To Evaluate and Improve OLSR Protocol to detect and isolate Gray hole Attack in Mobile Ad-hoc Network

[1]Vikramjeet singh,[2]Ranbir Singh
[1] M.tech scholar, [2]Assistant Professor
[1]Computer science and engineering,
[1]SUSCET, Mohali,India

***Abstract* - MANET is infrastructure less, decentralized multi hope network where the nodes are randomly to move in any direction, there each node works as a router and host to send packet to each other, there is no any requirement of fixed infrastructure. There are many security threats in MANET. Various types of attacks can be easily trigger in the network. So manet has a security issue. In this paper we have discussed about grayhole attack in OLSR protocol. Due to this attack network performances degrade. Therefore a novel technique has been proposed to detect and isolate gray hole attack in the network using monitoring nodes.**

***IndexTerms* - MANET, Attacks, Grayhole, Throughput, ZRP, internal attacks**

I.INTRODUCTION

MANET is a mobile ad-hoc network. An ad-hoc network is set of wireless mobile nodes that have ability to communicate with each other without the help any centralized administration [1]. MANET has a dynamic topology due to the mobility of nodes. Wireless network contain collection of mobile hosts (nodes) that are communicate with each other through the wireless links. MANET is infrastructure less, decentralized multi hope network where the nodes are randomly to move in any direction, there each node works as a router and host to send packet to each other, there is no any requirement of fixed infrastructure. MANET provide successful solution in several cases, where any wired or wireless infrastructure is not accessible damaged or destroyed and overloaded due to some reason such as military operations, emergency and rescue operations, disasters relief efforts and tactical batter field; as well as conferences and class rooms or in research area like a sensor network [2]. MANET is network which is fully distributed and able to work at anywhere without the help of any centralized administration or access points or base stations.

Fig.1.1 MANET Network

1.1 Challenges in MANET: There are many challenges in MANET which are as follows:

1.1.1 ***Routing:*** The most common challenging issue in MANET is Routing data packets in between nodes when there is change in the topology. Another challenge for MANET is multicast routing because the nodes are move randomly in the network. Several of the protocol based on the reactive routing rather than proactive routing [2].

1.1.2 Security and Reliability: In an ad-hoc network security is a biggest problem due to the nasty neighbors that are relaying on the information. So there we need of some security mechanism such as the authentication and the management of key to provide the security to each node in MANET. Another problem introduced in MANET is due to the wireless links that have finite transmission area is reliability [3].

1.1.3 Quality of service (QOS): The common challenge in changing environment is providing the different quality of service level. An adaptive QoS must be implemented over the traditional resource reservation to support the multimedia services [1].

1.1.4 Inter-networking: To interact with an ad-hoc network, inter-networking between MANET and infrastructure network is often expected in many terms. The coexistence of routing protocol for mobile hosts is a challenge to manage the speed of nodes.

1.1.5 Power consumption: For various light-weight mobile devices, the communication related function should be optimized for lean power consumption. Conservation of power and power aware mobility management [4].

1.1.6 Multicast: Multicast is able to support multi-party wireless interaction. The multicast routing protocol must be able to deal with the speed of nodes that include any time leave or join the network, so the multicast tree is no longer static.

1.2 Attacks in MANET: The higher challenging issue in MANET securing wireless ad-hoc network to provide the better security solution first we require to know about the type of attacks to protect the information transmission from the attacks. There are various kinds of attacks available in the MANET. It is classified into two groups:

***1.2.1 Active attack*:** There are two type of Active attacks are known as external as well as internal attacks. Active attacks are the attacks that disturb the network performance and task by sending the wrong or modified information and false message [5].

1.2.1.1 Internal attacks: Internal attacks are attackers that are present inside the network. In internal attacks the attacker nodes that belong to network take unauthorized access and deal as are normal node to disrupt the network. These nodes analyze the traffic between other nodes and also take part in other network activities.

1.2.1.2. External attacks: External attacks are attacker that not belongs to the network or outside the network. External attacks are attacks that done by the nodes that are outside the network or which is not present in the network. For example: jamming, modification and message reply.

***1.2.2 Passive attacks*:** Passive attacks are attacks that are difficult to find on the network and does not disturb the network task, performance and operations. The example of passive attacks is traffic analysis and traffic monitoring [6].

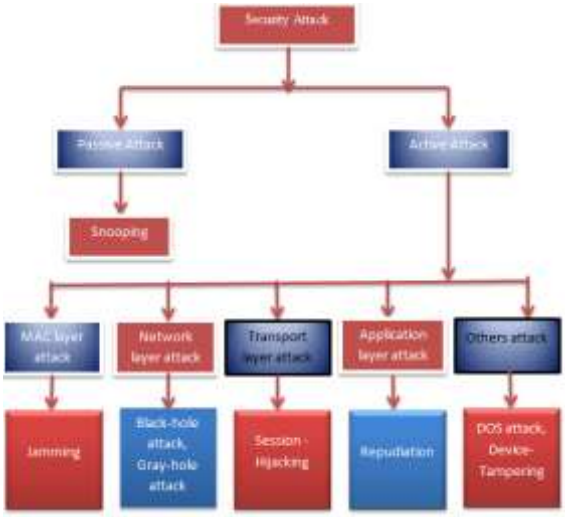

Fig.1.2 Security Attacks in MANET

II. Review of Literature

In this paper [3], simulation of secure AODV protocol is carried out by using various simulation parameters such as no. of mobile nodes, routing protocol, traffic, and transport protocol and packet size. Performance metrics PDR, end to end delay and packet delivery ratio are used to check the performance of network. Simulation is carried out by using NS2. In this paper the author provide the method to detect and prevent of gray-hole attack and also to know the behavior of malicious node. The algorithm is provides the better solution to improve the performance of ad-hoc.

In this paper [4] they have compared AODV, DSDV, DSR and ZRP protocol using the tool NS2 and was compared in term of packet delivery ratio, average delay, routing overhead and average throughput. In order to evaluate the performance of the protocols network size was 1200m x 1200m. Antenna model was Omni directional, simulation time was 10 second and the traffic type was CBR (constant bit rate) and number of nodes varies. The author have concluded that, in case of packet delivery ratio, AODV has better performance when number of nodes increase, packet delivery ratio also increase, DSDV performance is worst in this case. Average throughput of AODV was better while the DSDV was worst performance. In case of routing overhead ZRP has better performance. Due to smaller zone radius and DSR was worst. In case of average delay ZRP was better performance due to minimum delay, ODV is worst because the higher drop.

In this paper [5] author compared the routing protocols (DSDV, DSR, and ZRP). They have used the network simulator NS2 and were compared in term of packet delivery ratio and throughput by varying the pause time and the number of nodes. In simulation environment, they have constructed, the network area 500m x 500m, traffic type CBR (constant bit rate), antenna type was omni and packet interval 0.2 sec, radio propagation model was two ray ground. Number of nodes and pause time varying in this scenario. Simulation was carried out using NS2.33. They have concluded that DSR performance is same for different pause time while DSDV and ZRP when pause time increase packet delivery fraction decrees. When the number of nodes rises up, the packet delivery fraction decrease but still maximum in case of DSR as compare to DSDV and ZRP but ZRP have better performance in case of lesser number of nodes as compare to DSDV, ZRP performance goes down when no. of nodes increase. In case of throughput was increase when pause time increase for all DSDV, DSR and ZRP but maximum for DSR. But when pause time increase throughput DSDV and ZRP almost same. In term of no. of nodes increase the throughput of DSR increase but decrees for the ZRP when no. of nodes increases.

In this paper [6], they explained an advanced OLSR (AOLSR) protocol is proposed based on a modified Dijkstra's algorithm which enables routing in multiple paths of dense and sparse work topologies. The routing is based on the energy of nodes and links (implied from the lifetime) and the mobility of the nodes. It is a hybrid ad hoc routing protocol because it combines the proactive and reactive features. It is another form of source routing protocol which allows a sender of a data packet to partially or completely reveal the route the packets take through the network. Two cost functions are introduced to build link-disjoint or node-disjoint paths. Secondary functions, namely path recovery and loop discovery process are involved to manage the topology

changes of the network. AOLSR protocol is analyzed and compared with the existing MANET routing protocols namely, dynamic source routing (DSR) and OLSR. Its performance is observed to be satisfactory in terms of average end-to-end delay, packet delivery ratio (PDR), average time in first-in-first-out (FIFO) queue, and throughput.

III. Gray Hole Attack in MANET

Gray-hole attack finds on the network layer. It is kind of active attack. It acts as slow poison. It is variation of the black hole attack [7]. In Gray-hoe attack node shows the misbehavior and discards the packets when request send by source node. After sender receive some replies from the intermediate node and assign route path [8].

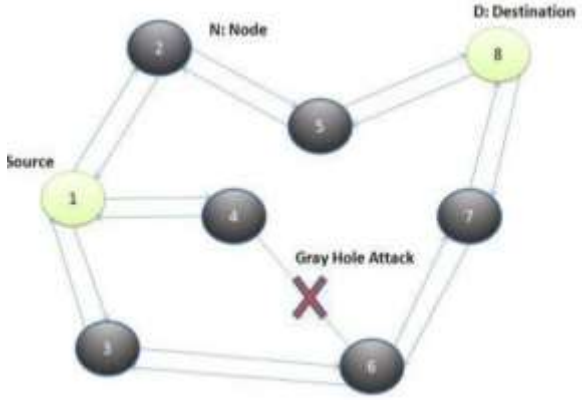

Fig.1.3 Gray hole attack

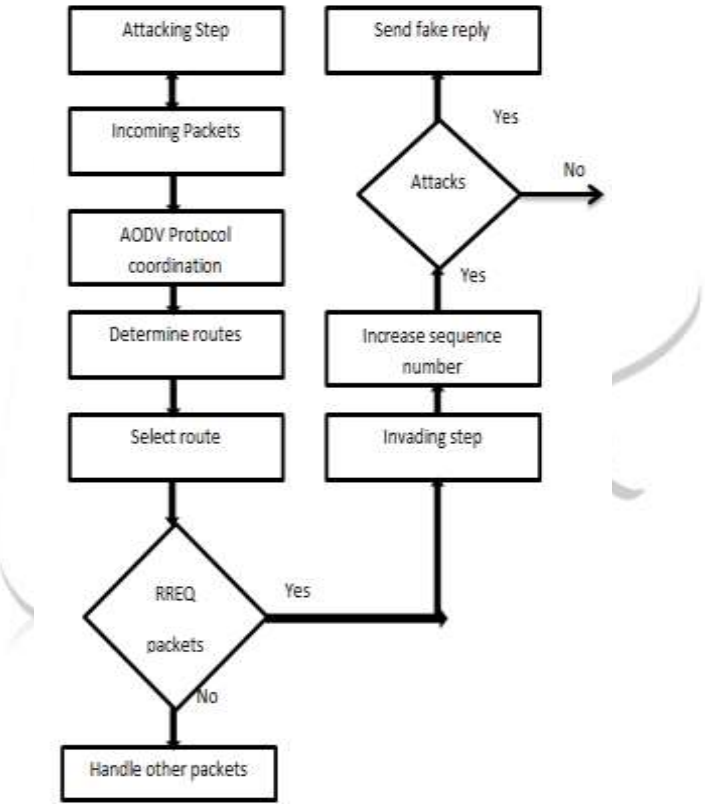

Fig.1.3 Simple framework for attack generation [2]

3.1 The Gray-hole Attack has Two Phases:

1. First phase: In this phase the node drop the packet selectively. Such as forward the TCP packet and discard the UDP packet [9].

2. Second phase: In this phase the nodes losses the received packet according to probability

To detect the gray-hole attack is more difficult than the black hole attack. A gray-hole attack shows its malicious behavior in different ways. It discards the data or information that are coming from the particular node in the network while transferring whole packets to other node [10].

3.1.2 Impact of gray-hole attack on ad-hoc network: When the gray-hole attack occur in the MANET, the performance of MANET starting to decrease in term of some performance metrics such as packet delivery ratio, end to end delay and packet loss [11].

3.1.2.1 ***Packet delivery ratio:*** Packet delivery ratio is nothing but the ratio calculated by dividing the no. of packet receives at destination by the no. of packet send at the source. Performance is best when PDR is high.

3.1.2.2 End to end delay: It is defined a total delay taken by node to reach from source to destination over a network [12].

$$\textbf{End to end delay} = T_r - T_s \qquad (3.1)$$

Where, T_r is time that packet is received T_s time that packet send at source node.

3.1.2.3 Packet loss ratio: Packet loss ratio is also known as packet dropped ratio Packet loss ratio is ration of total dropped packet from source to destination at specific time.

Packet loss = no. of packet send – no. of packet receive (3.2)

IV. Proposed Methodology

In MANET external and internal attacks are possible, that reduce the performance of the network. In internal attacks a node belongs to or present in the network become malicious node and it create attacks on network. In external attacks a malicious node which is not belongs to present outside the network, this node become the part of the networks and then creates an attack on network. An attacker that present outside the network can attack on the compromise nodes to make them as a malicious node in the network. In last times, Number of mechanisms has been proposed to separate the gray-hole attack from the network. When Gray-Hole attack is occurred in the network, the performance of network start to goes down such as throughput of the network decrease and delay increase as steady rate. In our proposed, a novel technique has been proposed to overcome the problem of gray-hole attack by detecting them and isolate them with the help of monitoring nodes. Simulating the detection of gray hole attack in OLSR protocol in MANET using NS-2 tool.

Algorithm:

1. Deploy mobile nodes in the fixed area
2. Divide whole network into zone using zone based clustering
3. Define source and destination nodes in the network
4. If (path exits from don't source to destination)

   {

   1. The source send path establishment request to gateway node
   2. The gateway node forward request to other gateway node
   3. The secure path established between source and destination

   Else

   1. Source start sending data from source to destination

   }

   If (malicious node exits)

   1. The gateway node start monitoring its adjacent node
   2. If(some node drop packet)
   3. {
   4. Isolate malicious node with its id
   5. }

      Else

      1. Keep sending data from source to destination }

V. Experimental Results

No of nodes	22
Routing protocol	OLSR
Antenna type	Omi directional
Standard	802.11
Queue	Priqueue
Packet size	1000
Interval	0.05 msecond

No of packets in queue	50

Fig.5.1 : Delay Graphs

As shown in the figure 5.1, the comparison graph is show of OLSR, AOLSR. In the figure, the delay of OLSR protocol in condition of gray hole attack is high. The enhanced OLSR protocol has less delay than existing OLSR protocol. The AODV protocol has minimum delay under the normal conditions.

Fig. 5.2 Energy Graph

As shown in the figure 5.2, the comparison graph is show of OLSR, AOLSR. In the figure, the energy of OLSR protocol in condition of gray hole attack is high. The OLSR protocol has less energy consumption than existing OLSR protocol. The AODV protocol has maximum energy under the normal conditions.

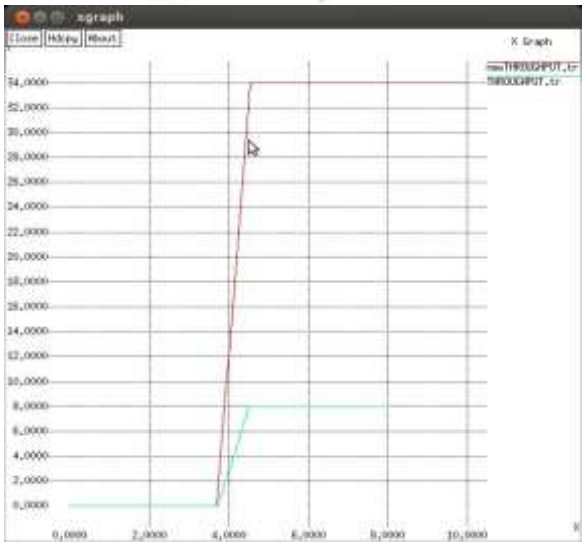

Fig.5.3 Throughput

As shown in the figure 5.3, the comparison graph is show of OLSR, AOLSR. In the graph packet loss of existing and enhanced technique packet loss is shown. The graphs shows that in enhanced technique packet loss is less than existing technique.

VI. Conclusion

Now days, Security of the network is most important and very biggest challenge in Mobile Ad-Hoc Network. There are various kind of security attacks are possible in the Ad-Hoc network. Gray-Hole Attack is one of the most common security attacks on the network layer in MANET. Due to, malicious behavior to detect the Gray-Hole Attack is from network is difficult than the Black – Hole attack. In this attacker can attack on the compromise nodes to make them malicious node. There can also possibility of more than one malicious node in the network. In this attack malicious node drop the packets rather than forward these packets to make the performance of network inefficient. So there is need of the proper and perfect mechanism to detect and remove the Gray-Hole Attack from the network to improve the performance of network such as to increase the Packet delivery ratio and Throughput and decrease the End-to-End Delay. In this paper, a novel technique has been proposed to detect and isolate grayhole attck to increase network performance.

VII. References

[1]A. Samuel Chellathuri, E. D. (2013). "EZRP: Evolutionary Zone Routing Protocol"ICACCS,1-5.
[2]Ashish K. Maurya, D. S. (Nov,2013). "Simulation based Performance Comparison of AODV, FSR and ZRP Routing protocol in MANET". IJCA,23-28.
[3]Awadesh Kumar, P.S. (July,2013). "Performance Anaysis Of AODV ,CBRP,DSDV and DSR MANET Routing Protocols using NS2 sIMULATION". *I.J computer network and information security,45-50.*
[4]Deepak Kumar, S.C. (May,2012). "Performance Comparison Of DSDV and AODV Routing Protocols in MANET",IJECCT,120-124.
[5] Divangna Gupta, R. K. (aug,2014). Simulation of Different Routing Protocols in MANET Using NS2. *International journal of Scientific and Research, Publication*, 1-5.
[6] Dhanalakshmi Natarajan and Alli P Rajendran, "AOLSR: hybrid ad hoc routing protocol based on a modified Dijkstra's algorithm", Natarajan and Rajendran EURASIP Journal on Wireless Communications and Networking,IEEE, 2014.
[7] Jaydip Sen, H. R. (2007). "A Mechanism for Detection of GRAY Hole Attack in Moile Ad-Hoc Network",ICICS ,1-5.
[8] M Ravi Kumar, D. G. (2013). "Performance Evaluation of AODV and FSR Routing Protocol in MANET,GJCST ,1-7.
[9] Onkar V.Chandure, A. P. (NOV,2012). "Simlation of secure AODVin Gray-hole Attack for Mobile ad-hoc Network IJAET, 67-75.
[10] Onkar V.Chandure, P. (2011). "A Mechanism for Recognition & Eradication of Gray Hole Attack using AODV Routing protocol in MANET". *IJCSIT* ,2607-2611.
[11] Preeti Gharwar, M. S. (April,2013). "Performance Comparison Of Routing Protocols".IJARCCE, 1920-1924.
[12] Rutvij H. Jhaveri, D. C. (2012). "A Novel Gray Hole and Black Hole Attacks in Mobile Ad-Hoc Networks". *International Conference on Advanced Computing& Communicaion Technologies"* , 556-560.
[13] Zaiba Ishrat, P. s. (2013). "Performance Evaluation Of DSDV, DSR and ZRP pROTOCOL in MANET",IJCAT ,345-349.