UGC Approved Journal

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified

Vol. 4, Issue 7, July 2017

Detection and Isolation of Selective Packet Drop Attack in MANET

Sandeep Singh[1], Rajinder Singh[2]

Research Scholar, Guru Kashi University, Talwandi Sabo[1]

Asst. Prof., University College of Computer Applications, Guru Kashi University, Talwandi Sabo[2]

Abstract: Wireless Networking is a technology in which two or more computers communicate with each other using standard network protocols but without using cables. In this we work based on MANET. MANET stands for Mobile Ad hoc Network. is a robust infrastructure less wireless network. It can be formed either by mobile nodes or by both fixed and mobile nodes. It has a limited physical security. There may be various types of Attacks like Black hole attack, Eavesdropping, jamming, Selective Packet Drop Attack. There are various existing Techniques like key distribution, monitoring mode etc. which have disadvantages like less throughput, packet loss, average delay. In our technique we will increase throughput, and minimize packet loss and average delay.

Keywords: MANET, Eavesdropping, jamming.

I. INTRODUCTION

Wireless Networking is a technology in which two or more computers communicate with each other using standard network protocols and without the using of cables [3]. There are two types of wireless networking. First is infrastructure mode is that mode in which wireless network adaptor is used to connect with the already existing networks with the help of access point. Wireless adaptor is also known as wireless clients [4].It has a central controller. Second is Infrastructure based network, communication is takes place only between the access points and the wireless nodes.

Mobile Ad hoc Networks (MANET) are the wireless networks of mobile computing devices without any support of a fixed infrastructure. The mobile nodes in a MANET self organize together in some arbitrary fashion. A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. These networks can be applied between persons or between vehicles in areas which are depleted of fixed infrastructure. Two nodes can directly communicate with each other if they are within the radio range. If the nodes are not within the radio range they can communicate with each other using multi hop routing. The wireless link between the nodes in mobile networks is highly vulnerable. This is because nodes can continuously move causing the frequent breakage of the link.[down].

Securing wireless ad-hoc networks is a highly challenging issue. Understanding possible form of attacks is always the first step towards developing good security solutions. Security of communication in MANET is important for secure transmission of information. Absence of any central co-ordination mechanism and shared wireless medium makes MANET more vulnerable to digital/cyber attacks than wired network there are a number of attacks that affect MANET [6]. These attacks can be classified into following:

1. Active Attack
2. Passive Attack

1. Passive attacks: A passive attack obtains data switched in the network without disturbing the communications operation. The passive attacks are difficult to detection [5, 6].This attack target confidentiality attribute of the system. It includes accessing network traffic between browser and server accessing restricted information on a website. Examples of Passive Attacks are eavesdropping, snooping.

2. Active Attack: An active attack in which any data or info is interleaved into the network so that information and procedure may harm [5,6]. It involves modification, fabrication and disruption and affects the operation of the network. Example of active attacks is impersonation, spoofing**.**

Eavesdropping:

This is a passive attack. The node simply observes the confidential information. This information can be later used by the malicious node. The secret information like location, public key, private key, password etc. can be fetched by eavesdropper. [6]

UGC Approved Journal

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified

Vol. 4, Issue 7, July 2017

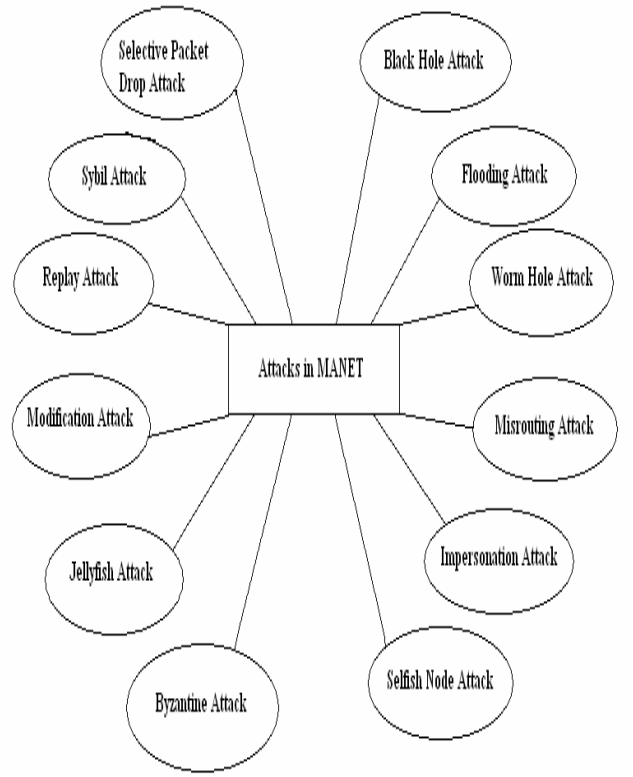

Fig 1.1 Attacks in MANET

Black hole Attack:
In this attack, an attacker advertise a zero metric for all destinations causing all nodes around it to route packets towards it. A malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. A malicious node drops all packets that it receives instead of normally forwarding those packets. An attacker listen the requests in a flooding basedprotocol. [6]

Wormhole Attack:
In wormhole attack, a malicious node, receives packets at one location in the network and tunnels them to another location in the network, where these packets are resent into the network. This tunnel between two colluding attackers is referred to as wormhole. [7]

Byzantine attack:
In this attack, a compromised intermediate node or a asset of compromised intermediate nodes works in collision and carries out attacks such as creating routing loops, forwarding packets on non-optimal paths and selectively dropping packets which result in disruption or degradation of the routing services. [7]

Jamming:
In jamming, attacker initially keep monitoring wireless medium in order to determine frequency at which destination node is receiving signal from sender. It then transmit signal on that frequency so that error free receptor is hindered [6].

Gray-hole attack:
This attack is also known as routing misbehavior attack which leads to dropping of messages. Gray hole attack has two phases. In the first phase the node advertise itself as having a valid route to destination while in second phase, nodes drops intercepted packets with a certain probability.

II. RELATED WORK

Chuachan T., Puangpronpitag S: Security attacks in MANETs can be classified into two major categories, namely passive attacking and active attacking. The passive attack receives data, and does not disrupt network operations. A malicious user wants to obtain private or sensitive information. Users in traditional MANETs can encrypt their traffic to avoid the passive attack. Yet, a data encryption increases computational power, and possibly leads to increase a risk

UGC Approved Journal

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified

Vol. 4, Issue 7, July 2017

from Denied of Service (DoS) attacks. The active attack involves in a manipulation of the network operations to pursue malicious objectives. An attacker forcibly acquires routing paths, and alters routing messages. Consequently, current MANETs can be assaulted by multiple types of MANET security attacks. [1]

N.Bhalaji and Dr. A.Shanmugam in their paper entitled "Reliable Routing against Selective Packet Drop Attack in DSR based MANET" proposed dynamic trust based approach to detect and isolate selective packet drop attack in MANET. Simulation results of this technique shows that this new routing mechanism is much better than other conventional techniques used for isolating selective packet drop attack in MANET. Other conventional techniques are usually based on encryption and hashing mechanisms. These techniques are only suited for planned networks. For network like MANET dynamic trust based technique is much better than existing techniques. This dynamic trust based technique is also responsible for identifying and isolating the malicious nodes from the active data routing and forwarding.[2]

Anita and Abhilasha in their paper entitled "A Novel Technique to Protect and Isolate Selective Packet Drop Attack in MANET", proposed a novel technique based on the DiffieHellman algorithm to reduce packet drop problem by detecting and isolating selective packet drop attack in MANET.By this technique throughput of the whole network will be improved. This Diffie- Hellman algorithm based technique is also responsible for less packet delay and less packet loss as compare to other techniques.[3]

Selective Packet Drop Attack

Selective Packet drop attack is the type of denial of service attack. Packet dropping attack is launched on the forward phase. So it is very complex and difficult to segregate. This attack is very easy to perform but very difficult to detect it. Selfish node also drop packet in their different ways. They drop packets only to save their resources not damage any other nodes. Selective forwarding attacks may damage some mission of applications. In these types of attacks, malicious nodes act as normal nodes every time but selectively drop sensitive packets, such as packet coverage the movement of the differing forces. Such selective dropping is tough to detect. Counter measures to selective forwarding attacks cannot recognize malicious nodes or need time synchronization [2, 4]].

Selective forwarding attacks can root serious threats on many applications. Selective forwarding attacks have some nodes which drop some or all packets. Attacker can initiate the selective forwarding attack and crash a portion of packets for which it require to store set while forward the rest. Selective forwarding attack is complex attack to detect, since packet drops in sensor networks may be caused by untrust worthy wireless communications or node failures.

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 fewer bendy 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 is occasionally drops a small part of consecutive packets and can be efficiently reducing the throughput of a TCP flow to near zero.

III. PROPOSED WORK

A passive outsider eavesdrops on all communication and aims to compromise privacy. Selective packet Drop attack is the partial denial of service attacks which is triggered by the malicious nodes in the network. In the past, many techniques have been proposed to isolate Selective attacks from the network. When this attack is triggered in the network, end to end delay increase as steady rate and throughput of the network reduced. In this work, a new methodology is proposed to detect and isolate Selective Packet Drop attack in AODV Protocol. There are nodes in the network one act as source and other act as destination. Suppose source sends packet from source to destination. It sends 10 packets. There is a malicious node at the centre which drops the packet and only forward few packets. This problem arise the packet loss problem. Toovercome this problem a novel technique will be proposed that is Diffie-Hellman.

Diffie Hellman Technique is applied on Source and Destination. In this both Source and destination share their public keys and then applying their formula and generate some value using their private key. After that this value is shared between again source and destination. Then both source and destination decode this value using their private key. If both has same value then communication starts. If both keys do not match then Source sends ICMP messages and call monitor mode.

Algorithm of Proposed Technique

Start ( )

1. Deploy the wireless ad hoc network with fixed number of mobile nodes and in fixed area
2. Select the shortest path between the source and destination using AODV routing protocol
3. Source and Destination verify the route

UGC Approved Journal

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified

Vol. 4, Issue 7, July 2017

To verify the route
{
4. Source node and Destination node apply Diffie Hellman Technique.
If (Malicious node==exits)
{
a. Source node sends ICMP packets.
b. Nodes other than path nodes start monitoring the path using fake messages.
c. Monitoring Nodes send malicious node information to source.
d. The source segregate the selected path.
e. The source select the other best path based on hop count and sequence number.
}
5. Else
{
The source keeps on communicating with destination
}
End
}

IV. RESULTS

The whole scenario has been implemented on NS2 simulator.

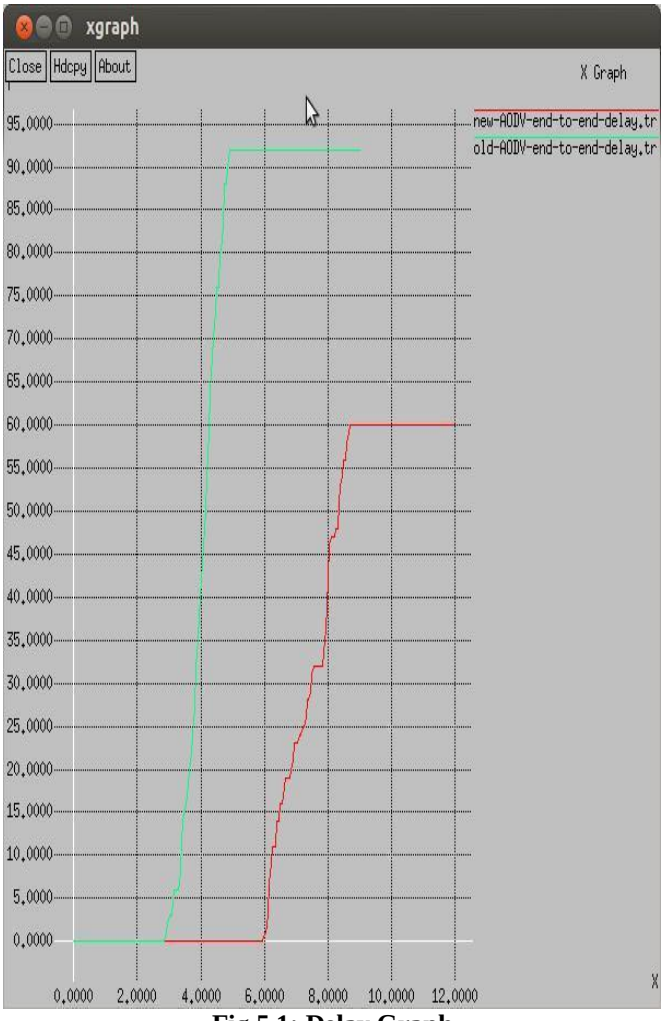

Fig 5.1: Delay Graph

In figure 5.1, it is shown that graph of network delay. The network delay is more in the previous scenarios. The network delay is reduced in the new scenario.

UGC Approved Journal

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified

Vol. 4, Issue 7, July 2017

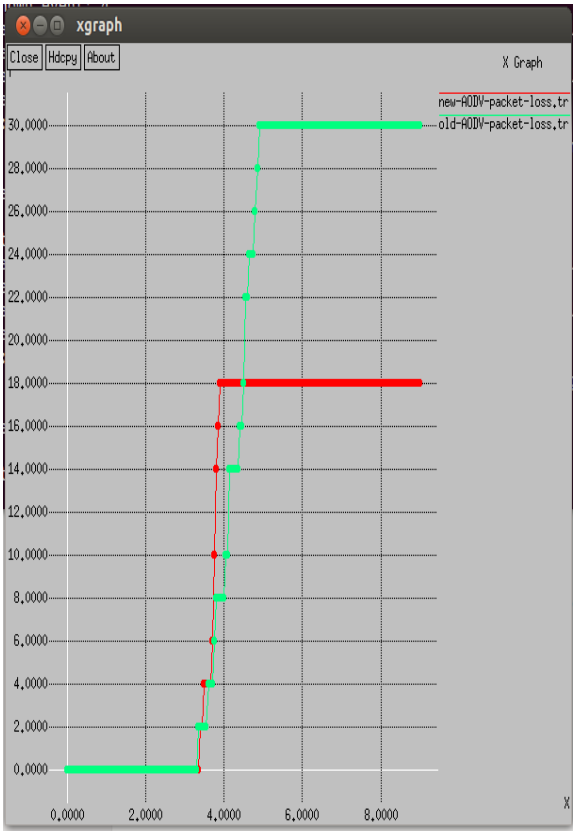

Fig 5.2 Packet loss Graph

In Fig 5.2, it is shown the graph of packet loss. The packet loss is more in the previous scenarios. The packet loss is reduced in the new scenario

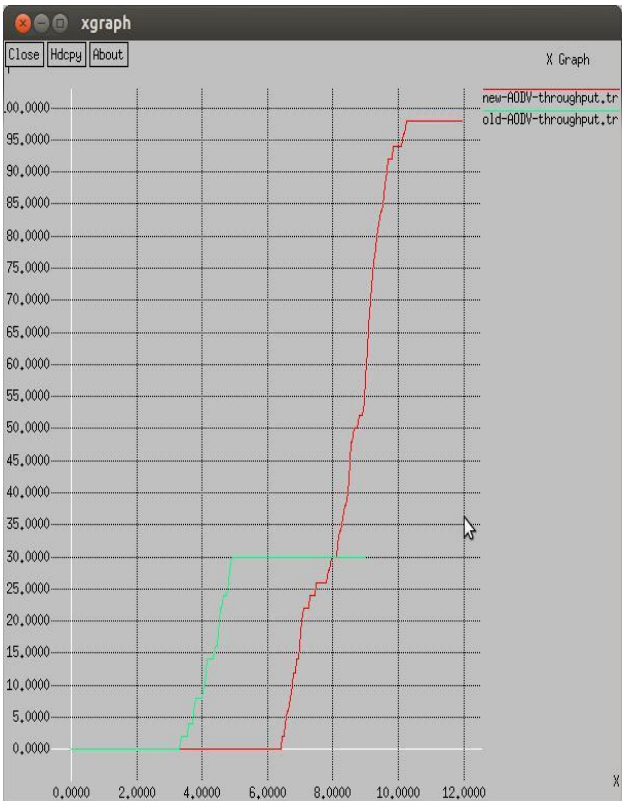

Fig 5.3 Throughput Graph

UGC Approved Journal

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified

Vol. 4, Issue 7, July 2017

In Fig 5.3, it is shown the graph of Throughput. The network throughput is more in the new scenario. In the old scenario it will reduced due to selective packet drop attack in the network which is triggered by the malicious node

Table 5.1 Comparison between Two Techniques

Sr. No.	Parameters	Existing Technique	Implemented Technique
1	Delay	92	60
2	Packet Loss	30	18
3	Throughput	30	95

V. CONCLUSION

There is increased through put, reduced delay of packets and packet loss during the Selective Packet Forward Attack. It can be said that the proposed technique is better as compared to the existing technique as shown in table 5.1. In this paper discussed about MANET, its attack which trigger on it and various techniques to isolate and prevent selective packet drop attack which degrade the system performance by decreasing throughput, increasing latency and end-to-end delay. In our proposed technique delay, packet loss and throughput are better.

REFERENCES

[1] Chuachan T., Puangpronpitag S., "A Novel Challenge & Response Scheme against Selective Forwarding Attacks in MANETs", 2013 IEEE
[2] N.Bhalaji and Dr. A.Shanmugam, "Reliable Routing against Selective Packet Drop Attack in DSR based MANET", "JOURNAL OF SOFTWARE", VOL. 4, NO. 6, AUGUST 2009.
[3] Anita and Abhilasha, "A Novel Technique to Protect and Isolate Selective Packet Drop Attack in MANET", "International Journal of Advanced Research in Computer and Communication Engineering", Vol. 3, Issue 6, June 2014, ISSN (Online): 2278-1021 and ISSN (Print): 2319-5940.
[4] Rani K., Magnat K., "A Process to Improve the Throughput and Reduce the Delay and Packet Loss in Ad-Hoc Wireless Network", International Journal of Computer Applications (0975-8887), Volume 99-No.9, Aug. 2014
[5] Patel C.V., Joshi A.H., Shah B.D., Patel C., "Security Attacks On MANET Routing Protocols" ,International Journal of Computer Trends and Technology (IJCTT), Vol. 4, Issue 10, Oct 2013
[6] Goyal P., Parmar V., Rishi R.,"MANET: Vulnerabilities, Challenges, Attacks, Application" , IJCEM International Journal of Computational Engineering & Management, Volume 11, Jan. 2011 ISSN (Online): 2230-7893, 2011.
[7] Nandy R., Roy D.B., "Study of Various Attacks in MANET and Elaborative Discussion Of Rushing Attack on DSR with clustering scheme" Int. J. Advanced Networking and Applications" Volume 03, Issue 01, Pages 1035-1043, 2011
[8] Sharmila S., 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