IJCSN International Journal of Computer Science and Network, Volume 6, Issue 3, June 2017
ISSN (Online): 2277-5420
www.IJCSN.org
Impact Factor: 1.5

A Review on Detection and Isolation of Selective Packet Drop Attack in MANET

[1] Sandeep Singh; [2] Dr. Rajinder Singh

[1] Research Scholar, Guru Kashi University
Talwandi Sabo (151001)

[2] Asst . Prof., University College of Computer Applications
Guru Kashi University, Talwandi Sabo (151001)

Abstract - In MANET many vulnerable attacks like passive and active are possible, by which performance of the network goes slow down. Among all the attacks discussed in literature 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 previous research, many techniques have been proposed to isolate Selective attacks from the network. When Selective packet attack is triggered in the network, throughput of the network reduced and delay increase as steady rate. In my research, I will use more optimized technique to improve the performance of the network by isolating the selective packet drop attack in AODV Protocol.

Keywords - *Manet, AODV, DSR, DSDV*

1. Introduction

Wireless Networking is a technology in which two or more computers communicate with each other using standard network protocols but without using cables. The transmission takes place with the help of radio waves at physical level In this type of network, devices can easily two using radio frequency [11].

1.1 MANET

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 and forming arbitrary topology. They can act as both routers and hosts. They have ability to self-configure 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. [2]

In multi-hop network when one node is out of transmission range of other node then data packet need to traverse multiple route to reach destination node. Due to mobility, route may also changes continuously from source to destination. There are much more ease of deployment of network in MANET. Fig 1 shows architecture of MANET.

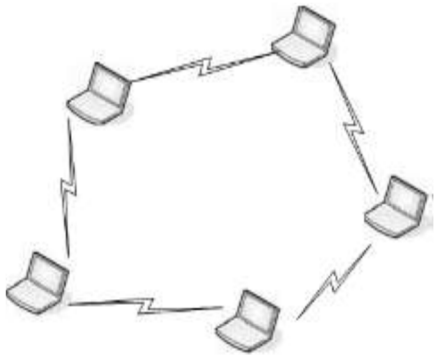

Fig 1. MANET Architecture [2]

1.1.1 ROUTING SCHEMES IN MANET

There exist several proposals that attempt to architect a secure routing protocol for ad hoc networks, in order to offer protection against the attacks mentioned in the previous section. The routing protocol means for wired networks cannot be used for mobile ad hoc networks because of the mobility of the networks. The ad hoc routing protocols can be divided into two classes:[3]
1. Table-driven routing protocols
2. On demand routing protocols.

A. Proactive (Table Driven)

In Proactive Routing every node maintains its routing table for the route to all the destinations in the network. To maintain that, updating messages are transmitted periodically for all the nodes. As a consequence of that, these protocols present great bandwidth consumption.

Also, there is a great routing overhead. However, as an advantage, the route to any destination is always available. Thus, the delay is very small. The Examples are: DSDV (Dynamic Destination Sequenced Distance Vector), OLSR, TBRPF, CGSR (Cluster head Gateway Switch Routing protocol), WRP (Wireless Routing Protocol), and OSPF (Open Shortest Path First). One example of proactive scheme is described as follows:[2]

Destination sequence distance vector (DSDV):

DSDV is a distance vector protocol also known as a proactive protocol and a table-driven routing protocol which is derived from the Bellman-Ford routing mechanisms. It has incorporated modifications to address the poor looping properties and time dependent nature of the interconnection topology describing links between mobile hosts. DSDV requires that each mobile host maintains a routing table which lists all available destinations with the number of hops to these destinations .Thus, each hop is forming a network which is required to advertise its own routing table to its "current" neighbors.[8]

Reactive (Demand driven)

The Reactive protocol or on-demand routing protocols do not maintain the network topology information. The source node creates routes only when it requiring communication with other nodes. Hence these protocols do not exchange routing information periodically. The routing overhead is small since the routes are determined only on demand. As a main disadvantage the route discovery introduces a big delay. The Examples are: AODV, DSR, TORA (Temporally Ordered Routing Algorithm), etc. One example of proactive scheme is described as follows [2]

Ad-Hoc on Demand Distance Vector (AODV)

The AODV routing protocol is a reactive protocol designed for wireless ad hoc networks [9]. AODV was an improvement on DSDV routing protocol because it minimizes the number of required broadcasts of data packet by creating routes on a demand basis. AODV routing protocol uses reactive approach for finding appropriate routes, that is, a route is established only when it is required by any source node to transmit data packets to destination. The protocol uses destination sequence numbers in routing process to identify the recent path. Intermediate nodes store the next node information corresponding to each data packet transmission.

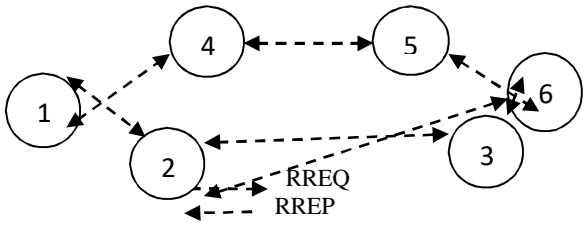

Figure 1.1 AODV algorithm

There are three main types of messages in AODV: route request (RREQ), route reply (RREP), and route error (RERR) messages. When a node wants to communicate with another node in the network and does not have a fresh route to this destination, it starts the route discovery process by broadcasting a RREQ message for the destination node into the network. Intermediate nodes that receive this request either send a RREP to the source node if they have a fresh route to the destination node and the "destination only" flag is not set, or forward the RREQ message to other nodes. A fresh route is a valid route entry whose sequence number is equal to or greater than that contained in the RREQ message. If the request packet has been forwarded by this intermediate node before, it is silently dropped. When the destination node receives a RREQ for itself, it sends back a RREP message on the reverse route.The requesting node and the nodes receiving RREP messages on the route update their routing tables with the new route. [10]

1.1.2 ATTACKS IN MANET:

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 two types:

Table 1.1 Classification of Attacks in MANET

Active Attacks	Black hole attack, modifications, wormhole, byzantine, Sybil etc
Passive Attacks	Eavesdropping, jamming, traffic analysis and monitoring

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]

Black hole Attack:: In this attack, an attacker advertises 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 based protocol. [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 [6].

Selective Packet Drop 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. 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.

2. Related Work

Chuachan T., Puangpronpitag S

A. Security Problems in MANETs

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 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]

B. Selective Forwarding Attack

Selective Forwarding Attack is one of the most potential MANET attacking methods.To attack MANETs, the attacker rejects to forward data messages for other nodes while forwarding routing messages. There are several security schemes proposed to protect against the selective forwarding attack. However, the previous schemes seem to have some drawbacks. [1]

Selective Packet Drop Attack

A selective packet drop is a kind of denial of service where a malicious node attracts packets and drops them selectively without forwarding them to the destination . As an example consider the scenario in figure 2.1. Here node 1 is the source node and node 7 is the destination node. Nodes 2 to 6 acts as the intermediate nodes. Node 5 acts

as a malicious node. When source wishes to transmit data packet, it first sends out RREQ packets to the neighbouring nodes. The malicious nodes being part of the network also receives the RREQ. The source node transmits data packets after receiving the RREP from the destination. As node 5 is also the part of routing path will receive the data packets and drops some of them while forwarding others. This type of attack is very hard to detect as the malicious nodes pretend to act like a good node. The selective packet dropping attacks have a great negative influence over the performance metrics of conventional protocols. In this article we propose a dynamic trust based approach to combat selective packet drop attacks. [4]

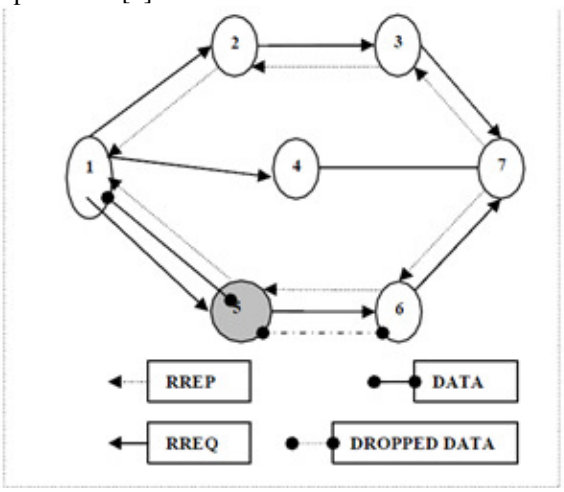

Fig 2.1 Selective Packet Drop Attack Scenario

3. Proposed Work

This section presents the extension of Association based routing which is to be applied over the AODV protocol in order to enhance the security. The purpose of this scheme is to fortify the existing implementation by selecting the best and secured route in the network.

In the present research, Diffie-Hellman technique had been used 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. Now source sends private key "A" to the source and when destination receive it, also send "B" to the source. When packet reaches to malicious node it does not have key "B". Then this path will not be established due to present of malicious node.

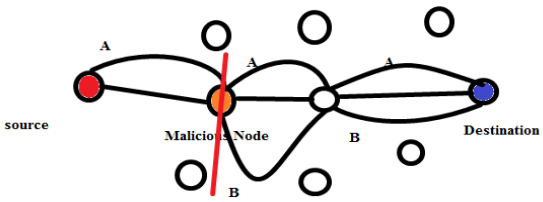

Figure 3.1 Secure Path with Diffie-Hellman

Now another path will be choose for communication where there is no malicious node. The secure path will be established after the exchange of the key. In this way packet loss problem due to malicious node will be minimized with the help of Diffie-Hellman technique.

3.1 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

   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
   }

3.2 Flowchart of Proposed Technique

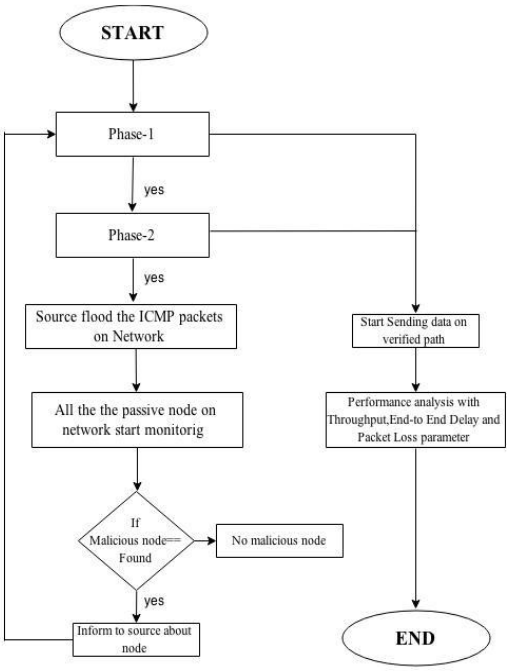

Figure 3.2 Flowchart of proposed technique

4. Conclusion and Future Scope

4.1 Conclusion

Mobile ad-hoc network have been wast area of research work from past few years because its widely used application in battlefield and business purpose. Due to openness and dynamic topology network is vulnerable from attacker. This research discussed 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. There is acknowledgement and IDS based schema which prevent this attack in AODV protocol. This feature work implemented new algorithm based on monitor node technique which improves network efficiency.

4.2 Future Scope

Although there was increased through put, reduced delay of packets and packet loss during the Selective Packet Forward Attack. It can be said that even if the proposed technique is better as compared to the existing technique yet there is further scope of improvement in the designed methodology and further investigation of the proposed methodology is required for better results.

References

[1] Chuachan T., Puangpronpitag S., "A Novel Challenge & Response Scheme against Selective Forwarding Attacks in MANETs", *2013 IEEE*

[2] 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), Volume 4, Issue 10, Oct. 2013*

[3] Garg V., Shukla M.K., Choudhury T., Gupta C., "Advance Survey of Mobile Ad-Hoc Network," *IJCST Vol. 2, Issue 4, Oct. - Dec. 2011*

[4] Bhalaji N., Shanmugan A., "Reliable Routing against Selective Packet Drop Attack in DSR based MANET", *JOURNAL OF SOFTWARE, Volume 4, No.6, Aug. 2009*

[5] kyasanur P., Vaidya N.H., "Selfish MAC layer Misbehavior in wireless networks", *IEEE on Mobile Computing ,2005*

[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] Bhatia A.S., Cheema R.K.,"Analysing and Implementing the Mobility over MANETS using Random Way Point Model", *International Journal of Computer Applications (0975 – 8887) Volume 68, No.17, Apr. 2013* .

[9] G. Vigna, S Gwalani "An Intrusion Detection Tool for AODV-based Ad hoc Wireless Networks".

[10] Sevil Şen, John A. Clark, Juan E. Tapiador "Security Threats in Mobile Ad Hoc Networks".