Performance Evaluation of MANET Routing Protocol under Black Hole Attack Using OPNET Simulator

Jaganath. M, Vikram. R

Abstract*: *MANET is self-governing circulated Wi-Fi coordination. Itinerant knobs are permitted to circulating inside & outside the MANET(mobile ad hoc network) network. The knobs having the stuff to organize themselves based on their automatic composition capability. The network environment joining devices or nodes with each other efficiently and create communication that is mobile adhoc network. It has some vulnerability against unity of attacks. One of these attacks is the black hole attack. In this attack, malicious node advertises itself as having freshest or shortest path to specific node to absorb packet to itself. In this paper we be there working to see, how the information is passing with stable manner, and one node to another node via the method of ant colony optimization & Intrusion-tolerant routing protocol for WSNs. We proposed a protected algorithm to preclude the information from black hole attacks in the MANET routing protocols. Finally the simulation analysis and results calculate from the OPNET simulator with the result certain comparisons.

Index Terms*: *MANET, AODV, Black hole attack, ACO, INSENS.

I. INTRODUCTION

A MANET consists of various mobile nodes which is joint by wireless connections. A router to establish a route and each mobile as a host. Each and every mobile node act as a transmitter router or transmitter. MANET routing protocols are ordered into three various kinds of protocols are as subsequent proactive, pre active and Hybrid protocols. Nodes in MANET function both as a host as well as a router for routing data between the nodes in the network. When the source node is sending data and if in this case the destination node is not in the collection of the source node, in such circumstance routing technique is used to ensure that the forwarded packet touches the destination node. The following figure 1 explain about the structure of Mobile ad hoc network. In MANET, the information which is exchanging routing details [11] and also save the data's into the routing tables in correct way and true manner. It is called proactive routing protocols. These MANETs such is used to military application and some emergency resave operations.

Revised Manuscript Received on May 10, 2019

Jaganath. M, PG Student, Computer Science and Engineering, M.Kumarasamy College of Engineering, Karur, Tamilnadu, India.

Vikram. R, Assistant Professor, Computer Science and Engineering, M.Kumarasamy College of Engineering, Karur, Tamilnadu, India.

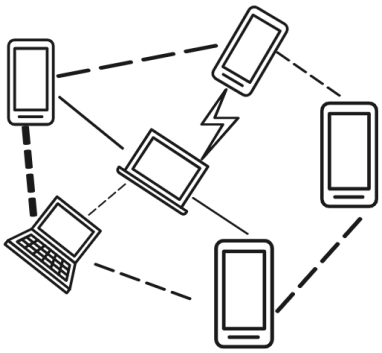

Fig 1. Mobile ad hoc Network

The MANET has blowing applications are as follows.

- ✓ Military services
- ✓ Emergency services
- ✓ Education
- ✓ Gaming
- ✓ Personal area network

II. LITERATURE STUDY

Ayesha Siddiqua et al. [1] proposed a secure knowledge algorithm to avoid the black hole attack in MANETs. In which, every node display other all adjacent nodes, and nodes compare information of its neighbor node with its knowledge table. In knowledge table have information about fm & rm morals of node. If nodes fm value does match with rm value, that node declare as a malicious node by using this algorithm, finds packet drop reason before requesting node as a black hole node.

Haque Nawaz Lashari et al. [2] going to calculate the power attribute from various MANET routing protocols. At the same time, calculating the transmission range and protocols performance observed from AODV, DSR, TORA. In various protocols they are examining the physical characteristics 802.11a or 802.11g by exploiting individual metrics of protocols. Also denoting the the power values decreasing or increasing manner and how it will be affected into that particular MANET routing protocols.

Ayanwuyi T. Kolade et al. [3] analyzed the presence of black hole attack in different scenarios into the AODV MANET routing protocol. They find the routing

protocols using different simulator parameters with and without loads in that working environment. How the black hole attack will destroy the data while send to destination end. Also calculate the packet delivery ratio, end to end delay, and throughput what they are deployed in the present network. Measuring the end to end delay into that destination node with out any packet loss. Able to send the data to other end without any malicious node attack and may be the slight change will happen in that end to end delay.

Mohammad Al-Shurman and Seong-Moo Yoo et al. [4] purposed two systems to detect the black hole attack. First system is based on RREP packet reaches from more than two nodes. This method is sheltered but longer time delay. Second method is based on send RREP with record of Last-packet sequence numbers. Second method is fast, reliable and reduces the overhead in network. But this method is not secure because from time to time malicious node can listen to channel and inform their tables.

H. A. Esmaili et al. [5] purposed a scheme to enquiry the performance of AODV protocol by using OPNET simulator, under black hole attack. In this paper chat two approaches to protected MANET. First is the securing ad-hoc routing by using a number of protocols like DSR (dynamic source routing), DSDV (destination sequence distance vector), ARAN (authenticated routing certificate process), TRP (real time transfer protocol) etc. Second one is, intrusion detection system deliver a mechanism in which each intermediate node sends back the subsequent hop information with RREP massage. By consuming this approaches packet delivery ratio is enlarged but PDR decreases the remarkably in occurrence of black hole attacks.

III. AD-HOC ON DEMAND DISTANCE VECTOR

Ad-Hoc On Demand Distance Vector is hand-me-down to treasure trove a way in the midst of foundation & terminus as desirable & this direction-finding code of behavior practices 3 various momentous kind of memos, path request (RREQ), path reply (RREP) & path error (RERR). Arena evidence of these memos are like foundation classification number, terminus classification number, stage count as well as etc. Every single knob having a direction-finding table that embraces data neighboring way to the meticulous terminus. At what time foundation knob needs to prime addicted to a terminus & present is not a few path flanked by them in its course-plotting table, at major stage foundation knob communications RREQ. As a result, RREQ is established by midway knobs, which be situated in the broadcast variety [10] of despatcher. These knobs transmission RREQ pending RREQ is conventional by terminus or a middle knob which has new sufficient path to the terminus. Which dispatches RREP unicast in the direction of the foundation. From now, a path surrounded by foundation and terminus. A new sufficient path is an effective path admittance. Its terminus classification number is at slightest as excessive as terminus classification number in RREQ. The foundation order number is rummage-sale to control cleanness approximately direction to the foundation. In accumulation, terminus order number is secondhand to describe cleanness of a path to the terminus. Once middle knobs take delivery of RREQ, with thought of basis order number and hop count, mark or inform an inverse path ticket in its direction-finding table for that foundation.

IV. BLACK HOLE ATTACK

Black hole attack is used to obtain straight path to the terminus node and the hateful knob can diverted by using direction finding protocols. It will check the obtainability of the new path to be fortified by antagonistic knob without read-through its path desk. The muggers always having access to responding to the path request by the node which one is requesting. And this process interject the data pack and recall it. The request node have to receive the reply from the malicious knob on or before reception reply from authentication knob by using protocol based flooding. The error or false path is formed when the route is recognized and then the knob [13] can drop all the packs or forward it to indeterminate address. The mentioned second figure explain about Black Hole problem. The knob A is absence to dispatch info pack to knob D & new comer path finding process described in following figure 2[6]. That's why knob E is a fault knob and then which is honor so that it having lively path to the recognized terminus as soon as which obtains RREQ packs. Before that some knobs send the response to knob A. So that knob A clearly known about the lively path of the knobs and the path finding is completed. Knob A would eliminate remaining actions and will starts sending packs to the knob E. by using this method all the info packs are drive or used.

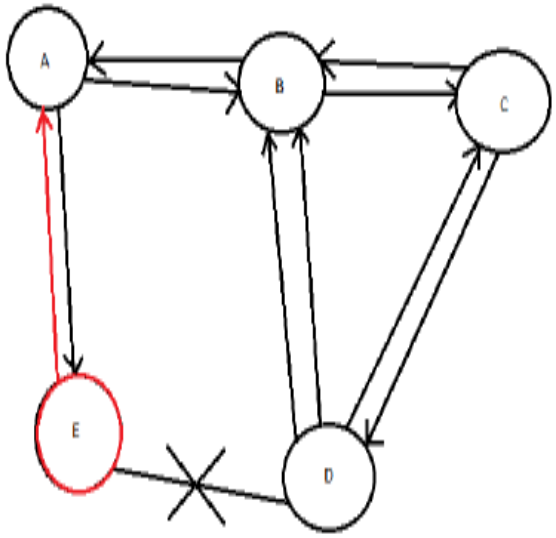

Fig 2. Black hole Problem

V. PROPOSED METHODOLOGY

The research design is divided into following research stages.

• To evaluate the information about mobile ad hoc networks with AODV

protocols.

• Literature study with various types of attacks and algorithms.

• To plan the scenarios of OPNET for calculating the AODV performance under black hole attacks using secure algorithm.

• To utilize the OPNET simulator for emerging the design scenarios.

A. Ant Colony Optimization

In the computer science, computational problems which is solving the from probabilistic technique to find the shortest and good paths. Al so used to reduce the time complexity to reach the information from source [15] to destination end. This is the method called ant colony optimization. This is the method enthused by the multi agent methods and the behavior of real ants. Swarm intelligence methods and constitutes some meta heuristic optimization [8] are the members of the ant colony algorithms. This is the method become new and wrathful method in the research area. In the algorithm, the ants are blind, lump and deft. The main concept of the algorithm, the ants spread their pheromones on the ground that from to a trail. The trail which is used to attracts other ants to follow the original paths. The basic Ant colony system explain in the following structure (figure 3).

Procedure of ACS Algorithm:

Begin

Initialize

While stopping criterion not satisfied **do**

Position each ant in a starting node

Repeat

For each ant **do**

Choose next node by applying the state transition rule

Apply step by step pheromone update

End for

Until every ant has built a solution

Update best solution

Apply offline pheromone update

End While

End

Fig 3. ACO Basic algorithm

B. Intrusion-Tolerant Routing In Wireless Sensor Networks

INSENS algorithm which is used to give the clear way of communication between the sensor nodes and a base stations. It helps to reduce the storage, communication and bandwidth transactions in the sensor nodes. At the same time, to increase bandwidth, communication, storage and computation into the base station end. In the algorithm, to establish the network routing for a hierarchical or asymmetric architecture consisting of a base stations and sensors. The routing protocol and security architecture are little different in the INSENS algorithm. A secret key shares to each nodes with in the base stations, not to the next nodes. Intruder has the contact to one secret key while the node is compromised that neighbors [7] or other nodes throughput from the network. Each node to be programmed with only one secret key to authenticating the bases station to each node. The following three methods are very important to the proposed algorithm as following;

- Route request
- Route Discovery
- Route feedback

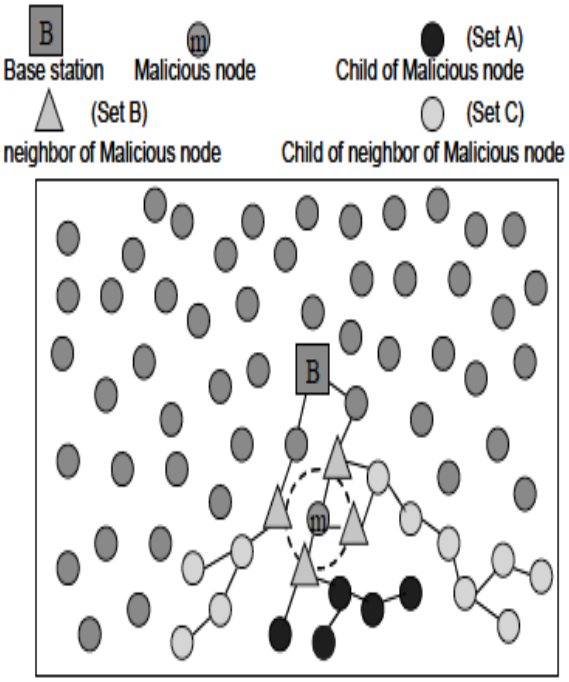

Fig 4. The damage imposed by a malicious node m is confined to a restricted portion of the sensor network, i.e. nodes downstream from m and downstream from m's neighbors.

The above figure 4 explained about to find malicious node and restricted portion in the wireless sensor network. Route discovery to create the forwarding tables to different nodes I various networking topologies. It performs in three types of rounds in the route discovery process. A “request message” send to each base station and all reachable sensor nodes in the present network. A feedback message to the base station which is sensor nodes send their information a routing message which is depends on the feedback message [14] based on the information received from each sensor nodes from base stations.

VI. SIMULATION ENVIRONMENT AND RESULTS

Mobile ad hoc network is rummage-sale for assessing the presentation of AODV direction-finding procedure underneath black hole attacks & this background is a humble MANET is replicated by means of OPNET. Wi-Fi LAN portable computer terminal are secondhand as the moveable customers and the situation total of 25 moveable nodes are recycled. They are

dragged as of the piece palette toward the workstation Request formation is secondhand to set the requests used slantwise the net and in this situation FTP & Web requests are recycled [9]. Application pattern piece is recycled to designate the indispensable requests that products the circulation in excess of the system. The future Table 1 labeled around the limits either used in imitation environs.

Simulation Parameter	Value
Simulator	OPNET Modeler 14.5
Area (m)	1000 * 1000
Network size	25 nodes
Mobility Model	Random way point
Simulation duration	1000(sec)
Source node	Mobile_node-01
Destination node	Mobile_node-25
Addressing mode	IPV4
Traffic mode	FTP
Routing protocol	AODV
Standard	IEEE 802.11 a/b

Table 1. Simulation Parameters

Set mobility profile is used to set the mobility defined across the mobile configuration and as the mobility used is default mobility all the mobile nodes now follow the corresponding mobility patterns in the following figure 5.

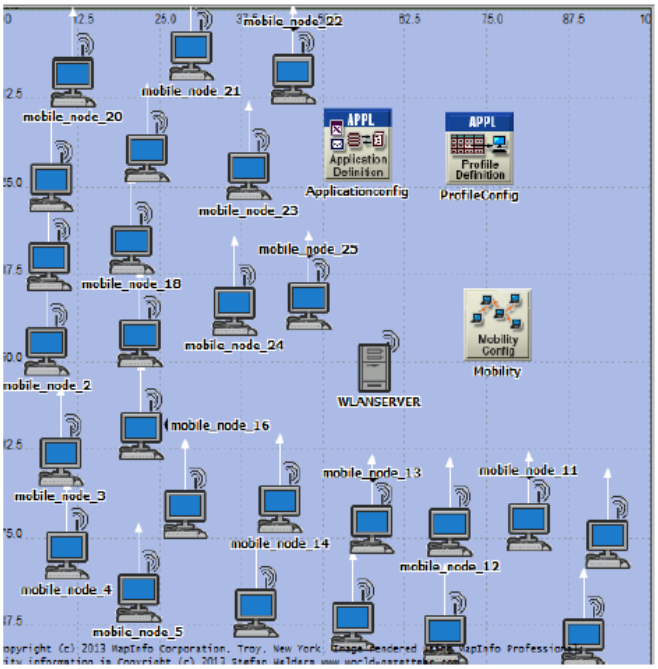

Fig 5. Designed scenario from Mobile Ad hoc Network

In the simulation, we used OPNET 14.5 simulator [12] to find the solutions to send the data from source node to destination node with stable manner. At the same to send the data with secure manner with the help of Intrusion-tolerant routing protocol for wireless Sensor Networks. In the algorithm they are using the technique to protect the information from the malicious attacks. The data is sent along with the one way sequence number and security key to open the content in the destination to the user who uses it is achieved by this secure path. The path dependency is based on the method of Ant colony optimization from the real life of ants to spread their pheromones in the regular paths. It will help to find the proper way to find the food source and get back to home itself. The following graph will show the average efficiency to drive the data to terminus.

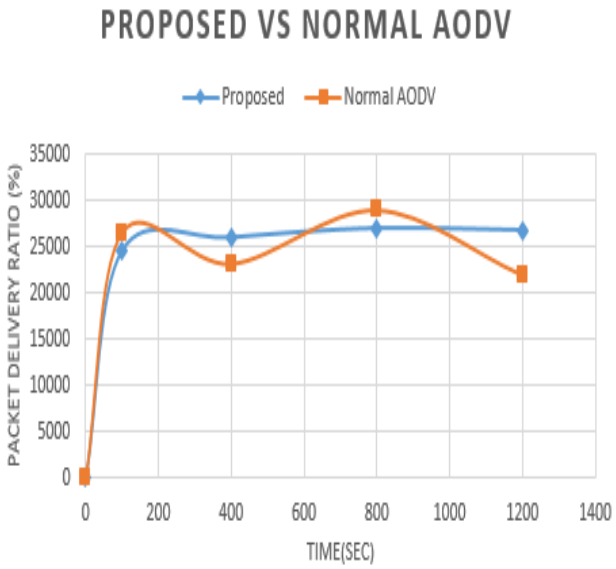

Fig 6. Proposed AODV Vs Normal AODV

Figure 6 explained and compared the normal AODV with the proposed AODV with the help of OPNET simulator.

VII. CONCLUSION

We have proposed an efficient framework which is first of its kind by integrating AODV routing protocol with ACO and INSENS algorithm which as a combination prevents the network from black hole attack. The proposed framework finds the shortest path from source to destination in a secured and stable manner. In order to evaluate the performance of the proposed system with the conventional AODV we have considered packet delivery ratio as parameter. The simulation results show that the modified AODV protocol performs better than the conventional AODV protocol. In the future we may adopt the same protocol to other routing protocols such as OLSR, DSR etc. to make them invulnerable to black hole attack.

REFERENCES

1. Siddiqua, A., Sridevi, K., & Mohammed, A. A. K. (2015, January). Preventing black hole attacks in MANETs using secure knowledge algorithm. In 2015 International Conference on Signal Processing and Communication Engineering Systems (pp. 421-425). IEEE.
2. Nawaz, H., Ali, H. M., & Nabi, G. (2014). Simulation based analysis of reactive protocols metrics in manet using opnet. Sindh University Research Journal-SURJ (Science Series), 46(4).

3. Kolade, A. T., Zuhairi, M. F., Yafi, E., & Zheng, C. L. (2017, January). Performance analysis of black hole attack in MANET. In Proceedings of the 11th International Conference on Ubiquitous Information Management and Communication(p. 1). ACM.
4. Al-Shurman, M., Yoo, S. M., & Park, S. (2004, April). Black hole attack in mobile ad hoc networks. In Proceedings of the 42nd annual Southeast regional conference (pp. 96-97). ACM.
5. Esmaili, H. A., & Shoja, M. R. (2011). Performance analysis of AODV under black hole attack through use of OPNET simulator. arXiv preprint arXiv:1104.4544.
6. Prashant Kumar Varma, Rajesh Upadhyay, Gulshan Katara, Performance Analysis of Black Hole Attack in MANET NETWORK. International Journal of Research and Scientific Innovation, Volume III, Issue III, March 2016.
7. Jing Deng, Richard Han, Shivakant Mishra, INSENS: Intrusion-Tolerant Routing in Wireless Sensor Networks. University of Colorado, Department of Computer Science Technical Report CU-CS-939-02.
8. Abdel-Moniem, A. M., Mohamed, M. H., & Hedar, A. R. (2010, November). An ant colony optimization algorithm for the mobile ad hoc network routing problem based on AODV protocol. In 2010 10th International Conference on Intelligent Systems Design and Applications (pp. 1332-1337). IEEE.
9. Naga Srinivasu S.V, Dr.I.Ramesh Babu, Performance evaluation of AODV under the black hole attacks using the OPNET, International Journal of Computers Electrical and Advanced Communications Engineering Vol.1 (2), 2012.(pp. 204-207).
10. Mahmood K. Ibrahem , Ameer M. Aboud, A Secure Routing Protocol for MANET , International Journal of Computer Science Engineering and Technology(IJCSET) | July 2014 | Vol 4, Issue 7,223-230.
11. B.Padminidevi."Anonymity,Unlinkability,Unobservability for routing protocol in MANETs." International Journal of Emerginf trends in Science and Technology(IJETST), Vol.01, Issue 01,2014.
12. T. T. Manikandan, Rajeev Sukumaran, M. R. Christhuraj, M. Saravanan, "Performance Evaluation of MANET Routing Protocols under Pulse Jammer Attack". International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume-8 Issue-5 March, 2019.
13. Rajaram, A., & Palaniswami, D. S. (2010). Malicious node detection system for mobile ad hoc networks. International Journal of Computer Science and Information Technologies, 1(2), 77-85.
14. Tseng, F. H., Chou, L. D., & Chao, H. C. (2011). A survey of black hole attacks in wireless mobile ad hoc networks. Human-centric Computing and Information Sciences, 1(1), 4.
15. Garg, A., & Juneja, D. (2012). A Comparison and analysis of various extended techniques of query optimization. International Journal of Advancement in Technology, 3.