing its topology may be one of the important reasons.many malicious nodes are being for their chance for attacking the nodes attacking may be in many form such as denies of service or interrupt the data or drop the data or make the data to flow apart from efficiency path etc.

Consider for example node A wants to send data to B,M is a malicious node interrupt between node A and B and corrupt the data that pass through between node A and B.

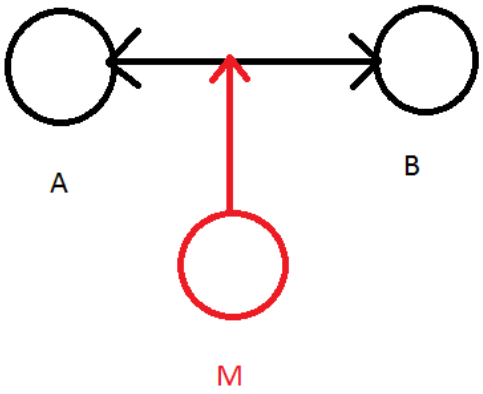

Figure 1:Attack of Malicious node

In Fig.1 malicious node M will disguise as a destination and steal all the data from the source node. There are basically 2 categories of attacks namely active and passive attack. Passive attack is introduced to just snoop the data it will never disturb the operation of the network such attacks are difficult to understand but active attacks will corrupt the data being exchanged and disturb the normal function of the network. In this paper we are focusing only on the network layer attacks such as black hole attacks, worm hole, grey hole attack.

3.1 Black hole attack*:*

In routing mechanism of ad hoc networks three layers namely physical, MAC and network layers plays a major role. As MANETs are more vulnerable to various attacks, all these three layers suffer from such attacks and cause routing disorders. The variety of attacks in the network layer differs such as not forwarding the packets or adding and modifying some parameters of routing messages; such as sequence number and hop count. The most basic attack executed by the nodes in the network layer is that an adversary can stop forwarding the data packets. The consequence caused by this is that, whenever the adversary is selected as an intermediate node in the selected route, it denies the communication to take place. Most of the times the black hole attack is launched by the adversaries, whenever AODV(Ad hoc On Demand Distance vector Routing)protocol is used as the data forwarding protocol. Consider a malicious node which keeps waiting for its neighbors to initiate a RREQ packet. As the node receives the RREQ packet, it will immediately send a false RREP packet with a modified higher sequence number. So, that the source node assumes that node is having the fresh route towards the destination. The source node ignores the RREP packet received from other nodes and begins to send the data packets over malicious node. A malicious node takes all the routes towards itself. It does not allow forwarding any packet anywhere. This attack is called a black hole as it swallows all the data packets.

3.2 Worm hole attacks:

Warm hole attack is a one of the Deniel of service attack that can affect the network following OLSR(Optimized Link State Routing)protocol without the knowledge of cryptographic techniques implemented. In worm hole attack 2 or more attackers are connected by high speed off channel link called warm hole.In this type of attack,attackers form the tunnel to transfer the data packets.This method is very tricky as the packet near the attacker node will take several hop to reach the node near the attacker on the other side of the tunnel but here when the attacker receive the packet it traverse very fast to reach the attacker on the other side of the tunnel.This traverse is very faster than the normal reach of the destination.

3.3 Grey hole attack:

In grey hole attack the malicious node is hard to detect.In this attack the malicious node is much disguised to be a normal node,It silently gathers the packets information by routing the correct route path by sending route reply as route exists through the malicious node.when the source node sends the data by receiving the route reply

source node starts to send the data.In this method malicious node attack the network by capturing the data and destination node will never get the data it needs.

TABLE 1:Summary of Attacks with Number of nodes and affected protoclos

Attacks	Number of malicious nodes	Affected protocols
Black hole attack	One	AODV
Worm hole attack	Two	OLSR
Grey hole attack	One	AODV

IV.CONCLUSION

There is a great demand for wireless networks at current situation of technology due to various application in all fields.Inspite of its advantages, wireless network are easily prone to attacks because of its various weak factors. Thus attacks are unavoidable in wireless network. As MANET also one of the wireless network there is various attacks as we discussed focused to attack MANET. More innovative ideas and concepts is being in progress to mitigate those attacks.

REFERENCES

[1].D.Helen and D.Arivazhagan,"Applications,Advantages and Challenges in MANET"*Journal of Academia and Industrial Research(JAIR)Volume 2, issue 8,January 2014.*

[2].L.Raja and Capt S.Santhosh Baboo,"An overview of MANET:Application,Attacks and Challenges",*International journal of computer science and Mobile computation.IJCSMC Vol3,issue 1,January 2014.*

[3].G.S.Mamtha and Dr.S.C.Sharma,"Network layer attacks and Defence mechanism inMANET",*International journal of computer application(0975-8887)volume 9,November 2010.*

[4].Poojajaiswal and Dr.Rakesh kumar,"Prevention of Black hole attack in MANET",*IRACST-International Journal of computer Network and Wireless Communication ISSN:2550-3501 vol2,October 2012.*

[5].P.Narendra Reddy,"Routing attacks in MANET",*International journal of computer science and Mobile Computing(IJCSMC) vol 2,May 2013.*

[6].Ashish kumar Pandey and Anurag Srivastava"Review on MANET:Evolution,challenges and uses" *International journal of Technical research and Application e-ISSN:2320-8163 vol 1,Jul-Aug 2013.*

[7].Pooja chachal et al,"Comparative analysis of various attacks on MANET"
International journal of computer application(0975-8887),vol 111-no12,Febraury 2015.