ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

A Novel Technique to Detect and Prevent Black Hole Attack in MANET

Sharndeep Kaur[1], Dr. Anuj Gupta[2]

Research Scholar, RIMT-IET, Mandi Gobindgarh , Punjab, India.[1]

HOD, Department of Computer Science, RIMT- IET, Mandi Gobindgarh , Punjab, India.[2]

ABSTRACT: MANET is a collection of various mobile nodes which communicates over relatively bandwidth through the wireless links. In MANETs, the nodes are mobile in nature hence the network topology may change rapidly and unpredictably over time.With the increase in the use of MANETS security became an indispensable requirement to provide communicational protection and improvement of network recital. The most possible attack in MANET is black hole attack. In which, a malicious node provides fake routing information by advertising itself having shortest path to the source node and then deprive the traffic from the source node or can drop the packets later. Here in this paper a novel approach is proposed to detect and prevent black hole attack in MANET. For this a meta heuristic search schema introduced by integrating the min and max variants of ACO with DRPI verification tables based on AODV routing protocol. Finally the NS2 simulation shows that this technique detect and isolate the malicious node as well as reduces the packet loss rate while increasing the data forwarding capacity of nodes.

KEY WORDS: AODV, MANET, Black hole attack, Network, Max-Min ant colony optimization.

I. INTRODUCTION

1.Mobile ad-hoc Network: Mobile ad hoc network is a collection of mobile nodes. It is a type of infrastructure less network. [2] In the infrastructure less network, no centralized access point is required. The access point contains the base stations.

Types of MANET:

- **Vehicular Ad Hoc Networks** : VANETs are used for communication among vehicles and between vehicles and roadside equipment.
- **Intelligent vehicular ad hoc networks**: In-VANETs are a kind of artificial intelligence that helps vehicles to behave in intelligent manners.
- **Internet Based Mobile Ad-hoc Networks**: i-MANET are ad-hoc networks that link mobile nodes and fixed Internet-gateway nodes.[2]

MANET is vulnerable to various kinds of attacks. These attacks are classified into two categories.
Attacks on mobile ad hoc networks can be classified into following two categories:

- Passive Attacks
- Active Attacks

Passive Attack: in case of passive attacks, confidentiality breaks. As the attacker snoops the data exchanged in network without altering it.Snooping is a unauthorized access to other person data. In this case, attacker only watch the data and it does not modifies it, hence it become very difficult to find the paasive attacks.
Active Attacks: in case of active attacks, data integrity is break. As the attacker modified the data and sends to the user.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

2.Black Hole Attack:

Black hole attack is one of the denial-of-service attack in ad-hoc networks. As we know RREQ, RREP, RRER are three types of packets that are used for route fining. In case when black hole node present in network when source node broadcast RREQ packets for route to destination, the black hole node fake reply with RREP packets. It shows that its having shortest path to destination but in actual its replying with fake RREP packets. After getting all replies from all possible paths when source node do hope count then it will found that the black hole node is having shortest path and it will selects this path to send data. But the black hole did not forward packets it will receive packets and drop them.

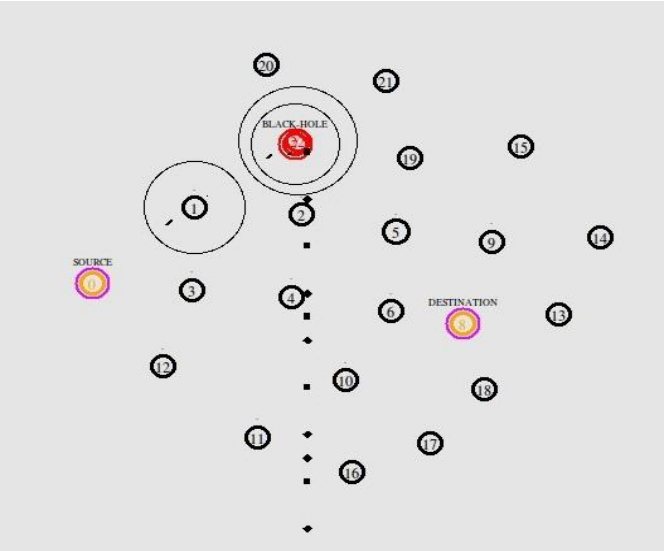

Fig 1: Black hole attack

The black hole has the two properties. First, the node exploits the ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination node. Second, the node consumes the intercepted packets.
Fig 1 shows the black hole attack on 23mobile nodes wireless network in which red circled node is a malicious node consuming the packets from source node 0 and further droped them.

3.Ant Colony Optimization and MMAS:

Ant Colony Optimization is a probalistic and meta-heuristic technique. It is also natural insipid technique which is meta-heuristic in nature and used to solve complex combinatorial problems. It uses the previous results to find out the present optimal paths. It is dynamic in nature.[3] It gives the idea for team coordination, their behavior and functionality. It is also based upon swarm intelligence. Ant starts from nest to reach to destination and follow different paths. Each ant secretes pheromone trails to attract other ants following that path. The path which has the highest pheromone trails are the optimal paths compared to others. So the path is depending upon the trails. ACO is basically the optimization approach that speeds up the algorithmic procedure. In a wireless network the ACO is use to optimize the communication process and also used in the nodes to find the optimal path over the network. Ant places the pheromones on the located path so that all the other nodes can follow these pheromones to communicate on this optimized path.

Max- Min ant system also called as MMAS is also a type of Ant Colony system with a difference that there is no stagnation in the result because there are some precise limits for pheromone trail updates in this. The limits are min to max bound value and that have to be respected by ants as updating their pheromone values. Also the pheromone values for each node are initialized to the maximum bound value and they keep decreasing as the pheromones evaporate. Because of this, the optimal path is established earlier and accurately. The probability for an ant to select one out of two nodes depends on the pheromone trail bound values which we store in DRPI tabels in our technique .

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

Applications of ACO
1. To solve job scheduling problem.
2. To solve many assignment problem.
3. To solve knapsack problem.
4. Fuzzy system is used in it.
5. It can be used in many routing and security problems.

II. LITERATURE SURVEY

A trust based approach for AODV protocol to mitigate black hole attack in MANET, (2012): in this paper, author discuss about the mobile ad-hoc networks. The black hole attack can disrupt the communication between the various nodes in AODV for MANET. In the AODV the malicious activities are not monitored. AODV is most widely used protocol for MANET.[4] In case of AODV all mobile nodes work in cooperation to find a route path from source to destination. Actual data transmission takes place only after the route is established. AODV uses the three control messages. These messages are RREP, RREQ and RERR. RREP stands for route reply packets, RREQ stands for route request packets, whereas, RERR stands for route error reply. In this paper, author presents a trust based collaborative approach to mitigate black hole nodes in AODV protocol for MANET. Here each node monitors the neighboring node and calculates the trust value of the neighboring node. if the trust value of a monitored node goes below a predefined threshold, then the monitoring node assume it as malicious and avoids that node from the route path.

Historical Evidence Based Trust Management Strategy against Black Hole Attacks in MANET, (2012): in this paper, author discuss about the MANET. As MANET can be classifies into three categories: proactive, reactive and hybrid. The destination sequence distance vector is comes under the category of proactive protocol and ad-hoc on demand vector protocol comes under the reactive protocol. The reactive protocols initiate a route discovery process.[5] The route discovery phase, contains the two types of black hole attacks: single attack and cooperative attack. In this paper, author proposed a method, which is focus on the black hole attack in the RREQ phase and the behavior of malicious nodes. Distributed, self-organized and infrastructure independent nature of MANET makes it vulnerable to various kinds of attacks. Trust management scheme is a common way to detect and isolate the compromised nodes while a cryptography mechanism shows a failure facing to inner attacks.

The Black-hole node attack in MANET,(2012): in this paper author discuss about the black hole attack in Mobile ad-hoc network. The attack in MANET contains the two purposes. It does not forward the packet or change the parameters of routing messages and to exhaust the battery of nodes by make them traversing the wrong packet in wrong direction. The black hole problem is one of the security attacks that occur in mobile ad hoc networks. [6] A black hole attack increases network overhead, decreases the network's lifetime by boosting energy consumption, and finally destroys the network. This makes this type of attack more dangerous as it does not check what kind of data just dropping the packets is meant for other nodes .That data may be critical. So this type of attack must be detected as early as possible and removed from network. Here author present two possible solutions. The first is to find more than one route to the destination. The second is to exploit the packet sequence number included in any packet header.

Detection of Malicious Attack in MANET A Behavioral Approach,(2012): in this paper, author discuss about the detection of malicious attack in MANET. Mobile ad hoc network is a set of mobile devices. These devices can communicate with each other without any centralized supervision. Hosts in wireless network travel without the constraints of wired connections.[7] The mobile ad-hoc network is dynamic in nature and it is unreliable. Multi-hop peer-to-peer routing is used by MANET as an alternative of fixed network infrastructure to provide network connectivity. In the MANET, two types of attacks are common, as black hole attack and grey hole attack. in this paper, author purposed a novel automatic security mechanism using SVM to defense against malicious attack occurring in AODV. Proposed method uses machine learning to categorize nodes as malicious.

An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET,(2012): in this paper, author discuss the black hole problem that occur in AODV protocol in MANET. Mobile ad-hoc network (MANET)

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

consists of wireless mobile nodes that are capable of communicating with each other without any centralized access point. In MANET, each node is free to join, leave, and move independently. As a result, the network topology changes rapidly and unpredictably, and connectivity among the terminal vary with the time. MANETs are more vulnerable to attacks. These attacks are generally classified as active attacks and passive attacks. Black hole attack is the most common attack that occurs in the MANET.[8] In this attack, a malicious node falsely advertise shortest path to the destination node with an intension to disrupt the communication. In this paper, author propose a solution to the black hole attack in one of the most prominent routing algorithm, ad-hoc on demand distance vector routing, for the MANETs.

Stutzle and Holger H. presented their paper on Max- Min ant system where they have explained the features of Min-Max Ant system also called as MMAS. They have shown how MMAS different from Ant System in numerous important aspects which they have demonstrated by means of an experimental study. In addition , they have related one of the characteristics specific to MMAS that of using a greedier search than Ant System to result from the search space analysis of the combinatorial optimization problems attacked in this paper. They have discussed that this MMAS is in any way better than the conservative ACO algorithms we use because of the limit they provide for the pheromone values in the same [9].

III. PROPOSED SCHEMA

This proposed technique introduced a novel method against malicious attack in MANETs. For this we used max- min variants of ACO which is also called max min ant system , its integration with DRPI verification tables ,based on AODV protocol. It will make the improvement to security issues as well as route discovery and maintenance stage . In this technique multiple paths are established between source node and destination node using idea of Max Min Ant System and the isolation of malicious nodes are based on the DRPI table's (dynamic route pheromone bound value information table) values of THROUGH and FROM which promiscuously updated as the ant agents travels from source to destination and vice versa. As seek road in the Ant colony algorithm , our improved secure mechanism introduce two kinds of ant as F-ANT and B-ANT .

F-ANT travel from source to destination . It carries the route request information to establish the source node overturn pheromone pathway. B-ANT is the ant agent which has a route from destination to back to source .

The function of F-ANT and B-ANT is same as the RREQ and RREP in AODV .

1. Pheromone Update Strategy : According to the idea of max min ant system pheromone updation is implemented as follows:

$$T_{ij} \leftarrow [\,(1-\beta)\,.\,T_{ij} + \Delta T_{ij}^{best}\,]_{T\,max}^{T\,min} \quad \text{to} \quad \text{.....(1)}$$

Where T max and T min are the pheromone upper and lower bound value and ΔT_{ij}^{best} is :

$$\Delta T_{ij}^{best} = 1/L_{best}$$ if (i,j) belongs to the best tour else, it will be 0. ……(2)

Where as L_{best} is the total no. of hops from source to the destination in communication link.

2.Path Selection and .DRPI verification table update strategy : While the FANT passed through the intermediate nodes as depositing there pheromone Tmax ,promiscuously the value of THROUGH in the DRPI table will be updated by threshold value 1. As in Backward process when BANT travels from destination node to source node and again deposit their pheromone value Tmax , the value of FROM in verification table updated by threshold value 1 and if there is malicious node then the THROUGH and FROM value in DRPI verification table will be 0 because no traffic will pass through that node it will immediately send the fake BANT packet to the source node but doesnot update the DRPI table . So in our scenario before communication, source node broadcast activation message to all nodes and requests them to show there DRPI tables . After that will choose the path in which all nodes are having FROM and THROUGH values 1, 1. The nodes are having value 0 will be isolated for communication and the path which is chosen on the bases on this scenario with highest pheromone bound value and least hop counts will be the safe path for communication. The

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

sample scenario is shown in Fig. 2 where node which have both FROM and THRO value 1 is selected and other rejected.

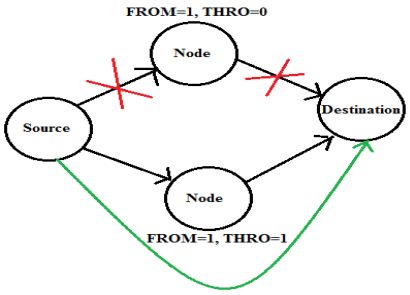

Fig 2: DRPI based path selection

IV. RESULTS AND DISCUSSIONS

The simulation is done by using network simulator (NS-2.34). Here the attack and purposed schema is implemented by taking 23 wireless nodes and the results are plotted in terms of throughput and delay measurement. Throughput can be defied as the number of results produced per unit time whereas end-to-end delay may be defined as the time taken between sending of a packet and it's receiving on the destination The comparison between both scenarios is shown in graphs. To perform simulation following parameters to be taken shown in Table1:

Network	Wireless
Antenna	Omni directional
BasedRouting Protocol	AODV
Queue	Drop tail (50)
Number of Nodes	23

Table 1: Simulation parameters

1. **Delay:** Here the delay between both scenarios is shown. In this graph red line shows delay curve for old scenario and green line show delay curve for purposed scenario. In old case because of black hole attack it drops packets in between path and destination is disabling to receive any packet so the delay curve is rising with packet loss but in new case because of prevention of black hole attack destination node can properly receive packets, so here it is less delay. In Fig. 3 the delay starts increasing when there is presence of a black hole node in the network whereas in absence of black hole nodes, the delay is almost zero as all packets arrive at their destination in a timely manner.

   Here, X-axis = Simulation Time
   Y-axis = delay in time

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

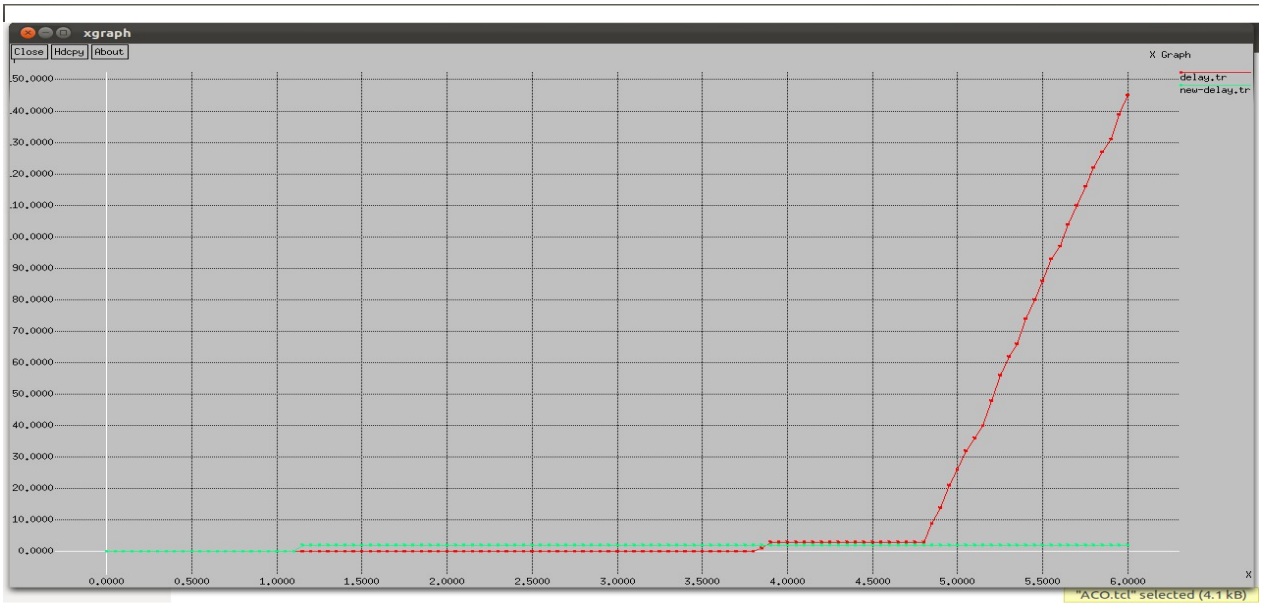

Fig 3: Delay Graph

2.Throughput: In this graph throughput comparison between both scenarios is shown. Here in figure 4 red curve shows throughput for old case and green curve shows throughput for new case. Because of packet loss in old case throughput is very low and because of prevention of attack in new case throughput is high. As the delay in the network is at a minimum due to isolation of black hole nodes, the throughput increases as more and more packets are delivered to their destinations.

Here , X-axis = Simulation Time
Y-axis = Number of packets received at destination

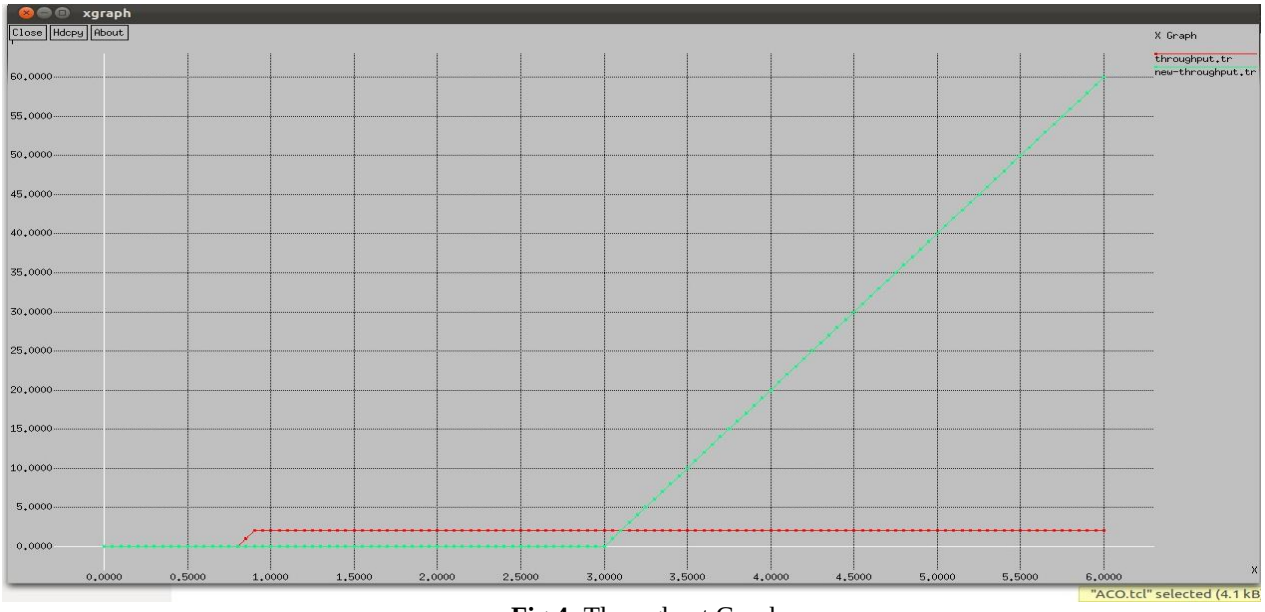

Fig 4: Throughput Graph

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

V. CONCLUSION

In this paper we used a very simple and very effectual way of providing security against blackhole attack by introducing some modification to Ant Colony Max Min Ant System. This algorithm is proficient in providing an optimal path because operations to be performed in each node are very simple ,thus it is robust and fault tolerant. It is investigated that the proposed method shows positive results as opposed to the other different security method using. The proposed method shows better Throughput as well as less delay.By integrating DRPI threshold vale factor to ACO the black hole attack not only detected , but also prevented. A lot of work has to be done in order to make the usage of mobile ad-hoc networks common a viable option. . Mobile ad-hoc networks will continue to evolve and new target applications will probably emerge. So there is need of research to provide more security from other threats also.
Future work: The protocol is not so perfect because of limit time. So this part of work will also be the next part of study.

REFERENCES

[1] http://computernetworkingnotes.com/wireless-networking-on-cisco-router/types-of-wireless-networks.html
[2] http://mobileeadhocnetwork.blogspot.in/2012/02/types-of-manet.html
[3] Marco Dorigo, Thomas Stutzle, The Ant Colony Optimization Metaheuristic: Algorithms, Applications, and Advances.
[4] Fidel Thachil, K C Shet, A trust based approach for AODV protocol to mitigate black hole attack in MANET, , 978-0-7695-4817-3/12 $26.00 © 2012 IEEE DOI 10.1109/ICCS.2012.7
[5] Bo YANG, Ryo YAMAMOTO, Yoshiaki TANAKA, Historical Evidence Based Trust Management Strategy against Black Hole Attacks in MANET, ISBN 978-89-5519-163-9 Feb. 19"-'22, 2012 ICACT2012
[6] Ms.Nidhi Sha rma Mr.Alok Sharma ,The Black-hole node attack in MANET , 2012 Second International Conference on Advanced Computing & Communication Technologies
[7] Meenakshi Patel, Sanjay Sharma, Detection of Malicious Attack in MANET A Behavioral Approach, , 978-1-4673-4529-3/12/$31.00 c_2012 IEEE
[8] Pramod Kumar Singh, Govind Sharma , An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET, 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications.
[9] G.Shen And X.Huang (Eds.); CSIE 2011,part 11, CCIS 153,pp 34-41,2011© Springer-Verlag Heidelbing 2011.