International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 06 | June-2016 www.irjet.net p-ISSN: 2395-0072

# Black Hole Attack Detection And Prevention In Wireless Networks

**Monika[1]**
[1]*M.Tech Student, Department of Computer Science & Applications, Kurukshetra University, Kurukshetra, Haryana*

---

**Abstract:** *A wireless network is a network that is made up of nodes that are self-configured without having the need for fixed infrastructure. However, the open source nature of this medium leaves it vulnerable to multiple security threats. The nodes are vulnerable to various kinds of attacks due to their mobility and resource constrained nature. One such attack is Black-Hole attack. In this attack a compromised node advertises itself to have a shortest path for sending data packets to destination. This way the malicious node deceived other nodes and obtains sensitive information. Therefore the data packets are dropped by the malicious nodes and does not reach the destination node. This results in data loss. This paper is focused on detection and prevention of the black-hole attacks in wireless networks.*

***Keywords:*** MANET ,RREP, RREQ, AODV, ONE, DTN

## 1. INTRODUCTION

Wireless Networks are gaining its popularity due to its ease of deployment, more economic and so on. These networks do not have any constraints of wired networks. Wireless network can be categorized into infrastructure wireless network and infrastructure less wireless network [1]. MANET (Mobile Ad-hoc Network) is an infrastructure less network where mobile nodes can move freely and can form network. Wireless networks rely on uninterrupted availability of the wireless medium to interconnect participating nodes. However the open nature of this medium leaves it vulnerable to multiple security threats. That means most of the time does not guarantee about the packets can be easily transfer over the network. It affects network performance degrade.

Due to the absence of trusted centralized authority or openness of network topology, wireless networks are susceptible to security threats. Black-Hole attack is one of the route disruption attacks that cause a greater damage to the network. In this attack, a malicious node advertises itself as having freshest or shortest path to specific node to absorb packets to it .

The goal of the proposed solution is the detection and avoidance of black-hole attack by using cryptography mechanism and prevent network from black-hole attack.

**BLACK HOLE ATTACK**

A Black-Hole attack is one of active DoS (Denial-of-Service) attack possible in mobile ad-hoc networks. Basically it is route disruption attack . This attack occurs during route discovery phase. In this attack a malicious node believe that it is having shortest path and traps packets thereby degrading network performance. When a malicious node starts trapping the packets black hole comes into picture. Black hole is also called packet drop attack as it keeps on drops the packets in Ad Hoc Networks [2].

When a source node desire to communicate with other node in a network, it initiates route discovery mechanism by broadcasting RREQ (Route Request) message to its neighboring nodes. Malicious node being a part of network sends back RREP (Route Reply) soon after receiving RREQ there by misleading source that it is having the shortest path and fresh enough route. The source node responds to RREP sent by malicious node discarding RREP from other nodes as it reaches quickly. Then source node starts packet transmission to that malicious node. In this way black hole attack comes into picture.

In black hole attack hop count value is set to lowest value and the sequence number is set to the highest value. Malicious node send RREP to the nearest available node which belongs to the active route or it can also be sent directly to the source node if there is a route. The RREP received by the nearest available node to the malicious node will relayed via the established inverse route to the data of source node [3]. The malicious node will drop all the data to which it belong in the route. Therefore packets will not be forwarded to destination. Black Hole is shown below.

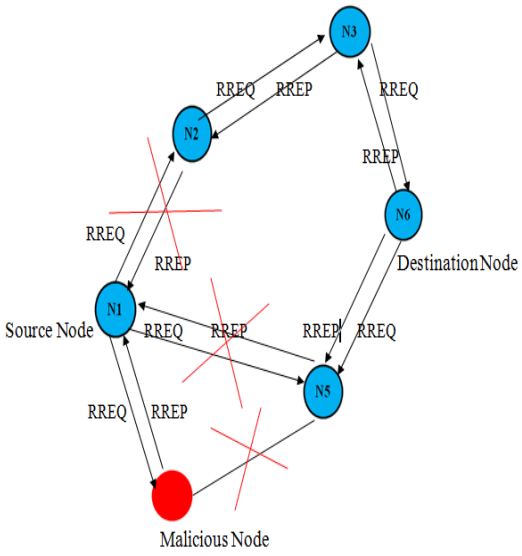


**Figure 1: Black Hole Attack**

In the above Figure N1 is source node and N6 is the destination node.N4 node is made malicious. It clearly explains Black-Hole attack.

## 2. RELATED WORK

This section introduces the related work of black-hole attack in wireless networks by various authors with different perceptions. In the literature, the black-hole attack solutions can be solutions which are interested in the black-hole attack acting in an individual manner or those which are interested in the cooperative black-hole attack on general security mechanisms. Therefore in order to carry out the present research work an intensive literature survey was reviewed are the findings are listed below:-

Payal N. Raj, Prashant B. Swadas (2009) proposed "DPRAODV: A dynamic learning system against black hole attack in AODV based MANET" (detection, prevention and reactive AODV) to prevent security of black hole by informing other nodes in the network. It uses normal AODV in which a node receives the Route reply (RREP) packet which first checks the value of sequence number in its routing table. The threshold value was the average of the difference of destination sequence number in each time slot between the sequence number in the routing table and the RREP packet. The node that was detected as the anomaly was black listed and ALARM packet was sent. The main advantage of this protocol was that the source node announces the black hole to its neighbors in order to be ignored and eliminated. Their solution increases the average end-to-end delay and normalized routing overhead [4].

Deng et al (2002) stated a solution using one more route to the intermediate node that replays the RREQ message to check whether the route from the intermediate node to the destination node existed or not. In the proposed method, each intermediate node was required to send back the nexthop information when it sends back an RREP message. When source node received the reply message, it did not send the data packets right away, but sends a Further-Request to the nexthop to verify that it had a route to the intermediate node who sends back the reply message, and that it has a route to the destination node. To avoid the problem of recursiveness, only the requested nexthop can send back a Further-Reply message, which included the check result. If the path existed data packets were transferred else an alarm message was sent across the network to isolate the node from the network [5].

Marti et. al. (2000) described the misbehavior detection using the watchdog and the pathrater. The watchdog identified misbehaving nodes by listening promiscuously to the next node transmission whereas the pathrater used the knowledge from the watchdog to choose a path that was most likely to deliver packets. This technique was imperfect due to limited transmit power, collision and partial dropping [6].

## 3. PROPOSED METHODOLOGY

The major aim of the proposed methodology is to purpose a new algorithm based on cryptography mechanism to detect and prevent network from black-hole attack. The routing scheme used in the proposed solution is the "Probability Based Routing Scheme". In this probability-based scheme the sender forwards the node having the highest priority of successful message delivery.

**Proposed Algorithm for Detection and Prevention of Black-Hole Attack**

**Algorithm 1**

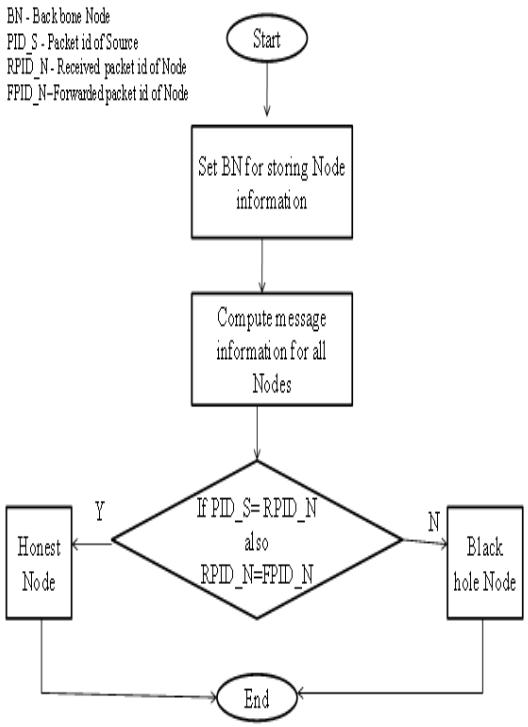


**Figure 1: Algorithm Depicting the Detection of Black-Hole attack**

In proposed work, firstly the number of nodes in the network are initialized. Each node has its own buffer memory. A buffer is a temporary memory in which a message is stored during data transmission. Next a message period i.e. TTL (Time-To-Leave) is set. Thus TTL is the time taken to deliver a message from message creation by source to the message delivery to the destination node. If the value is expired then message is aborted. Now, a backbone node is initialized for storing node routing information and after storing routing information it checks each node by checking their delivered message information.

If PID_S=R PID_N

also

R PID_N=F PID_N

If packet ID is same forwarded by node to destination then node status is "Honest" node, otherwise node status is Black Hole node.

**Algorithm 2**

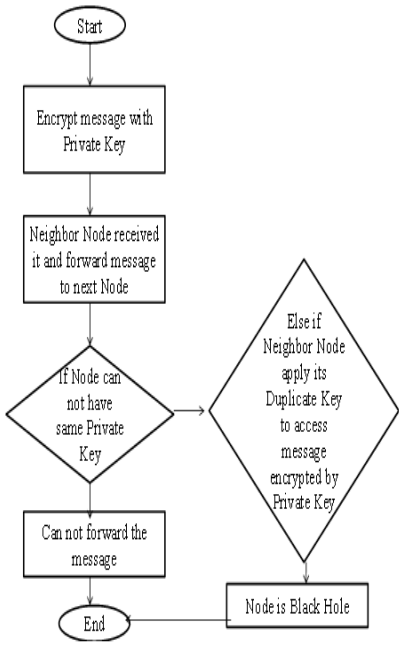


**Figure 2: Algorithm Depicting the Prevention of Black-hole Attack**

The Algorithm 2 of the proposed solution describes the prevention of the Black-Hole attack in Wireless Networks. After detecting the black-hole node, the process of prevention is being carried out. Firstly, initialized the number of in the network. Now in order to maintain privacy a cryptography mechanism is applied i.e. encrypting/decrypting the message with private key. In cryptography, a private key is an encryption/decryption key known only to the part or parties that exchange secret messages.

A private key is tiny bit of code that is paired with a public key to set of algorithms for text encryption and decryption. It is created as part of public key cryptography during asymmetric-key encryption and is also used to decrypt and transforms a message to a readable format.

Now the neighboring that received the information and forwards message to the next node. If the next node doesn't have the same Private key then it can not forward

the message further to the next neighboring node and hence terminated. Else if the neighboring node or the malicious node apply its duplicate key to access message which was encrypted by private key and thus is not able to detect. Hence the malicious node is Black-Hole.

## 4. SIMULATION And RESULTS

In this section, simulation environment and simulation results are described and reported respectively.. Simulation is basically the limitation of the operation of a real-world process or system over time. Simulation is used in many contexts, such as simulation of technology for performance optimization safety engineering, testing, training and education. Often computer experiments are used to study simulation models. By changing variables in simulation, predictions may be made about the behavior of the system. It is a tool to virtually investigate the behavior of the system under study. Computer simulation is done using the network simulator ONE (Opportunistic Network Environment). The ONE Simulator is a wireless simulator that has been designed specially for Delay Tolerance Network (DTN). It has experienced growth in its researchers mainly because of its simplicity and easy customization. Here red line shows the simulation results of the proposed solution and blue line shows the routing black hole.

Firstly we investigated the packet delivery ratio at various number of nodes. Initially at node 30 delivery ratio is measured and lastly at node 75, number of packets delivered are 176 through the proposed solution and 153 through the routing black hole which clearly shows that the delivery ratio of the proposed algorithm is increased as compared to the routing black hole .

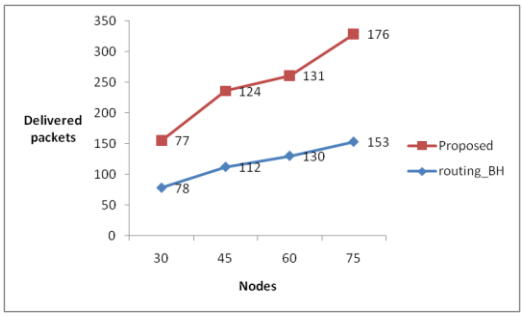


Figure 1: Delivery Ratio

Now the second graph shows the number of packets dropped and the results clearly shows that the packet drop rate is less through proposed algorithm as compared to the routing black hole.

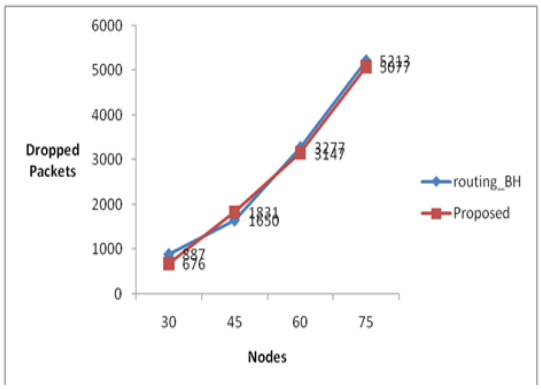


**Figure 2: Packet Drop Rate**

The third graph of simulation results shows the message delay through proposed algorithm and routing black hole

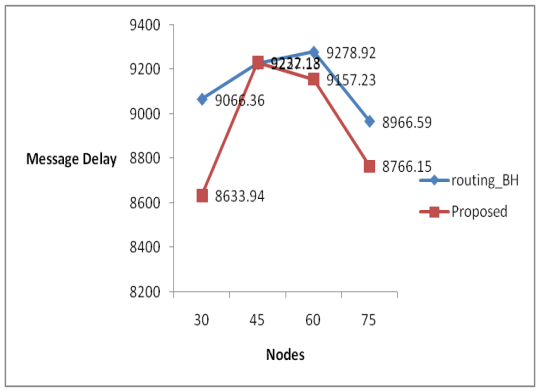


**Figure 3: Message Delay**

The last graph shows the Overhead ratio of the simulation results. The graph clearly depicts that the overhead ratio is resulted low as compared to the routing black hole with proposed algorithm.

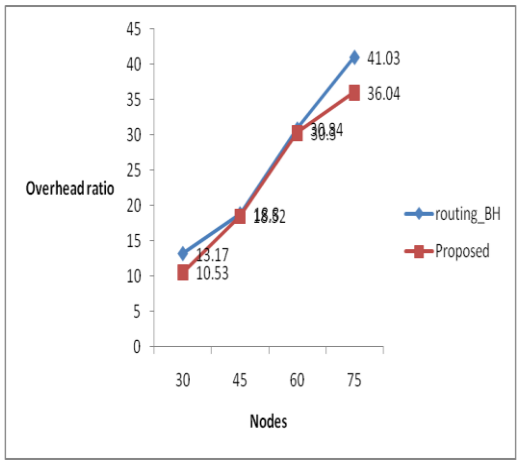


**Figure 4: Overhead Ratio**

## 5.CONCLUSION

In this paper focus is on detection and prevention of Black Hole attack in Wireless Networks. Black Hole attack is one of the most important security attack in Wireless Networks. It is an attack that a malicious node impersonates a destination node by sending forged RREP to a source node that initiates route discovery, and consequently deprives data traffic from the source node. In the proposed methodology, algorithms for detection and prevention of black hole for wireless networks are designed.

Simulation showed that various metrics namely delivery ratio, packet drop rate, message delay and overhead ratio resulted better as compared to the routing black hole with the proposed algorithms. Future work in this direction is in progress.

## REFRENCES

[1] Rashmi Mishra Mohit Kumar, ""An Overview of MANET: History, Challenges and Applications"," *Indian Journal of Computer Science and Engineering (IJCSE)*, vol. 3, Feb-Mar 2012.

[2] Narendra S chaudhar Rakesh kumar Sahu, ""Performance Evaluation of ad hoc network under black hole attack," *IEEE*, 2012.

[3] Rajkumar Singh, "Ad-hoc On-Demand Distance Vector Protocol and Black Hole Attack in AODV" , April 10, 2012.

[4] Payal N. Raj and Prashant B. Swadas, "DPRAODV: A dynamic learning system against black hole attack in AODV based Manet," *International Journal of Computer Science Issues (IJCSI)*, vol. 2, no. 3, pp. 54-59, 2009.

[5] H., Li, W., Agrawal, D.P Deng, Routing Security in Wireless Ad Hoc Networks, 2002.

[6] T. Giuli, K. Lai, and M. Baker S. Marti, ""Mitigating routing misbehavior in mobile adhoc networks"," in *Proceedings of the ACM Conf. on MobileComputing and Networking (Mobicom)*, 2000, pp. 255-265.