International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-4 Issue-2, July 2014

Improvement of Network Efficiency by Preventing Black Hole Attack in Manet

Gurnam Singh, Gursewak Singh

Abstract: ***Black hole is a malicious node that always gives the false replay for any route request without having specified route to the destination and drops all the received packets. This can be easily employed by exploiting vulnerability of on demand routing protocol AODV. Within mobile Ad hoc networks black hole attack is a harsh threat which is able to prevent by broadcasting the malicious node id to the entire nodes in the network. The obtainable method recognized the attacked node, retransmit the packets and once more find a new way as of source to destination. Here the proposed method to prevent black hole attack with reduced energy consumption of the network this results in improving lifetime by minimizing the packet loss and improved throughput of the network.***
Keywords: Ad-hoc, AODV, Black hole.

I. INTRODUCTION

A mobile ad-hoc network (MANET) is a collection of wireless mobile nodes which have the ability to communicate with each other without having fixed network infrastructure or any central base station. It is one of the recent active fields and has received spectacular consideration for the reason that of their self-configuration and self-maintenance. Early research assumed a friendly and cooperative environment of wireless network. As a result they paying attention on problems such as wireless channel access and multihop routing.
Since mobile nodes are not controlled by any other controlling entity, they have unrestricted mobility and connectivity to others. Routing and network management are done cooperatively by each other nodes. Due to limited transmission power, multi hop architecture is needed for one node to communicate with another through network[2]. In this multi hop architecture, each node works as a host and as well as a router that forwards packets for other nodes that may not be within a direct communication range. Each node participates in an ad-hoc route discovery protocol which finds out multi hop routes through the mobile network between any two nodes. These infrastructure-less mobile nodes in ad hoc networks dynamically create routes among themselves to form own wireless network on the fly [7, 8].

II. SECURITY ISSUES IN MANETs

Security is more challenging to preserve in MANETs due to their vulnerability, than wired networks.

Manuscript published on 30 July 2014.
***Correspondence Author(s)
Gurnam Singh, M.Tech in CSE (Networking System) from Punjab Institute of Technology, Kapurthala, India.
Gursewak Singh, M.Tech Degree in Computer Science and Engineering from Lovely Professional University, India.

The utilization of wireless links creates an ad-hoc network vulnerable toward link attacks range as of passive eavesdropping to active impersonation, message replay and distortion. The MANET vulnerabilities contain:

a) **Dynamic network topology**: Mobile nodes link and disappear the network randomly, approaching about to change the network topology dynamically. This permits a malicious node to link the network without preceding detection.

b) **The limited physical protection of each of the nodes:** A network nodes typically do not be a resident of in physically protected spaces, for instance locked rooms. Therefore, they know how to move without difficulty and fall under the control of an attacker.

c) **The vulnerability of the links:** messages are capable to eavesdrop and fake messages are capable to be injected keen on the network missing the complexity of have physical access to the network components. Eavesdropping might give an attacker access to secret information thus defy confidentiality [3].

d) **Adversary inside the Network:** The mobile nodes within the MANET can freely join and leave the network. The nodes within network may also behave maliciously [9]. This is hard to detect that the behaviour of the node is malicious. Thus this attack is more dangerous than the external attack. These nodes are called compromised nodes.

The security goals for ad hoc networks include confidentiality, availability, integrity, non-impersonation, authentication, non-repudiation and non-fabrication.

III. CLASSIFICATION OF ATTACKS

The attacks could be classified on the groundwork of the origin of the attacks i.e. Internal or External, and resting on the performance of the attack i.e. Passive or Active attack. This classification is imperative as the attacker be able to use the network either as internal, external as well as active or passive attack against the network.

a) **Internal/External Attack:** External attackers are fundamentally exterior the networks who desire to obtain access to the network and just the once they obtain access to the network they begin sending fake packets, denial of service inside order to interrupt the performance of the entire network. The nature of the attack is similar to the wired network attacks [11]. This is called an internal attack because here node itself belongs to the network internally. Internal attack is more severe to attack because here malicious node present inside the network actively.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

b) Active/ Passive Attack: In active attack, the performance of the network is made upset and critical information is taken and the information is destroyed throughout the replacement in the network. Active attacks are able to be internal or external attack. active attacks are intended to obliterate the performance of system in such case the active attack take action as internal node in the network. In passive attacks, the normal operations of the network are not disrupted. The attacker listens to network in order to get information about the current transmissions. It snoops to the network in order to recognize and be aware of how the nodes are exchange information through each other, and how they are positioned in the network [4].

c) Denial of Service attack: This attack aims to attack the availability of a node or the entire network. If the attack is successful the services will not be available. The attacker generally uses radio signal jamming and the battery exhaustion method.

d) Eavesdropping: This is a passive attack. The node simply observes the confidential information. This information can be later used by the malicious node. The secret information like location, public key, private key, password etc. can be fetched by eavesdropper.

e) Routing Attacks: The malicious node makes routing services a target in light of the fact that it is a critical service in MANETs [10]. There are two flavours to this routing attack. One is attack on routing protocol and another is attack on packet forwarding or delivery mechanism. The leading is pointed at obstructing the propagation of routing information to a node. The latter is aimed at disturbing the packet delivery against a predefined path.

f) Wormhole Attack: In a wormhole attack, an attacker receives packets at one point in the network, tunnels them to another point in the network, as well as it replays them keen on the network from that point. Routing can be disrupted when routing control message are tunnelled. This tunnel between two colluding attacks is known as a wormhole.

g) Gray-hole attack: This attack is also known as routing misbehaviour attack which leads to dropping of messages. Gray-hole attacks have two phases. In the primary phase the node advertise itself as having a valid route to destination while in second phase, nodes drops intercepted packets with a certain probability.

h) Black Hole Attack: Black hole is a malicious node that always gives the false replay for any route request without having specified route to the destination and drops all the received packets. This can be easily employed by exploiting vulnerability of on demand routing protocol AODV [12].

The malicious node for all time sends RREP immediately it receives RREQ lacking performing standard AODV operations, as keeping the Destination Sequence number extremely high. Since AODV consider RREP have high value of destination sequence number to be fresh, the RREP sent through the malicious node is treating fresh. Therefore, malicious nodes be successful in inject Black Hole attacks [5].

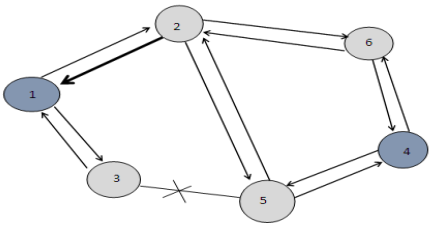

Fig. 1 Black Hole Attack

Types of Black Hole Attacks

A Black Hole attack is a type of denial of service attack wherever a malicious node be able to be a focus for all packets by incorrectly claiming a new route to the destination and after that attract them without forwarding them in the direction of the destination.

Single Black Hole Attack

In single black hole attack only one malicious node attack on the route. The core functionality of WMNs is the routing capability and attackers take advantage of the shortcomings as the routing protocol has some loop holes. The AODV protocol is vulnerable to the well-known black hole attack. AODV uses sequence numbers to determine the freshness of routing information and to guarantee loop-free routes [13]. In case of multiple routes, a node selects the route with the highest sequence number. If multiple routes have the same sequence number, then the node chooses the route with the shortest hop count.

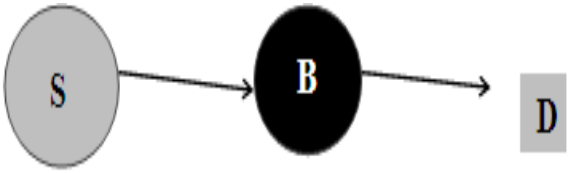

Fig. 2 Single Black Hole Attack

- **Co-operative Black Hole Attack:** In the Co-operative Black Hole attack the malicious nodes have an effect in a group. The nodes 2 and 3 act as black holes. A more complex form of the attack is a Co-operative Black Hole Attack where multiple malicious nodes collude together resulting in complete disruption of the routing and packet forwarding functionality of the network [6].

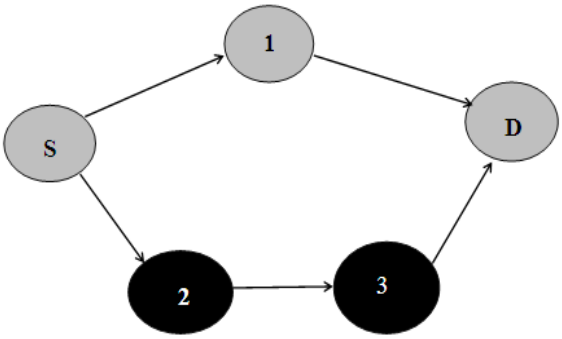

Fig. 3 Co- Operative Black Hole Attack

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

IV. PROTOCOL IMPLEMENTATION

The security problems are all related to malicious nodes that intentionally damage or compromise network functionality. However, selfish nodes, which use the network but do not cooperate to routing or packet forwarding for others in order not to spill battery life or network bandwidth, constitute an important problem as network functioning entirely relies on the cooperation between nodes and their contribution to basic network functions. To deal with these problems, the self-organizing network concept must be based on an incentive for users to collaborate, thereby avoiding selfish behavior.

ALGORITHM STEPS:

Broadcast route request packet in a network.
Do until destination is found.
Destination reply via shortest path using AODV protocol
Source specifies particular nodes of path from Source to destination
Start communication
While sender of the packet is in the path
If sender is not in the path
Then
Receiving node informs all the nodes in the path with malicious node and receiving node discards the path
End
Start normal communication
End

V. PERFORMANCE METRICS

THROUGHPUT: Throughput is defined as the amount of data bytes received at the destination in the given time interval. It is one of the important parameter when it comes to measuring the performance of the network. More the throughput, better the performance of the network. In this achieved a maximum throughput of 180Kbps.

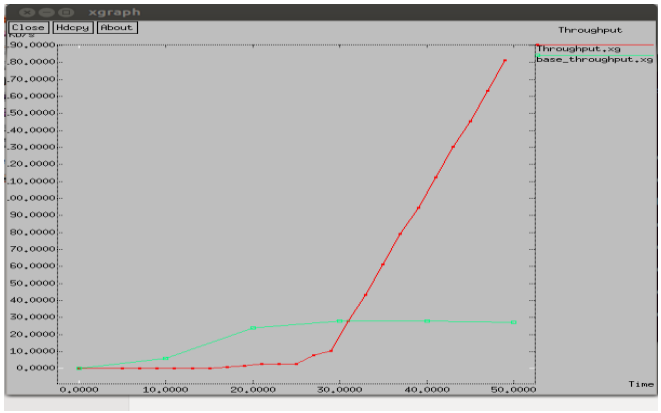

Fig. 4 Throughput Comparison

VI. SIMULATION PARAMETERS AND RESULTS

The variety of parameters which are measured for network simulation is specified in the table1.

Table 1. Simulation Parameters

Parameter	Value
Simulator	NS-2
Version	NS 2.34
Number of Nodes	50
channel	Wireless channel
Traffic Type	CBR
Routing Protocol	AODV
MAC Type	802.11 MAC Layer
Packet Size	512 bytes
Antenna Type	Omni directional

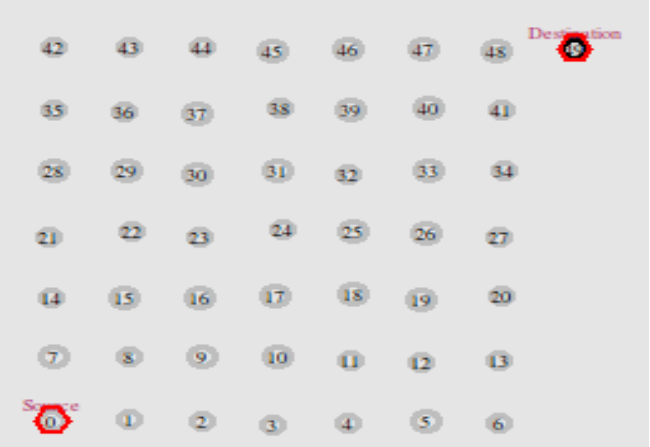

Fig. 5 Finding Shortest Path Nodes from Source to Destination Using AODV in NAM

This figure 5 shows the shortest path which is finding by using the ADOV algorithm in the network. Due to the algorithm the source and destination are finding and apply the prevention method of black hole attack on source and destination shown in figure 6.

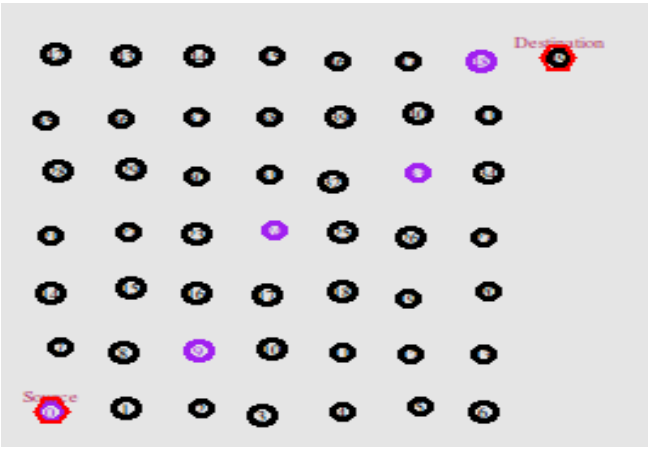

Fig. 6 Prevention of Cooperative Black Hole Node Attack

ENERGY: The graph shows the average energy consumed in the network. Initially 100 joules of energy was assigned to nodes deployed in the network.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

After running the simulation for 50 sec, energy remaining was found to be 60 joules. In the past work malicious node id broadcasting method is used. During broadcasting a lot of energy is consumed. In this paper the new mechanism is used which ID checking mechanism at the one path thick nodes is so avoiding the broadcasting method saves energy. This eventually increases the network lifetime.

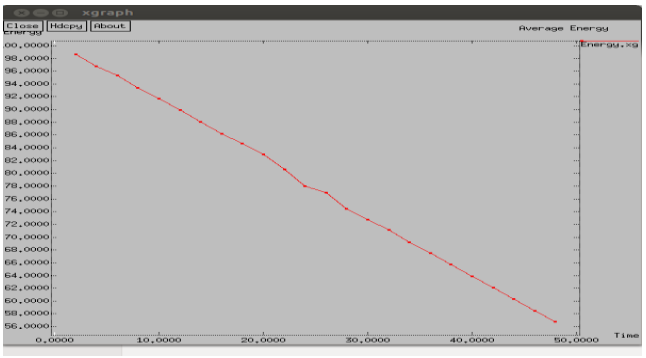

Fig. 7 Overall Energy Scenario

PACKET DELIVERY RATIO: PDR is defined as number of packets received at the destination to the total number of packets that were sent by the source. Malicious node id broadcasting method achieved a maximum value of 0.95; our method achieved a maximum value of 1.This means that all the packets that were sent from source were successfully delivered at the destination.

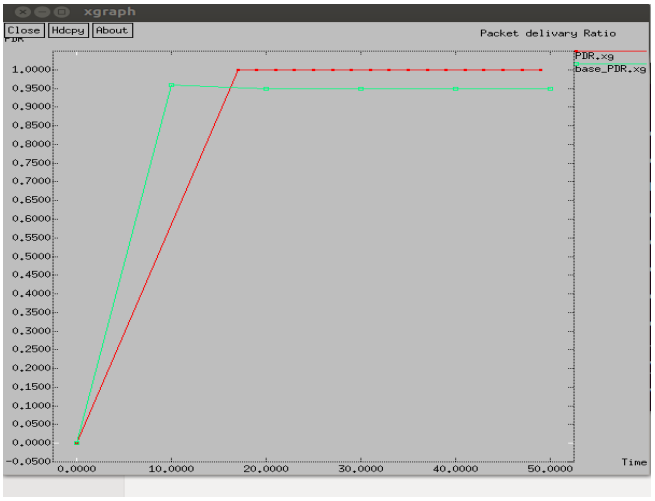

Fig. 8 Packet Delivery Comparison

PACKET DROP: This graph shows how many packets are lost during its journey from source to destination. In our study, it was found that no packet was lost. In past where average number of packets dropped varies between 1.9 to 0.4 but this paper is found to show better results. This is because during the broadcasting of malicious node id, some packets tend to get lost due to collision at the receiver side.

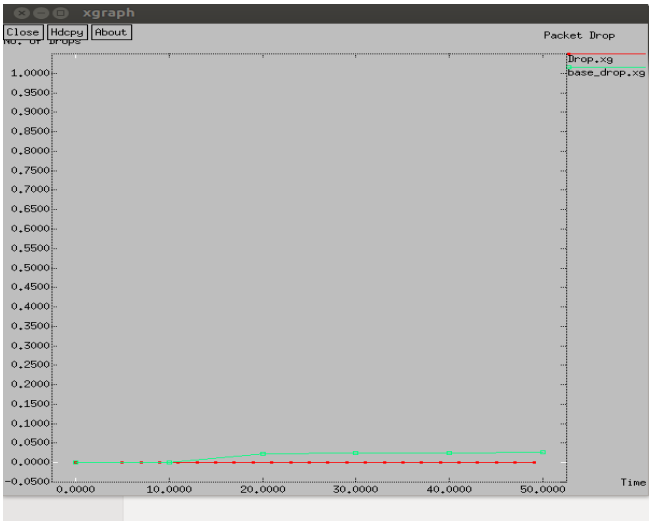

Fig. 9 Packet Drop Comparison

VII. CONCLUSION

In this paper, we considered the difficulty of supportive black hole attacks in MANET routing. Our Approach provides better performance of throughput packet delivery ratio and condensed packet loss comparing with older methods like H.Fu method and malicious node broadcasting method (MN-ID). For that reason our approach gives better network performance and lowest amount packet loss in the packet transmission.

REFERENCES

1. Tayal, S., & Gupta, V. (2013). "A Survey of Attacks on Manet Routing Protocols."*International Journal of Innovative Research in Science, Engineering and Technology*, *2*(6), 2280-2285.
2. Muthukumaran, K., Jeyakumar, D., &Omkumar, C. U. A "Concise Evaluation of Issues and Challenges in MANET Security".
3. Jain, S., &Hemrajani, N. (2013). "Detection and mitigation techniques of black hole attack in MANET: An Overview." *International Journal of Science and Research (IJSR), India Online ISSN*, 2319-7064.
4. Kaur, A., & Singh, A. "A Review on Security Attacks in Mobile Ad-hoc Networks".
5. Dangore, M. Y., &Sambare, S. S. (2013). "A Survey on Detection of Blackhole Attack Using AODV Protocol in MANET". *International Journal on Recent and Innovation Trends in Computing and Communication*, *1*(1), 55-61.
6. Jain, S. "Review of Prevention and Detection Methods of Black Hole Attack in AODV-based on Mobile Ad Hoc Network".
7. Sowmya, K. S., Rakesh, T., &Deepthi, P. H. (2012)." Detection and Prevention of Blackhole Attack in MANET Using ACO". *International Journal of Computer Science and Network Security*, *12*(5), 21-24.
8. Tripathi, R., &Tripathi, S. (2001). "PREVENTIVE ASPECT OF BLACK HOLE ATTACK IN MOBILE AD HOC NETWORK".
9. Devassy, A., &Jayanthi, K." Prevention of Black Hole Attack in Mobile Ad-hoc Networks using MN-ID Broadcasting".
10. John, N. P., & Thomas, A. (2012)." Prevention and Detection of Black Hole Attack in AODV Based Mobile Ad-hoc Networks-A Review". *International Journal of Innovative Research and Development*, *1*(6), 232-245.
11. Patel, B., & Trivedi, K." A Review-Prevention and Detection of Black Hole Attack in AODV based on MANET".

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

12. Hongmei Deng, Wei Li, and Dharma P. Agarwal, (2002) "Routing Security in Wireless Ad Hoc Networks", University of Cincinnati, IEEE Communications magazine, Vol.40, No.10
13. Charles E. Perkins, and Elizabeth M. Royer, "Ad-hoc On-Demand Distance Vector (AODV) routing," InternetDraft, November 2002.

AUTHOR PROFILE

Gurnam Singh, received the B.Tech (honours) Degree in Computer Science Engineering from Lovely Professional University and M.Tech in CSE (Networking System) from Punjab Institute of Technology, Kapurthala. His research area is wireless sensor network, network security protocols design and Mobile and Ad-hoc Network.

Gursewak Singh, received the B.Tech Degree in Computer Science Engineering from Punjab Technical University, India, in 2011. He has done his M.Tech Degree in Computer Science and Engineering from Lovely Professional University, India, in 2013. His research interest includes RFID (Radio Frequency Identification), Security Analysis of RFID System and Cryptography Algorithms for RFID, Security Schemes in Wireless Sensor Networks and Mobile Ad-hoc Network.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)