ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 6, June 2014

A Novel Technique to Protect and Isolate Selective Packet Drop Attack in MANET

Anita[1], Abhilasha[2]

[1]Student MTech(CSE) , GZS PTU Campus, Bathinda, Punjab, India[1]

[2]Head of Deptt. CSE, GZS PTU Campus, Bathinda, Punjab, India[2]

Abstract: Wireless Networking is a technology in which two or more computers are communicating with each other. It can have a fixed infrastructure or it may not comprise of any infrastructure. MANET is one of the types of wireless networking which is a self configuring network in which a node can join or leave the system at any time. The nodes can form any topology as per the requirement for the given situation. Various routing protocols are used in MANET that can be reactive like AODV or proactive like DSDV or hybrid protocols like ZRP. There are many types of attacks which are possible to be triggered in MANET. In this paper we will focus on selective packet drop of selective forwarding attack. This packet reduces the throughput of the system. A novel technique will be proposed which will reduce packet drop problem. Experimental result shows that the proposed technique gives better results as compared to existing technique.

Keywords: MANET, security and selective packet drop

I. INTRODUCTION

To exchange information, a number of computer are joined together to form networks and share resources. Networking is used to distribute information and data communication. Sharing resources can be software type or hardware types. Wireless Networking is a technology in which two or more computers referred to as nodes communicate with each other using standard network protocols and without using the cables. There are two types of wireless networking. First is the infrastructure mode in which a wireless network adaptor is used to connect with the already existing networks with the help of access points. Wireless adaptor is also known as wireless client. It has a central controller. Second is the infrastructure less network, in which the communication takes place only between the wireless nodes and the access points. The communication does not directly take place between the wireless nodes. Here the access point is used to control the medium access as well as it acts as the bridge to the wireless and wired networks. Ad-hoc networks are a new standard of wireless communication for mobile hosts. Basically it is a type of network which is used in real time systems. No fixed infrastructure in ad hoc network like base station is required. Nodes within each other's radio range communicate directly via wireless links while the ones which are far apart rely on other nodes to relay messages. MANET stands for Mobile Ad hoc Network. It is a robust infrastructure less wireless network. It can be formed either by mobile nodes or by both fixed and mobile nodes. Nodes are randomly connected with each other forming an arbitrary topology. They can act as both routers and hosts. They have the ability to self-configure which makes this technology suitable for provisioning communication to, for example, disaster-hit areas where there is no communication infrastructure or in emergency search and rescue operations where a network connection is urgently required. There are two types of attacks present in MANET which can break the security of networks. These attacks are as follows:

A. Passive Attacks:

A passive attack obtains data exchanged in the network without disturbing the communications operation. The passive attacks are therefore difficult to detect. In this, operations are not affected. The operations supposed to be accomplished are ignored by a malicious node it attempts to recover valuable data by watching data travel through the channel. Examples of Passive Attacks are eavesdropping, snooping.

B. Active Attacks:

An active attack is that attack in which any data or information is inserted into the network so that information and operation may be harmed. It involves modification, fabrication and disruption of information and affects the operation of the network. Example of active attacks is impersonation, spoofing etc.

Other types of attacks are as follow:

C. *Internal Attack:*

Internal attacks are comprised of nodes that are part of the current path. In an internal attack, the malicious node gains

unauthorized access and behaves as a genuine node. Traffic can be analyzed between other nodes and may participate in the activities of other networks like blackhole, wormhole, selective packet drop attack etc.

D. External Attack:

The external attack is conceded out by the nodes which do not belong to network. It may cause unavailibity and congestion by sending false information for the network jamming attack.

II. LITERATURE REVIEW

S. Sharmila and G. Umamaheswari discussed about the defensive mechanisms based on cumulative acknowledgement and energy based scheme is proposed to detect selective forward attack in mobile wireless sensor networks. The scheme is evaluated in terms of packet delivery ratio and throughput. The malicious node is detected based on the acknowledgement and energy level of the node [5]. The energy consumption of the detection scheme is less when compared with existing detection schemes. From the simulations, byte overhead is 0.39 percentages and detection accuracy of 80% are observed and thus the throughput increases. These results show that the packets can be forwarded without any selective packet drop by minimizing the malicious nodes in the network. The further enhancement of the proposed scheme is to improve the success rate to 100% with mobility and receiver sensitivity of the node. N.Bhalaji introduced [6] that Ad-hoc networks are frequently targeted by participating malicious nodes to damage the network. A common mechanism to guard these networks is through the use of encryption and hashing mechanisms. However, the implementations of these mechanisms generally impose certain unessential requirements, which are considered as restrictive for unplanned environments. In this paper we have discussed the dynamic trust based approach through which association between nodes are used to resist selective packet drop attacks connected to adhoc networks. With the help of the Network simulator we were able to prove that the proposed scheme increases the routing security and encourages the nodes to cooperate in the adhoc structure. Our scheme is equipped with technique to identify and isolate the malicious nodes from the active data forwarding and routing. Aikaterini Mitrokotsa et.al discussed [7] that evolution of wireless network technologies and the recent advances in mobile computing hardware have made possible the introduction of various applications in mobile ad hoc networks. Not only is the infrastructure of these networks inherently vulnerable but they have increased requirements regarding their security as well. As intrusion prevention mechanisms, such as encryption and authentication, are not enough regarding security, we need a second line of defense Intrusion Detection. The focus of this paper is on anomaly detection techniques in order to exploit their main advantage of being able to detect unknown attacks. First, we briefly describe intrusion detection systems and then we suggest a distributed schema applicable to mobile ad hoc networks. This anomaly detection mechanism is based on a neural network and is evaluated for packet dropping attacks using features selected from the MAC layer. The performance of the proposed architecture is evaluated under different traffic conditions and mobility patterns. Jacek Cicho et.al discussed the problem of efficient alarm protocol for ad-hoc radio networks consisting of devices that try to gain access for diffusion through a shared radio communication channel [8]. The problem arises in tasks where sensors have to quickly inform the target user about an alert situation such as presence of dangerous radiation, fire, seismic vibrations, and more. In this paper, we show a protocol which uses O (log n) time slots and show that (log n= log n) is a lower bound for used time slots.

III. SELECTIVE PACKET DROP ATTACK

Selective Packet drop is only possible when jamming attack is unsuccessful. Once the packet is expected by the compromised node, it can examine the packet headers, categorize the packet, and decide whether to forward it or not. This action is known as misbehavior. Post-reception dropping is a little flexible than selective jamming because the challenger is limited to dropping only the packets routed through it. Selective policy known as the Jellyfish attack which is a compromised node that occasionally drops a small part of consecutive packets and can be constantly reducing the throughput of a TCP flow to near zero. This attack can be achieved even by reminding random delays to TCP packets, without dropping them, while left over protocol compliant. Similar selective dropping attacks can be constructed for other network functions such as the association/de-association of STAs, and topology management [5].

IV. PROPOSED TECHNIQUE

Among all the attacks discussed in the previous section, selective packet drop attack is the most common active type of attacks. Selective Packet Drop attack is the partial denial of service attacks which is triggered by the malicious nodes in the network. In the last few years, many techniques have

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 6, June 2014

been proposed to isolate selective attacks from the network. When Selective packet attack is triggered in the network, throughput of the network is reduced and delay increases at a steady rate. In our work, we intend to detect and isolate Selective Packet Drop attack in AODV Protocol. The aim of the study is to detect the Selective Packet Drop in MANET using AODV protocol. We aim to analyze the effects of Selective Packet drop attack in the light of Packet loss, throughput and end-to-end delay in MANET. A new scheme is proposed to detect malicious nodes in the network which are responsible for triggering the Selective packet Drop attack in the network. Simulation of the detection of Selective packet Drop attack is done using AODV protocol in MANET using NS-2 tool. In the present work a Diffie-Hellman technique is applied to detect malicious node in the network. First of all a secure channel will be established with the help of Diffie-Hellman technique. After the establishment of the channel, communication begins. In the Diffie-Hellman technique, two systems participating in the information called the master and the slave first select their random numbers 'p' which is a prime number and 'g' which is another generator number and their private numbers 'a' and 'b' respectively. From this, M and S are computed by the using the following formula

$M=g^a \bmod p$

$S= g^b \bmod p$

These numbers are exchanged to calculate another secret key K which is done as follows in both the systems:

$K= S^a \bmod p$

$K=M^b \bmod p$

These both keys are then compared and if the K value comes out to be equal that prove the validity of the algorithm. And hence this algorithm lets the communication begin only when the secure channel is established between the sender and the receiver.

The flowchart shown in figure 1 explains the proposed technique and also describes how the embedded Diffie-Hellman works in the network.

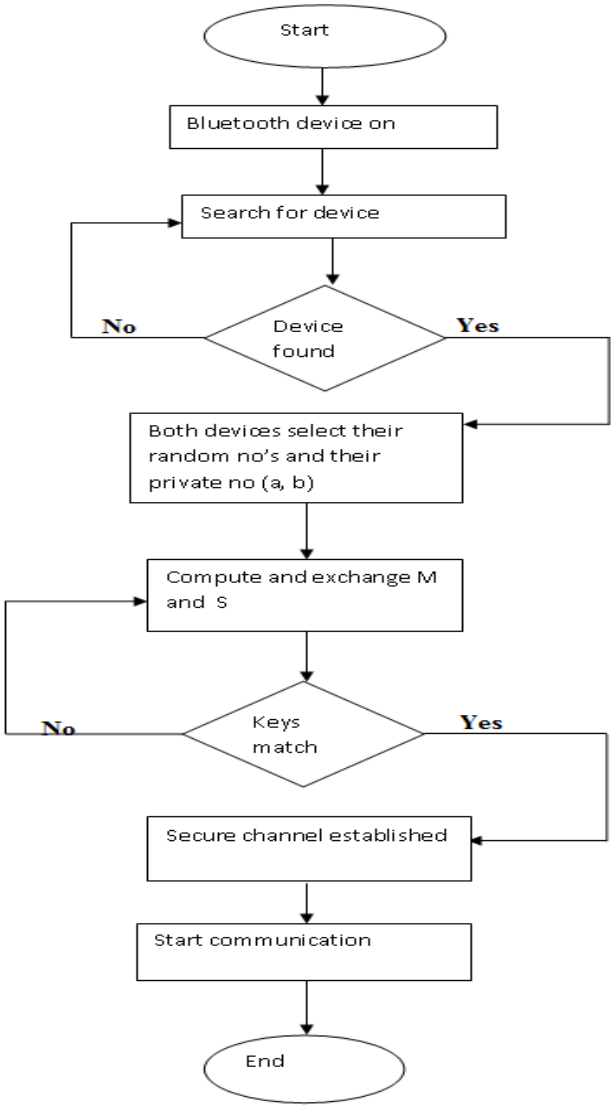

Figure 1: Flow chart for detection and isolation of selective packet drop.

V. RESULTS AND DISCUSSIONS

The Diffie Hellman algorithm has been used in MANET for isolating the selective packet drop attack that optimises various factors like Delay, Packet loss and throughput in the existing system. The results of the applied technique are hereby explained with the tables and their corresponding graphs.

The simulation has been carried out in NS-2 tool and the parameters of the same are discussed here:

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 6, June 2014

Table 1: NS-2 simulation parameters used for the validation of the mechanism

Parameters	Settings
Dimension	800*800 meters
Number of nodes	24
Topology	Flat grid
Simulation time	9 seconds
Base routing Protocol	AODV
Packet size	1000 Bytes
Packet generation rate	0.5 seconds
Network standard	802.11
Channel sensing	CSMA/CA

Table 2: Comparison of Delay with and without new technique.

Time(seconds)	Old Technique delay(seconds)	New Technique delay(seconds)
2.0000	0	0
4.0000	110	10
6.0000	275	10

The delay to transmit data from source to destination data is calculated in old and new technique with respect to time. The network delay is more in the previous scenarios. The network delay is reduced in the new scenario.

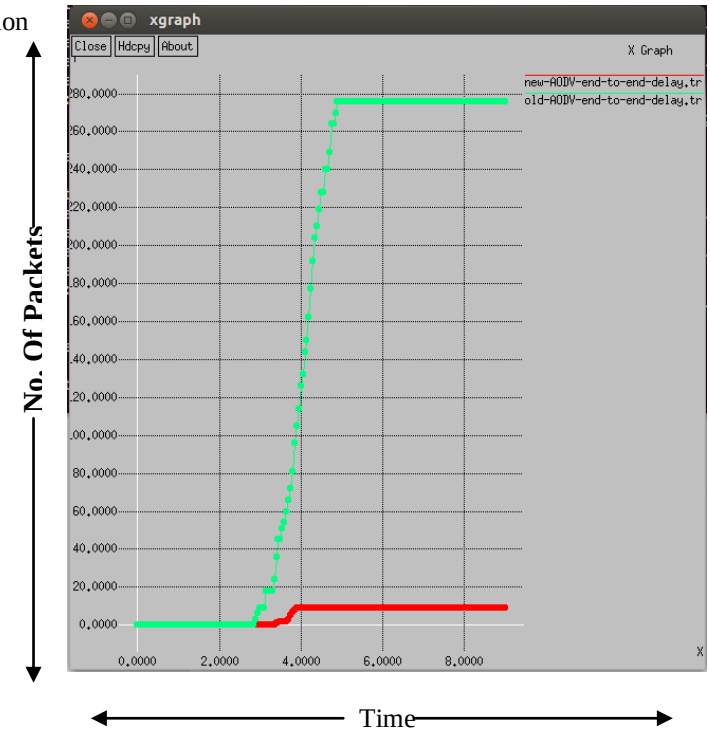

Figure 2: Graph for comparison of end to end delay

Table 3: Comparison of Packet Loss with and without old Technique

Time(seconds)	Without Technique	With Technique
2.0000	0	0
3.0000	0	0
4.0000	10	18
5.0000	30	18
6.0000	30	18

As we have applied the Diffie Hellman algorithm for setting up the path then the packet loss is less as compared to the previous scenario.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 6, June 2014

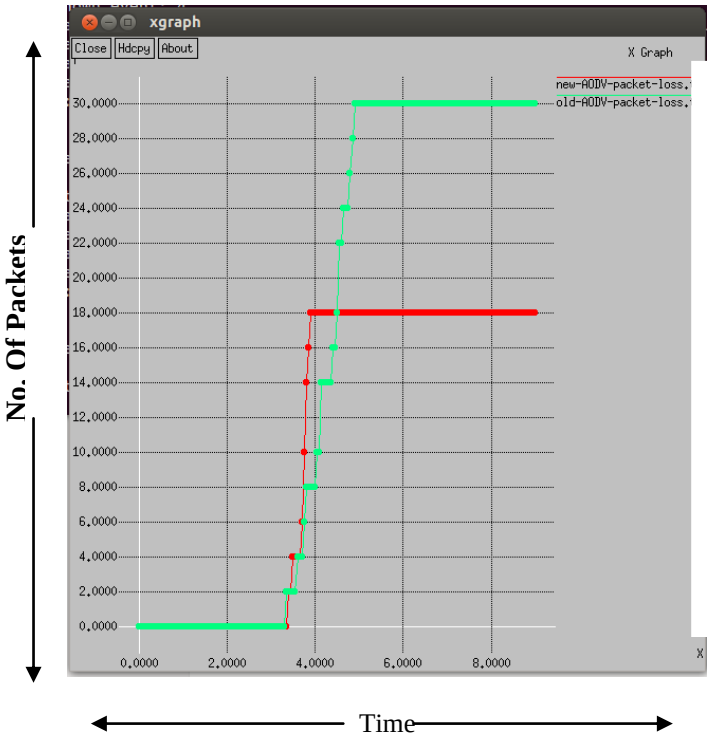

Figure 3: Shows packet loss

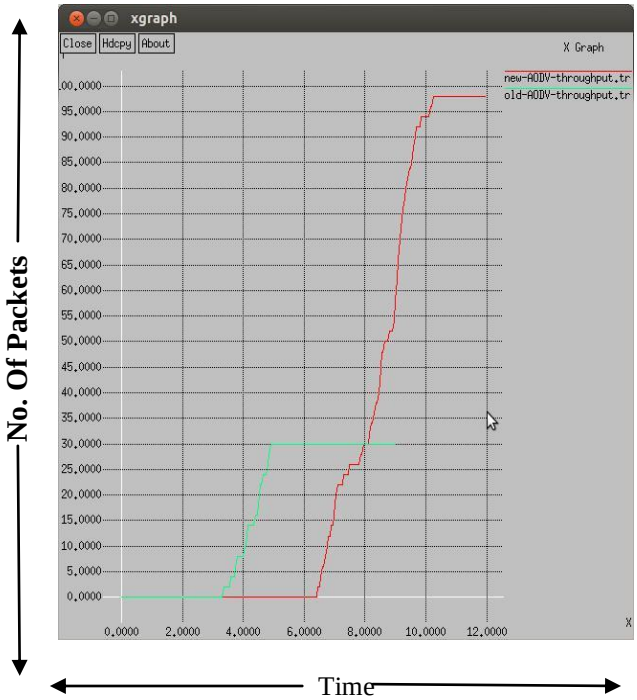

Figure 4: Comparison of Throughput with and without new technique

Optimising the throughput parameter for Selective packet drop attack:

Calculating the Throughput of the system for new technique, we have used the following formula:

Throughput = Packet received / Amount of Packet forwarded (Over certain time interval)

Table 4: Comparison of Throughput parameter

Time(seconds)	Without Technique	With Technique
6.0000	30	0
8.0000	30	30
9.0000	30	55
10.0000	30	95

The throughput is higher as compared to the system where no such algorithm was used.

In Figure 2 that represents the graph of network delay which is reduced. The network delay is more in the previous scenarios. Red line shows new delay and green line shows old throughput. Figure 3 shows the graph of packet loss. The packet loss is more in the previous scenarios. The packet loss is reduced in the new scenario as indicated with green line. Figure 4 shows the graph of Throughput is shown. The network throughput is more in the new scenario. The throughput with the new technique is constant in the beginning and increases with a sharp value after a certain interval of time. Thus this technique has proved to be better in isolating the attack.

VI. CONCLUSION

We mainly aim to study the Mobile Ad-hoc network and its various features. In these kinds of networks, mobile nodes communicate with each other and they are self-configuring nodes that can join the network or leave it any instant of time. In this paper we have studied various types of attacks like internal attack that is done by the nodes in path, external attack where an outside node is malicious, active and passive attack. The main concern of this paper is to focus on Selective packet drop attack. There are many problems and vulnerabilities in selective packet drop attack which can be

removed with the help of monitor nodes. We tend to use the Diffie-Hellman technique in this case where the selective packet drop attack can be isolated to an extent. Experimental results shows that proposed technique is far better than old ones as it has better throughput, less delay and less packet loss as compared to existing techniques.

ACKNOWLEDGEMENT

I hereby acknowledge that the above mentioned work is my own research work and I am completely responsible for any kind of misuse of material. I thank my mentor Er. Abhilasha to guide and encourage me and for putting all her valuable time for me to get the desired output. I also thank my parents and friends who have in any way helped me to complete my work with sheer hard work.

REFERENCES

[1] S. Taneja, Dr. K. Ashwani, M. Amandeep x, End to End Delay Analysis of Prominent On-demand Routing Protocols", IJCST Vol. 2, Issue1, March 2011

[2] A. mohamed, thesis, "analysis and simulation of wireless ad-hoc network routing protocols"2004

[3] G. Vigna, G. Sumit , Kavitha S., Elizabeth M. Belding-Royer Richard A. Kemmerer, "An Intrusion Detection Tool forAODV-based Ad hocWireless Networks", 2004

[4] S. Şen, John A. Clark, Juan E. Tapiador, "Security Threats in Mobile Ad Hoc Networks", 2010

[5] S. Sharmila and Umamaheswari G., " Defensive Mechanism of Selective Packet Forward Attack in Wireless Sensor Networks", International Journal of Computer Applications (0975 – 8887) Volume 39– No.4, February 2012

[6] N.Bhalaji , "Reliable Routing against Selective Packet Drop Attack in DSR based MANET", JOURNAL OF SOFTWARE, VOL. 4, NO. 6, AUGUST 2009

[7] A. Mavropodi, Christos D. , "Intrusion Detection of Packet Dropping Attacks in Mobile Ad Hoc Networks", Ayia Napa, Cyprus, July 6-7, 2006

[8] J. Cicho, Rafał K., Jakub L, and Marcin Z "On Alarm Protocol in Wireless Sensor Networks", 2010