Detection and Prevention of Sinkhole attack in Manet

Jeewan Jyoti
M. Tech (CSE), Lovely Professional University, Jalandhar, India

Abstract: *Mobile ad hoc networks are popular networks used broadly due to their dynamic nature. These types of networks are suffered from the sinkhole attack as there is no centralized security management. We will discuss the problems in on-going communication by sinkhole attack in this paper. Sinkhole attack isin MANET is important security problem.A Sinkhole attack is one type of attack in network layer. The data is attracted by sinkhole from the neighboring nodes and then it fake the routing information which make the node which make the local area network know its way on specific node. So, sinkhole tries to attract all the network traffic to itself. Therefore, it alerts the data packet or drops the packet mutely.In this paper we determine one of the most severe routing attacks in adhoc network namely the sinkhole attack.*

I. INTRODUCTION

Mobile Ad hoc Network (MANET) is a temporary network of mobile nodes, interconnected via wireless links without any central administration or fixed infrastructure. Nodes within transmission range of each other can communicate directly. But nodes which are outside the range of each other rely on other nodes to communicate, that is each node in the network has to forward the traffic of other nodes also. So every node works as a host and as a router. In MANET, as nodes are mobile, so network topology is highly dynamic and very unpredictable.

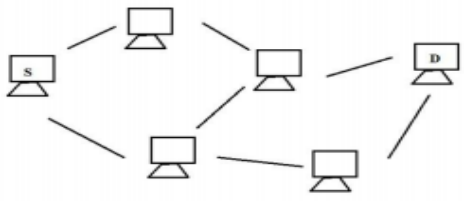

Figure 1.1 MANET

The unique inherent characteristics of the MANETs like open medium, lack of central monitoring, dynamic topology and having nodes with limited battery based energy, make them vulnerable to various attacks. Attackers can easily join the network and then tap information being communicated, change that information or may disrupt the network operation and then without being detected, leave the network. Also almost all routing protocols in MANETs inherently assume that nodes will behave well or are cooperative so even a single malicious or non-cooperating node can disrupt the network functioning. Also nodes in MANET are battery operated. So traffic forwarding for other nodes in the network consumes lot of energy. Thus nodes may show noncooperation to conserve its own energy [3].

The major design approaches used by protocols to security the adverse effects produced due to limits of mobile networks are: the table-driven and the source-initiated on demand approaches.

Table-driven: Reliable routing information between any two nodes connected in the network is conserved using accurate routing tables. Modifications and bring up-to-date are reflected immediately.

Source-initiated on-demand: Source starts this route discovery protocol when it needs a path to the destination. This method detects all possible route opportunities and then sets up a final route.

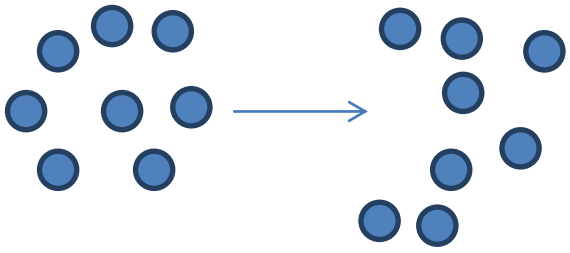

Fig.1.2 Deployments of nodes in MANET

Route maintenance process preserves this recognized route up to the destination turn out to be inaccessible i.e. gets detached from the network or the route is no longer needed. Organization of the paper is listed in the following manner. In section II, an overview of

literature survey is described. In section III, proposed methodology which extends the existing technique is chronicled, followed by the experimental results in section IV and conclusion in section VI.

A. Attacks in MANET

Security involves the identification of possible attacks and susceptibilities or unauthorized access which confrontations the confidentiality, availability, and integrity of any system [8]. Attacks can be gathered into passive and active attacks [10]. A passive attack is very durable to discover as it determines valuable material by snooping on to the routing traffic without disturbing or operating the routing protocol. Malicious nodes trigger an active attack to advance illegal access to the system by introducing fake packets or changing the existing packet transmission. Active attack can further be divided into external attacks and internal attacks. In an external attack the nodes are a portion of external network try to interrupt an internal network. In an internal attack, the cooperated or hijacked nodes and the attacking nodes both fit to the similar network. Further down, some of the common attacks are itemized which affects the routing process adversely.

1. *Black Hole*: In a black hole attack [11] a lethal node places itself among the interactive nodes by presenting a false optimum route to trap the packets in the communication stream.

2. *Replay*: An attacker in replay attack [2] misuses the flexibility feature in MANETs by resending previously recorded packet and producing other nodes in the system to supply stale route in their routing tables.

3. *Blackmail*: In this group of attacks malicious nodes attempt to blacklist permitted nodes by cooking up false information which directs that they are malignant [8].

4. *Link Withholding and Link Spoofing Attacks*: In this category of attacks vital material about links are suspended or false routing data is announced to disturb the network [10].

5. *Sink Hole*: Here a vicious module falsely announces itself as the end to receive the complete network traffic. It then confuses the network by falling these packets after creating important changes which unintentionally affects the network.

6. *Rushing attacks*: Rushing attacks typically causes inadequacy of system resources and disconnects accredited users from the network.

7. *Sybil Attack*: In this type of attacks the lethal nodes create aliases of themselves to gain extravagant influence on the network.

8. *Resource consumption attack*: Here a compromised node efforts to waste the battery volume of the victim by advancing unnecessary packets or by endorsing an extensive long route [10].

9. *Worm Hole*: Attackers keep the packets from reaching the destination node by always tunneling the packets between the malicious nodes.

II. REVIEW OF LITERATURE

Kisung Kim et. aldeveloped the sinkhole detection algorithm using 3 indicators as sequence number duplication. This sinkhole detection algorithm is based all incremental learning proposed to reflect the networking topology changes. It works very well for sequence number below the threshold value. Subsequently a node broad casts alarm message to other node to exclude the sinkhole node in their route.

P. N. Raj et al. defined a simple Detection, Prevention and Reactive AODV (DPRAODV) Scheme which indicate and instructs all the nodes when a Black Hole attack occurs. They single out the deadly nodes from active data promoting and routing operations with the help of a control packet called ALARM limiting their interference. Conversely a vast duration of time now is missed in order to inform or broadcast alarm packets to all nodes in the network. Sometimes owing to their higher sequence number some normal nodes are misclassified and blacklisted illegally. However this technique does not ingest energy for observing the network, it undergoes from the supplement to process and advertise the ALARM packets.

Y.F Alem et al. match audit data collected from the system with the pre-collected set of anomalies to snag any discrepancy thereby confining the node which has elicited it. Due to smaller number of routing packets this technique enables a faster communication and is effective in avoiding assault by other together single and multiple black hole nodes. The only drawback in this approach lies with the faulty data provided by the neighbors presents false alarms which delays the process.

GisungKimet. al, proposed co-operative sinkhole detection algorithm consist of 3 packets named as SAP, SDP & SNP. He proposed a sinkhole indicator which detect the assessment of the RREQ. If a node accepts an RREQ where id of receiving node and source id are equal, it observes the squatness number. If the sequences number of RREQ is larger than the current sequence number of the node then the node know the presence of sinkhole and it recognize this RREQ is from the pseudo node. When the sinkhole indicator is observed, the sinkhole detection procedure is started by distributing a sinkhole detection alarm packet (SAP).

M. S. Sonalet. alproposed that discontinuity in sequence number and advantages of cooperative technique can be approached together.It uses four messages while doing detection. In first one, biggest value will be selected.The biggest value is collection of discontinuity in sequence number.whenever any RREQ receive biggest value, it will calculate by compare with recent RREQ.

D. Sheelaet. al, algorithm based on mobile agent based on routing algorithm to attack against sinkhole attack in WSN. Mobile agent is software program which is controlled by self that visits every node in the network randomly or periodically. By using the gathered information , every node gets alert of while network so that a right or accurate node will not listen to wrong information which can cause sinkhole at tack .

MalihehMagellanet. al briefed about the new algorithm for finding sinkhole attacks . The given algorithm works by discussing the controlled fields of the received data packet with the original control packers, when there is need to send data to BS, it initially send a control packet to main BS. After it reaches BS, it compare control field in the data packet.

III. METHODODLOGY

Sinkhole attack is one of the most important security problems in Manet. The main aim is to detect and isolate the sinkhole node in mobile ad hoc networks and its security is critical challenge because its nature is independent network creation with frequently topology changes. That's why MANET is survival from physical to application layer unsecure. But security is measure issue for the communication so we study number of prevention mechanism and protect thread-hoc network through different attack. In this thesis, our basic objective to protect the ad-hoc network through sinkhole attacks. Sinkhole attack is a type of attack where network traffic is attracted by the comprised nodes by advertising the fake routing update. Other affect of sinkhole attack is that it allows other attacks like selective forwarding attack, drop roying attack. Following is the methodology steps that we follow to implement our proposed technique:

1. Define the deployment area of network.
2. Initializes the number of nodes for sink hole attack in the network
3. Initialize the no of monitoring nodes
4. Define the network parameters like node placement, mobility maintenance and distance vector calculation.

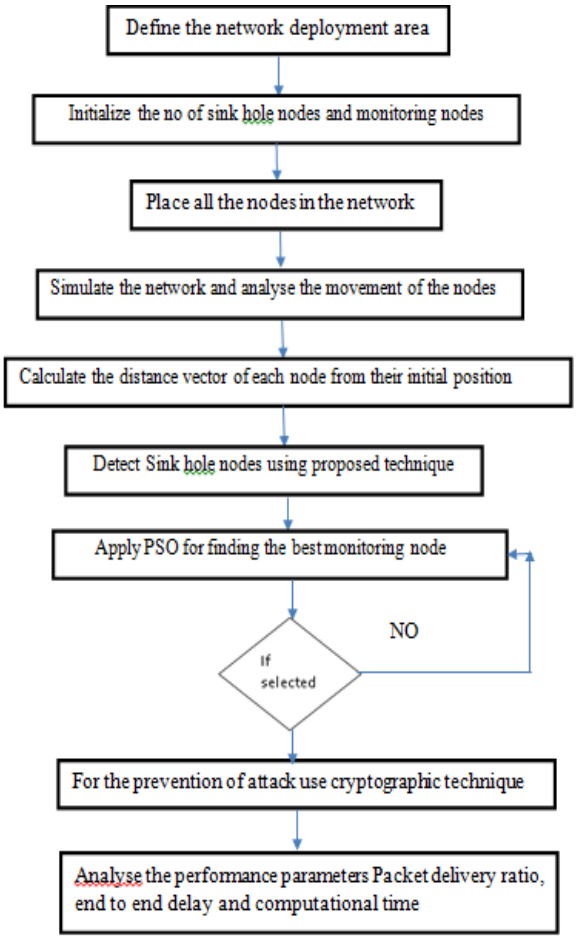

Fig 1.3Proposed Flowcharts

5. To create the area for the deployment of the manet and place the network nodes , monitoring nodes and sink hole nodes and destination node in the network
6. Apply movement to all the nodes from its initial position
7. Calculate the distance vector of all the nodes from their initial position
8. Detect the sink hole nodes using proposed technique.
9. Apply PSO to select the monitoring nodes based on the probability.
10. Provide authentication and integrity to data packets between the source and destination by using cryptographic techniques.
11. Calculating the difference in the parameters like Packet delivery ratio, end to end delay and computational time

IV. RESULT **AND DISCUSSION**

Since Sinkhole attack is one of the dangerous and biggest attacks in wireless ad hoc network. a malicious node is given in sinkhole attack, it gives a wrong routing information so that it can become a specific node and receives traffic of whole network itself. After getting whole network traffic, the secret information is modified, such that the data packet is changed to make it more complicated. A harmful node tries to attract the secure data or information from all neighboring nodes. the performance of ad hoc networks protocols such as AODV, DSR etc is affected by sinkhole. In this process the path presented through the harmful node appears to be the better route for the nodes to communicate. Following is the result screenshots that we predicate

Figure 1.4: Perform Network Simulation with Sink Hole Nodes

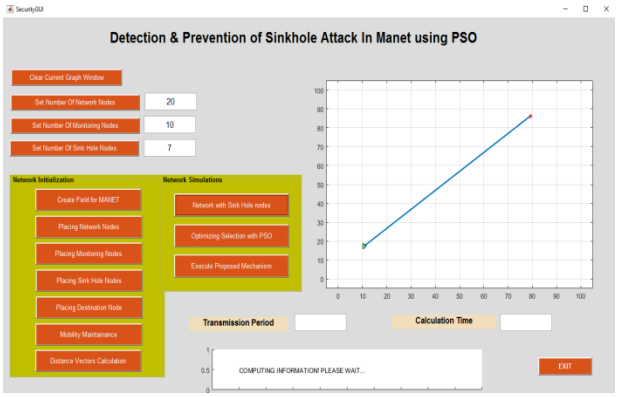

Figure 1.5: Network Simulation with Sink Hole with PSO

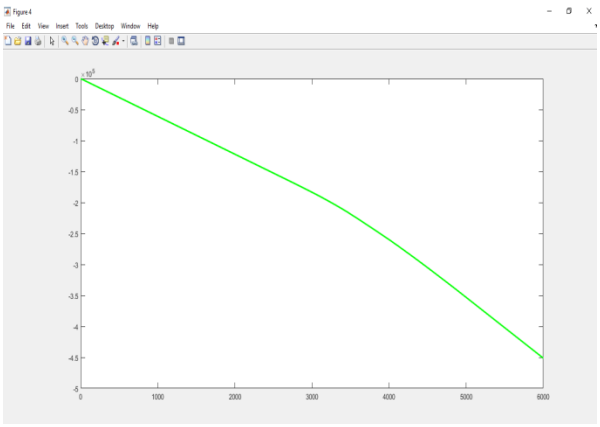

Figure 1.6: Number of Packets to BS, x -label-> number of round

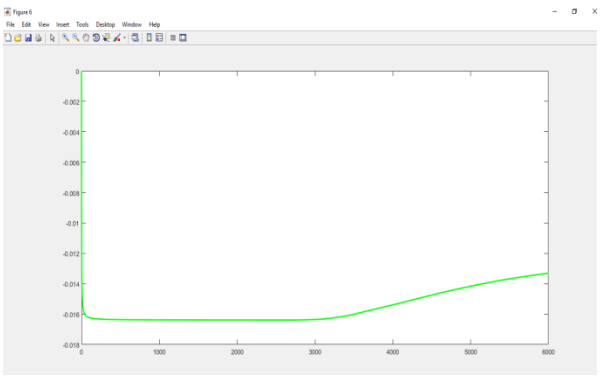

Figure 1.7: Number of Packets to Main = round/number of packet to BS, x -label-> number of round

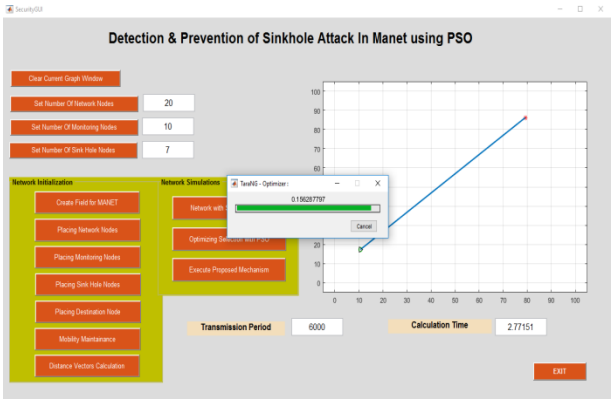

Figure 1.8: Optimization selection using PSO

```
x =

    0.7392    0.5492    0.9756


fvalue =

    0.1505

    0.1505

fx >>
```

Figure 1.9: Fitness Value for Particle Swarm Optimisation

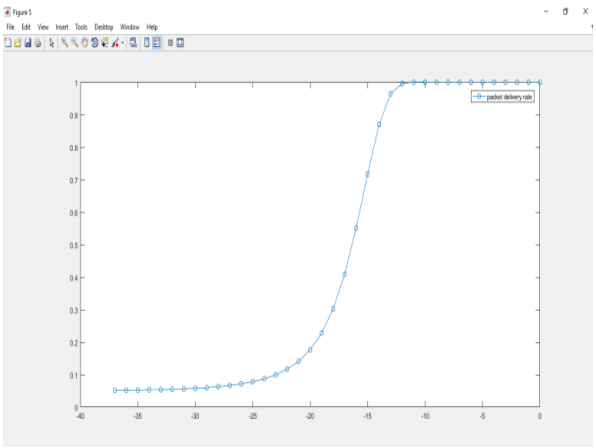

Figure 1.10: Packet Delivery Ratio

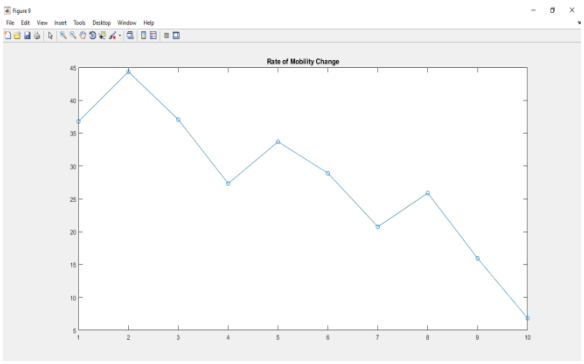

Figure 1.11: Rate of mobility Change

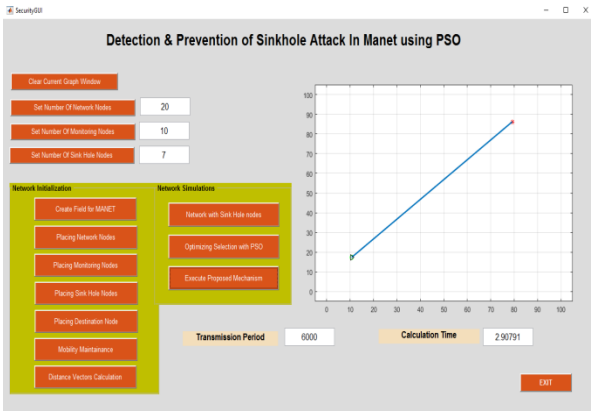

Figure 1.12: Transmission Period and Calculation Time

IV. CONCLUSION

The Mobile Ad hoc Network (MANET) is a dynamic cost-effective network and provides communication with random movement of mobile nodes. The security is the major problem in this kind of decentralized network. The centralized administrator control absence is venerable to network from different attacks. In this research we studythe sinkhole attack, security and normal routing in networks and find its affects.

MANETs are popular networks used broadly due to their dynamic nature. These types of networks are suffered from the sinkhole attack as there is no centralized security management. Here in this paper,we focus on to analyses and report sinkhole attack violation in Manet

REFERENCES

[1] Jeba veer singhjebadurai, Alfred raja melvin A, Immanuel john raja jebadurai, "Sinkhole detection in mobile ad hoc network using mutual understanding among nodes". India. IEEE-2011.

[2] Kisung Kim and Sehun Kim, "A Sinkhole Detection Method based on Incremental Learning in Wireless Ad Hoc Networks"

[3] C. Piro, C. Shields, and B. N. Levine, "Detecting the Sybil attack in mobile ad hoc networks," in Proc. Securecomm Workshops, 2006, pp. 1–11

[4] RoopaliGarg, Himikaharma "Proposed Lightweight Sybil Attack Detection Technique in MANET" International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 3, Issue 5, May 2014

[5] Satyendra Singh, Vinod Kumar Yadav, Ganesh Chandra, & Rahul Kumar Gangwar, " An Efficient and Improving the Security of AODV Routing Protocol" IJCST Vol. 3, Issue 1, Jan. - March 2012.

[6] NidhiJoshi,ProfManojChalla,"Secure Authentication Protocol to Detect Sybil Attacks in MANETs" International Journal of Computer Science & Engineering Technology (IJCSET), ISSN : 2229- 3345 Vol. 5 No. 06 Jun 2014

[7] Sohail Abbas, MadjidMerabti, David Llewellyn Jones, and KashifKifayat," Lightweight Sybil Attack Detection in MANETs", IEEE systems journal, vol. 7, no. 2, June 2013.

[8] Yamini D Malkhede,PurnimaSelokar "ANALYSIS OF SYBIL ATTACK DETECTION IN MOBILE ADHOC NETWORK" Proceedings of 19 th IRF International Conference , 1st February 2015, Pune, India, ISBN: 978-93-84209-85-8.

[9] P.Kavitha, C.Keerthana, V.Niroja, V.Vivekanandhan," Mobile-id Based Sybil Attack detection on the Mobile ADHOC Network", International Journal of Communication and Computer Technologies Volume 02–No.02 Issue: 02 March 2014.

[10] Saurabh, ShekharTandanandPraneet. "A PDRR based detection technique for blackhole attack in MANET.",2011.

[11] Nath, Ira, and DrRituparnaChaki. "BHAPSC: A New SYBIL Attack Prevention System in Clustered MANET." International Journal of Advanced Research in Computer Science and Software Engineering 2012.

[12] Bhosle, Amol, TusharThosar and SnehalMehatre. "Black-hole and wormhole attack in routing protocol AODV in MANET." International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol 2 (2012).

[13] Gagandeep, Aashima, Pawan Kumar, "Study on Sinkhole Attacks in Wireless Ad hoc Networks", International Journal on Computer Science and Engineering (IJCSE), Volume-4, Issue-5, June 2012

[14] Rupinder Singh Brar and HarneetArora," Mobile Agent Security issue in Wireless Sensor Networks ", Issue 1, January 2013(IJARCSSE).

[15] H. Shen and X.-G. Ye, "Research on the location attack based on multiple counterfeit identities tech-nology in sensor networks," in 2014 International Conference on Wireless Communication and Sensor Network (WCSN), pp. 193-197, IEEE, 2014.

[16] L. Tamilselvan and Dr. V.Sankaranarayanan,,"Prevention of Black hole Attacks in MANET", In The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, 2007 IEEE.

[17] M. Zapata and N. Asokan, "Securing Ad-hoc Routing Protocols", In Proc. of ACM Workshop on Wireless Security (WiSe), Atlanta, GA, Sept. 2002.

Jeewan Jyoti was born in Jalandhar on 16th March. She completed her M.C.A and MSc(IT) Degree from Punjab Technical University Jalandhar and M.TECH Degree from Lovely Professional University. She is having 9 years teaching experience. She is currently working as Assistant Professor, Department of Computer Science & IT, G.N.N.C for Women Nakodar, Jalandhar. Her area of interest includes Mobile Networks, Routing protocols design, Security, Wireless Network.