To Evaluate and Improve ZRP Protocol to Detect and Isolate Gray Hole Attack in Mobile Ad-hoc Network

Rajwinder Kaur
M.Tech Student
Department of Computer Science and Engineering
Sri Guru Granth Sahib World University,
Fatehgarh Sahib, India

Vinay Bharadwaj
Assistant Professor
Department of Computer Science and Engineering
Sri Guru Granth Sahib World University,
Fatehgarh Sahib, India

ABSTRACT

The mobile ad-hoc network is a type of network which has decentralized and self configuring nature. Due to which malicious nodes may join the network which is responsible to trigger various type of active and passive attacks. In this work, technique will be proposed which will improve in zonal routing protocol. In the zonal routing protocol whole network is divided into zones, in each zone zonal heads are selected which is responsible to route the data from one zone to another zone. In this work, selective routing attack is possible which reduce network performance. The improvement in the zonal routing protocol will be proposed which will be based on the monitor mode technique. In the monitor mode technique, each technique will watch its adjacent technique and node which is responsible to drop packets will be detected as malicious node from the network.

Keywords

MANET, Attacks, Gray-hole, Throughput, ZRP, internal attacks

1. 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 communicated with each other through the wireless links. 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 for 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].

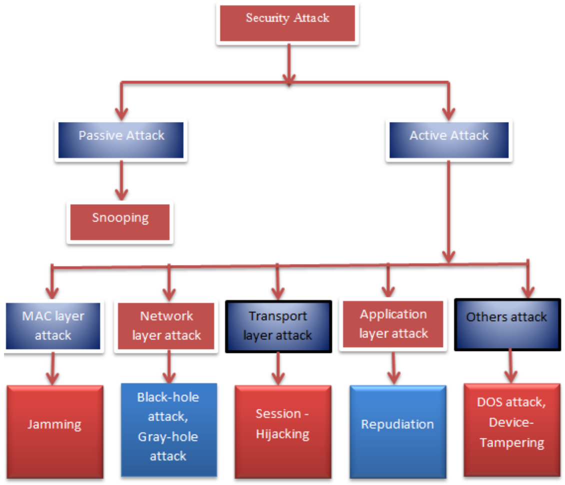

Fig.1.2 Security Attacks in MANET2. Review of Literature

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 were 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], author compared the routing protocols AODV, FSR and ZRP using Qualnet version 5.0 simulators. The result obtained for the metrics: average end to end delay, delivery ratio, throughput and average jitter. They have constructed two types of scenarios for the performance evaluation of AODV, FSR and ZRP. In one scenario the pause time was varying and in other scenarios the no. of nodes was varying, node placement strategy for both scenarios was random and simulation time 300sec was same for both and other simulation parameters was also same for both scenarios. The author has been concluded that AODV performance was better than the FSR and ZRP in term of packet delivery ratio and throughput. FSR has lowest end-to-end delay in scenario 1 and ZRP has lowest end-to-end delay in scenario 2. In both scenarios AODV has worse in case of average jittering and ZRP performance worse in case of throughput**.**

In this paper [7], author have compared the AODV, DSDV and DSR, simulation was done using NS2 (version 2.35) and constructed the area 2000m x 500m, traffic type was TCP (Transmission control protocol) and performance is evaluated by varying no. of nodes. They have compared the routing protocols in case of packet delivery ratio, packet dropped and average end-to-end delay. The author has concluded that, in case of average end-to-end delay, the performance of AODV is better than the DSR and DSDV because the AODV has less end-to-end delay. In term of packet delivery ratio AODV and DSR performance is better than DSDV. In case of packet dropped, DSR drops more packet than the AODV and DSDV so performance of DSR is worst in case of packet dropped.

3. 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-hole 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].

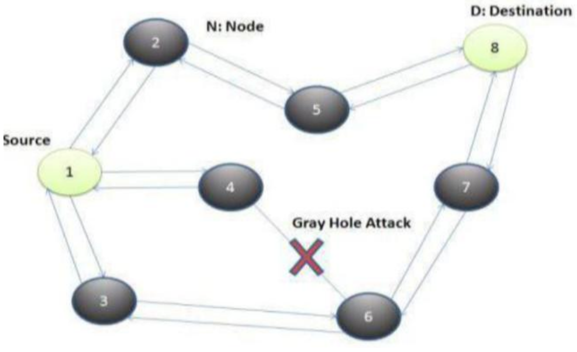

Fig.1.3 Gray hole attack

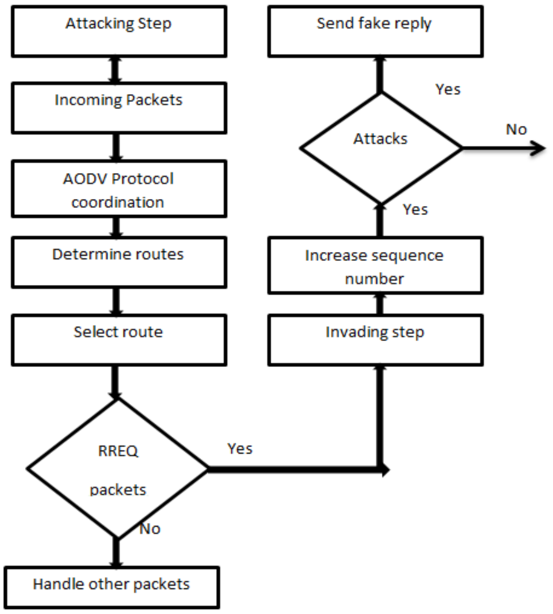

Fig.1.4 Simple framework for attack generation [2]

3.1 The Gray-hole Attack has Two Phases:

1. First phase: In this phase the node drops 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 is 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].

End to end delay = T_r - T_s

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

4. 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.

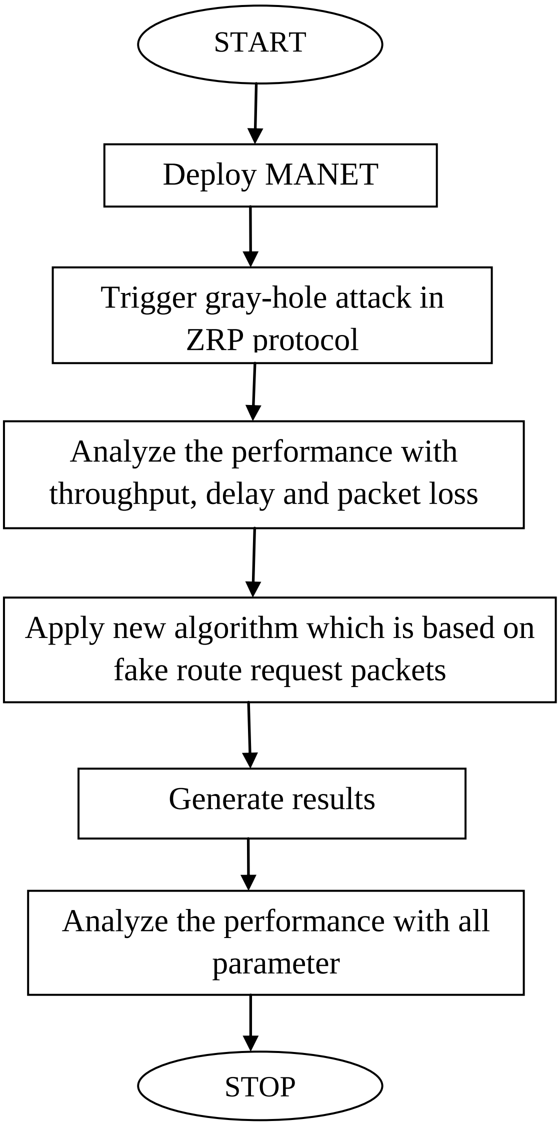
START
Deploy MANET
Trigger gray-hole attack in ZRP protocol
Analyze the performance with throughput, delay and packet loss
Apply new algorithm which is based on fake route request packets
Generate results
Analyze the performance with all parameter
STOP

Fig.1.5 Flowchart of methodology

5. EXPERIMENTAL RESULTS

a) As shown in the figure 1.6, the comparison graph is show of ZRP, enhanced ZRP and AODV protocol. Delay of OLSR protocol in condition of gray-hole attack is high. The enhanced ZRP protocol has less delay than existing ZRP protocol. The AODV protocol has minimum delay under the normal conditions.

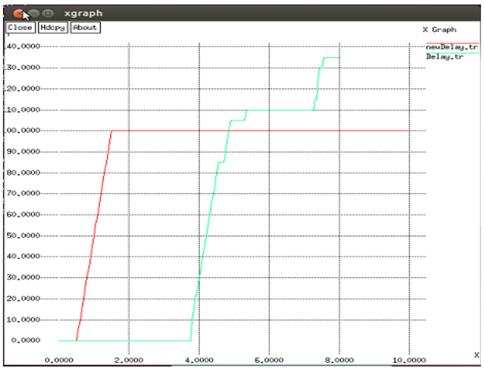

Fig.1.6: Delay Graphs

b) As shown in the figure1.7, ZRP protocol has minimum throughput in the case when gray-hole attack is triggered. The enhanced ZRP protocol had more throughput than the normal ZRP protocol. The AODV protocol has maximum throughput under normal conditions.

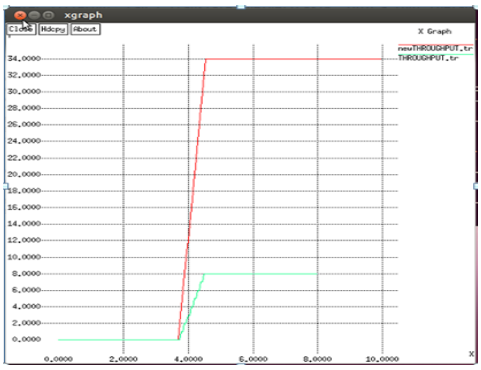

Fig.1.7 Throughput graph

c) As shown in the figure1.8, the enhanced ZRP protocol has less packet loss consumption than existing ZRP protocol. The AODV protocol has maximum energy under the normal conditions.

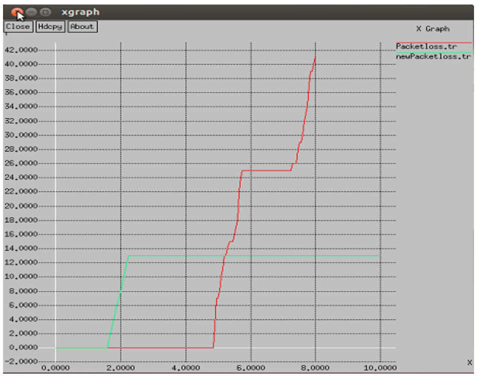

Fig.1.8 Packet loss graph

d) As shown in the figure 1.9, energy of ZRP protocol in condition of gray-hole attack is high. The enhanced ZRP protocol has less energy consumption than existing ZRP protocol. The AODV protocol has maximum energy under the normal conditions.

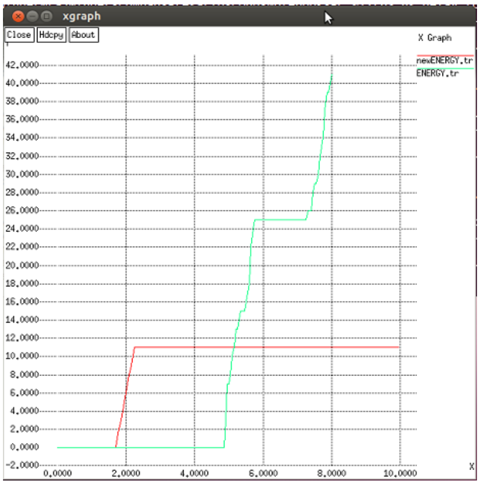

Fig.1.9 Throughput graph

6. CONCLUSION

There are various kind of security attacks which are possible in MANET. Gray-hole attack is the one of the most common security attacks on the network layer in MANET. Nowadays security of attack is most prominence and biggest challenge in MANET. In the current research, malicious node drops the packets rather than forward these packets to destination node. In this work, it is concluded that the packets send from source to destination in the shortage path without dropping packets. ZRP gives the high throughput. The defined results have shown the parameters like delay, packet loss, and throughput and energy graph.

7. 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 Protocolin 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). Simulationof Different Routing Protocols in MANET Using NS2. International journal of Scientific and Research Publication , 1-5.

[6] Ginni Tonk, I. K. (June,2012). "Performance Comparison Of Ad-Hoc Network Routing Protocols Using NS2". IJITEE , 53-57.

[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.