Simulation study of Sinkhole Attack with DSR Routing Protocol on MANET

1Mandeep Kaur, 2 Khushboo Bansal, 3 Neha Soni
1CSE Dept, Desh Bhagat University, MandiGobindgarh,Punjab , India
Mandeep0133@gmail.com
2HOD CSE Dept, Desh Bhagat University, MandiGobindgarh,Punjab , India
erkhushboo1985@gmail.com
3CSE Dept, RIMT, MandiGobindgarh,Punjab , India
ruheesoni@yahoo.co.in

Abstract: **Now a day Wireless Mobile Communication used in many applications such as military, defense etc. However this type of network have many constraint including less range of communication capability, insecure transmission channel , less consumption power which lead the system Vulnerable to many attacks . In this paper we can discuss that how the sinkhole attack degrade the performance of network. We also analyze the Simulation study of Sinkhole attack and discuss how by changing parameters performance of network will improve.**

Keywords: **Sinkhole attack, MANET, DSR routing protocol, OPNET tool.**

I. Introduction

Mobile adhoc networks playing an important role in wireless communication. It is collection of various autonomous nodes. Each node can be determines by its TCP & network Topology .Mobile adhoc network do work without any preexisting infrastructure and have centralized support which is used by many applications such as disaster rescue management military surveillance and robot network. In Distributed cooperation of nodes communication exist between two nodes which is known as Source and destination .Many nodes can be gain and loss in manet simultaneously and nodes are pushed into resource constraints such as storage, energy capacity and bandwidth.manet are thus more emotional attack to a network. The performance of any routing protocol can be realized quantitatively by means of various performance metrics such as, end to end delay, and PDR packet delivery ratio and throughput & packet loss.Manet can be classified into two major groups: internal and external . A compromised node of same network is originated in internal attack. Internal nodes can be drop, fabricate, alter, eavesdrop or misroute data packets. External attack is not participating in the routing process but disrupts network operations like flooding, dos, or cut off nodes from network. Sink hole attack is a kind of denial of service where a malicious node can read all packets by falsely claiming a fresh route to the destination. In Sink Hole Attack the node can alter or drop the data coming from the source. So it will difficult to know whose node will read the data.

II. Sinkhole

In Manet Environment Sinkhole attack act as potential threat as it grasps the dynamic property. A sinkhole node attracts all the traffic from a network through itself and exploits the information .The above objective by keeping itself updated and attractive is achieves by sinkhole. Sinkhole nodes draw other nodes attraction towards it by routing packets propagated. High quality and forged data packets are sent throughout the network in sinkhole attack.so sinkhole divert their traffic to all surrounding to a node that ignores the original data packets. Sink hole attack is a kind of denial of service where a malicious node can read all packets by falsely claiming a fresh route to the destination. In Sink Hole Attack the node can drop the data coming from the source .So it will difficult to know whose node will read the data.

III Problems of sinkhole attack

In this type of attack sinkhole node broadcasting fake routing address tries to attract data to itself by convincing neighbors and let them know itself is the only way to destination nodes. By this procedure, sinkhole node attracts all network traffic to itself. Thereafter it modify or you can say alter the data packet or drops the packet silently due to that it increase network overhead, decreases network's life time by boosting energy consumption; finally destroy the network.

IV DSR

DSR is based on-demand routing protocols which executes the route discovery process by path-finding

process when a path is required by a node. Dynamic source routing protocol (DSR) protocol designed to restrict the bandwidth consumed by control packets in ad hoc wireless networks.

Our proposed method is stated on the context on demand based algorithm of dynamic source routing protocol. This paper focuses on throughput bit per sec performance of the sinkhole attacker on dynamic source routing (DSR) protocol effectively.

Packet drop

In Scenario Packet drop is calculated by using checking on the difference between the numbers of packets sent by the source node to that of the number of packets received by the destination node. In the Sinkhole attack sinkhole act as malicious node it may drop the packets that are being received by it. Hence the packet drop parameter will show increase in the presence of sinkhole attack.

Packet delivery ratio

PDR show the ratio between numbers of packets which is received by destination node to that of number of packets sent by source node. Packet delivery ratio is expressed in percentage. As sinkhole will drop and hold the packets of the network the packet delivery ratio (PDR) of the network will decrease. The packets which are not delivered to the destination node that is either dropped or may be forwarded to some other node in the network.

Simulation results analysis

To study the effect of sinkhole attack on DSR protocol, the following network parameters like throughput, packet drop and packet delivery ratio are analyzed without the sinkhole on the network and with the sinkhole nodes present on MANET.

Network throughput

Throughput is the total number of packets received by the destination node over a period of time and the metric used to calculate the throughput is kbps. The reason is sinkhole has access to more packets on the network and sinkhole will not allow the packets to reach the destination and hence the throughput decreases.

V Simulation

A network have created in opnet with DSR protocol & checked that throughput bits per sec by DSR protocol. For this a simple network is created with the DSR protocol is shown in Fig 1 and various parameters. By using these parameters this network will help to find out, throughput bits per sec using DSR protocol so that it will help to improve the performance of the network. In this Scenario Manet network have created with 11 nodes, application definition & profile definition. All these are connected with topology 802.11. Extended g.

Fig 1 MANET Network with DSR Protocol

The result of scenario 1 is shown in fig 2 in which the throughput bits/sec in the network.

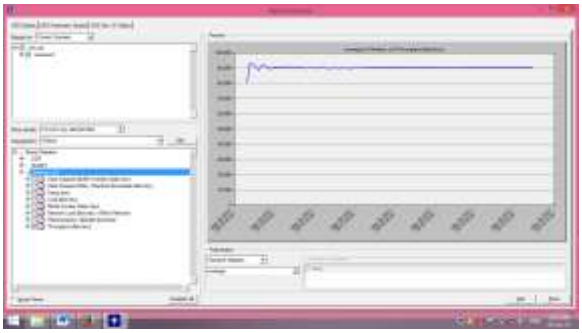

Fig 2 Throughput bits/sec using DSR Protocol

As it can be seen from fig 3, the node 3 acts as a Sink Hole node in scenario 2. The node 3 can attract all the data by pretend himself as destination node or by giving fraudulent image. In Fig 4 it is been shown that how the throughput bits per sec decreased by Sinhk Hole attack.

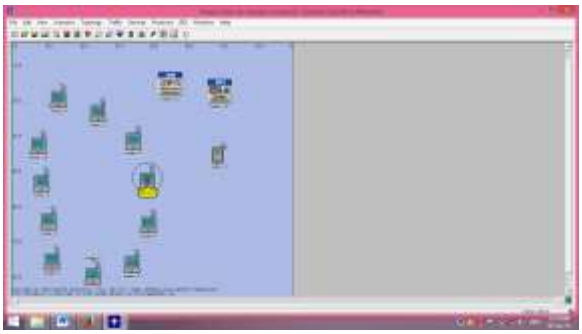

Fig 3 MANET Network with Sink Hole Attack

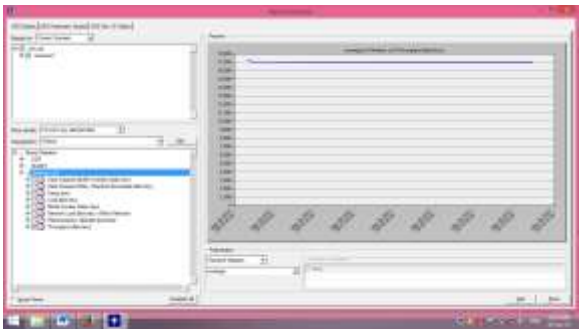

Fig 4 Throughput bits/sec in Sink Hole attack

The comparison of the results of both the scenarios it has been find out that the throughput bits per sec decreased on applying the Sink hole attack on the nodes. The difference between both the scenarios is shown in Fig 5. So the data can be protected from the attackers by applying Protection scheme on the Protocols.

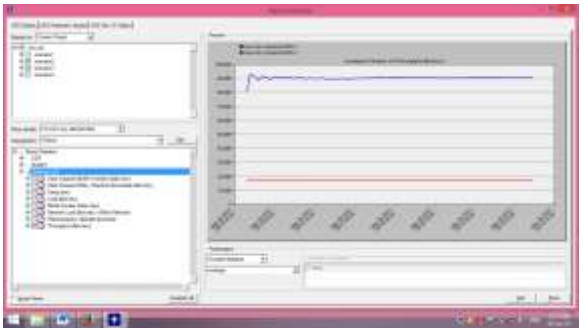

Fig 5 Comparison between throughput bits per sec manet network, Network with Sink hole attack

As it can be seen from fig 6 , a simple network have created with different parameters anfd hiher transmission In Fig 7 it is been shown that how the delay will reduce in improved manet Network..

Fig 6 improved MANET Network

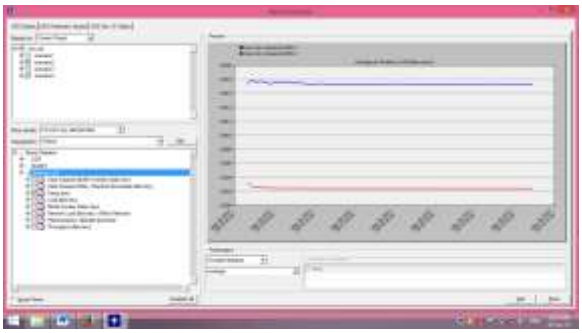

Fig 7 Comparison between Delay manet network, with improved network

The comparison of the results of both the scenarios it has been find out that the total packet dropped increased on applying the black hole attack and Wormhole on the nodes. The difference between both the scenarios is shown in Fig 8. So the data can be protected from the attackers by applying Protection scheme on the Protocols.

VI Conclusion

In this we seen how Sink hole attack degrade the nectork performance by decreasing throughput bits per sec.. In Future Scope There are various Prevention Methods in the DSRto Protect it from the Sink Hole Attack.

REFERENCES

[1] Drs. Baruch Awerbuch and Amitabh Mishran, Dynamic Source Routing (DSR) Protocol, Advanced Topics in wireless Networks, CS: 647.

[2] P. Samundiswary and P.Dananjayan, "Secured Dynamic Source Routing Protocol for Mobile Sensor Networks ", Proc of the 12th International Conference on Networking, VLSI and Signal Processing, 2010

[1]. Abhishek Pandey and R.C. Tripathi. (2010). A Survey on Wireless Sensor Networks Security, International Journal of Computer Applications (0975 – 8887) Volume 3 – No.2.

[2]. Changlong Chen, Min Song, and George Hsieh (2010) Intrusion detection of Sinkhole attack in large scale Wireless Sensor Networks, In Wireless Communications, Networking and Information Security (WCNIS), 2010 IEEE International Conference on (pp.711-716).IEEE[3]. Chen, C., Song, M. and Hsieh, G.

(2010). Intrusion Detection sinkhole attack in large scale wireless sensor network, In Wireless Communication, Networking and Information Security (WCNIS), 2010 IEEE Interational Conference on (pp. 711-716). IEEE. [4]. Choi, G. B., Cho, J. E., Kim,H. J., Hong, S. C. and Kim, H. J. (2008).A sinkhole attack detection mechanism for LQI based mesh routing in WSN. In ICOIN (pp.1-5).

[5] Chun-ming Rong , Skjalg Eggen, Hong-bing Cheng. (2011). A Novel Intrusion Detection Algorithm for Wireless Sensor networks. In Wireless Communication, Vehicular Technology, information Theory and Aerospace

& Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on (pp. 1-7).

[6] Coppolino, L., D'Antonio, S., Romano, L., and Spagnuolo, G.(2010). An intrusion detection system for critical information infrastructures using WSN technologies. In Critical Infrastructure (CRIS), 2010 5th nternational Conference on (pp. 1-8). IEEE

[7] Daniel Dallas, Christopher Leckie, Kotagiri Ramamohanarao. (2007). Hop-Count Monitoring: Detecting Sinkhole Attacks in Wireless Sensor Networks, In Networks, 2007. ICON 2007. 15th IEEE International Conference on (pp. 176-181

.

