Proceedings of 8th IOE Graduate Conference
Peer Reviewed
ISSN: 2350-8914 (Online), 2350-8906 (Print)
Year: 2020 Month: June Volume: 8

Detection and Prevention from Blackhole attack in MANET

Sujan Shrestha [a], Surendra Shrestha [b]

[a, b] *Department of Electronics and Computer Engineering, Pulchowk Campus, IOE, TU, Nepal*
Corresponding Email: [a] shrestha.sujan1400@gmail.com, [b] surendra@ioe.edu.np

Abstract
A Mobile Ad-hoc Network (MANET) is an infrastructure-less network where nodes can move randomly without help of any fixed infrastructure. There is no centralized administrator, dynamic topology and wireless connections so it is powerless against various types of assaults. MANET has more threat contrast to any other conventional networks. AODV (Ad-hoc On-demand Distance Vector) is the most utilized well-known routing protocol in MANET. AODV protocol is vulnerable to “Black Hole” attack. A blackhole node replies for each path requests even if it doesn’t have active path to targeted destination and drops all the packets that received from sending node. If blackhole nodes are present in the network, then the targeted receiver won’t be able to receive the packet. In this paper, a new concept for detection and prevention of black hole attack is presented with the help of transmitting fake RREQ packet that has non-existing destination which results blackhole node to response while normal nodes just bypass it by broadcasting for neighbor nodes.

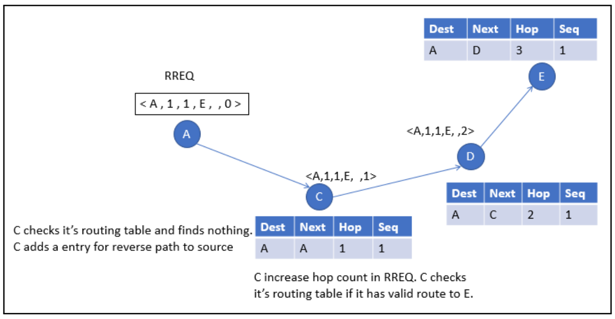
Keywords
mobile ad-hoc network; AODV routing protocol; black hole attack; detection and prevention

1. Introduction

Wireless networks use some sort of radio frequencies in air to transmit and receive data instead of using some physical cables. Wireless networks are formed by routers and hosts. Ad-hoc networks are wireless networks where nodes communicate with each other using multi-hop links. Networks that support mobile wireless ad hoc architecture are typically called mobile ad hoc networks (MANET). A mobile ad hoc network is formed by mobile hosts. There is no stationary infrastructure or base station for communication. So the functioning of Ad-hoc networks is dependent on the trust and co-operation between nodes. Nodes help each other in conveying information about the topology of the network and share the responsibility of managing the network. As each mobile node acts as a host when requesting/providing information from/to other nodes in the network, and acts as router when discovering and maintaining routes for other nodes in the network [1]. There are three main routing protocols proposed for MANET: Ad hoc On-demand Distance Vector (AODV) routing, Dynamic Source Routing (DSDV), and Destination Sequence Distance Vector routing protocols [2]. AODV and DSR belong to on-demand routing protocols and DSDV is a table-driven routing protocol. These protocols are vulnerable to different security attacks. In this paper, we use AODV routing protocol because the AODV protocol is vulnerable to the blackhole attack in network. MANET inherits security threats that are faced in wired as well as wireless networks and also introduces security attacks unique to itself due its characteristics [3]. Based on the routing information update mechanism, routing protocols in ad hoc wireless networks can be classified into three broad categories: Proactive (or table-driven) protocols, Reactive (or on-demand) protocols, and Hybrid routing protocols. Protocols are vulnerable to routing attacks. Routing attacks in ad hoc wireless networks can also be classified into five broad categories: Attacks using Impersonation, Modification, Fabrication, Replay, and Denial of Service (DoS). In this paper, we focus on blackhole attack that belongs to category of fabrication attacks. We introduce a new blackhole resisting mechanism that can be used for all on-demand routing protocols. Each node in this mechanism is responsible for monitoring the behaviour of its neighbors to detect malicious nodes and exclude them. We incorporate our proposed mechanism into AODV as an example of its use with on-demand routing protocols. This paper demonstrates a significant improvement in performance when using our mechanism. The rest of the paper is organized as follows. In Section 2, AODV protocol and its behavior is described. Section 3 presents AODV under blackhole attack. Section 4 presents the methodology of detection and prevention in MANET. In Section 5, our simulation approach and parameters is presented. In Section 6, results and analysis are given. In Section 7, conclusions are drawn.

2. AODV Routing Protocol

AODV is the most efficient routing protocols for MANET. It offers several benefits as compared to others such as dynamic, supports multi-hop directing, circle free and automatically detects inactive routes. Instead of all these features it is defenseless against many attacks. MANET routing protocols can be classified as proactive or reactive routing protocols. In proactive (table-driven) routing protocols, each node maintains one or more tables containing routing information to every other node in the network. While in reactive (on-demand) routing protocols, routes are created whenever a source requires to send data to a destination node which means that these protocols are initiated by a source on-demand. We focus on the AODV protocol [4] which is one of the extensively studied reactive protocols, considered by the IETF for standardization. Ad-Hoc On-Demand Distance Vector (AODV) is a reactive routing protocol in which the network generates routes at the start of communication. Ad Hoc On-Demand Distance Vector (AODV) routing protocol described in builds on the DSDV algorithm. AODV is an improvement on DSDV because it typically minimizes the number of required broadcasts by creating routes on a demand basis, as opposed to maintaining a complete list of routes as in the DSDV algorithm [5]. AODV routing protocol works on phases. Source node will initiate a route discovery phase and this phase consist of route request and route reply (RREP) messages.



Dest	Next	Hop	Seq
A	D	3	1

Dest	Next	Hop	Seq
A	C	2	1

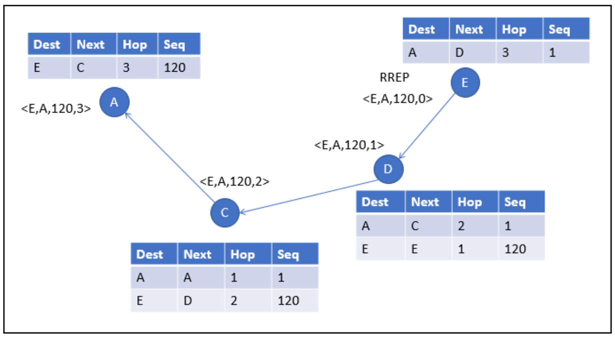
C checks it's routing table and finds nothing.
C adds a entry for reverse path to source

Dest	Next	Hop	Seq
A	A	1	1

C increase hop count in RREQ. C checks it's routing table if it has valid route to E.

Figure 1: Routing Table updation due to RREQ

The explanation of how AODV works is shown in Figure 1.The first phase of route discovery consist of RREQ forwarding from source to destination. Node A generate RREQ packet indicating it wants to send information to Node E. RREQ includes source address, source sequence number, broadcast id, destination address, destination sequence number, hop count. When Node C receives the broadcast packet from A i.e. RREQ packet it updates the hop count by 1 and checks for the destination. But C doesn't have the information of destination so it first updates its routing table and then broadcast to its neighbour. As both A and D receives the RREQ from C. A discards the packet as A itself has broadcasted it before considering it is duplicate packet while D updates hop count and its routing table .Node E which is destination node finds the RREQ packet and acknowledge that it is meant for itself so it prepares RREP (Route Reply) packet in which it adds sequence number of a node to specify its time stamp.



Dest	Next	Hop	Seq
E	C	3	120

Dest	Next	Hop	Seq
A	D	3	1

Dest	Next	Hop	Seq
A	C	2	1
E	E	1	120

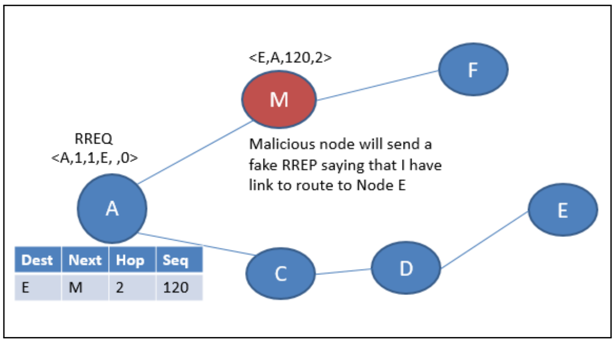
Dest	Next	Hop	Seq
A	A	1	1
E	D	2	120

Figure 2: Routing Table updation due to RREP

The second phase consists of how RREP packet is responded back from destination to source and it is shown in Figure 2. Node E sends RREP with the help of routing table as it has information about how Node A can be reached i.e. via node D with hop count of 3. After that Node D updates its routing table by backtracking the sender i.e. E and store the information of E in its routing table. Similarly, C which is intermediate node receives the RREP from D and updates its table as in Figure 2 and broadcast to its neighbour A and D. After node A receiving the RREP communication starts with the help of routing information of each node. On route discovery, if there are multiple routes possible to destination then the node selects the shortest path considering hop count.

3. Blackhole Attack

Blackhole is an attack in which the attacker promote itself having the fresh path to the destination node even though the node has intention to forward the packet. This attack highly decrease the packet delivery ratio, throughput and the network performance[6]. Once a malicious node receives a RREQ packet from any other node, it immediately sends a false RREP; without checking its routing table; with a high sequence number and hop count equals 2 (i.e. one hop from the source and the destination) to spoof its neighbours that it has the best route to the destination[7]. The malicious node reply will be received by the source node before any other replies. The high sequence number will cause the route including the malicious node to be selected. When the data packets routed by the source node reach the blackhole node, it drops the packets rather than forwarding them to the destination node.



Dest	Next	Hop	Seq
E	M	2	120

Figure 3: Blackhole Attack

Let us take a scenario to illustrate it in detail. Node A be a sender and E be the receiver and M be the malicious node as shown in Figure 3. Then it works as described in previous section to forward RREQ and receive RREP from destination node. Now Node A broadcast the RREQ packet to its neighbour nodes i.e. C and M. After receiving RREQ Node C being malicious node will send a fake RREP packet saying that “I have link to route to Node E, you can pass me the data” and make ready the RREP packet and broadcast to node A.Now, Node A updates its routing table and get ready to send data to destination node E. Later node M receives all the data to be sent from node A to node E as shown in Figure 3. In this way, black hole attack occurs in network and malicious node receives all the information of sender which leads network to be vulnerable.

4. Related Work

Since the on-demand routing protocols have been introduced, many significant algorithms have been proposed to secure MANET against blackhole attack. Some of these solutions use various cryptographic techniques to secure the routing packets. While these solutions introduce high immunity to the blackhole attack, network nodes suffer from the high computations required which does not suit the characteristics of MANET.Other solutions suggest modification to the routing protocols by adding some packets, modifying the existing packets or changing the procedure of these protocols. Such solutions focus their suggested mechanisms on the RREP received from a blackhole node is that this reply is usually received before any other replies as a result of blackhole node not needing to check its route table. These solutions make assumptions about blackhole behavior and cannot guarantee that excluded nodes are genuine blackholes. In this section we introduce some of the existing algorithms used to avoid the blackhole attack.

SAODV [8] is an enhancement of AODV routing protocol to fulfill security feature. The protocol operates mainly by appending an extension message to each AODV message. The extension messages include a digital signature of the AODV packet using the private key of the original sender of the routing message and a hash value of the hop count. SAODV uses asymmetric cryptography to authenticate all non-mutable fields of routing messages as well as hash chain to authenticate the hop count (the only mutable) field. Since all fields except the hop count of routing messages are non-mutable they can be authenticated by verifying the signature using the public key of the message originator. So, when a routing message is received by a node, the node verifies the signature of the received packet. If the signature is verified, the node computes the hash value of the hop count; if the routing message is RREQ or RREP; and compares it with the corresponding value in the SAODV extension. If they match, the routing message is valid and will be forwarded with an incremented hop count and a new hash value or if the destination has been reached generate the RREP.

L. Tamilselvan[1] proposed a solution that designed upon a Fidelity Table in which each participating node is assigned with a fidelity level that determines the node reliability. A default fidelity level is assigned to each node and this level is updated based on the behavior of the node. When a source node receives RREP, it waits to receive further route replies from its neighboring nodes and then selects a neighbor node with a highest fidelity level to forward data to the destination node. A destination node acknowledges receiving the data by sending ACK. Updating the fidelity level of node relies on trusted participation of the node in the network. The source node increments or decrements the fidelity level of the forwarding node upon receiving or missing the ACK respectively. Node is eliminated from the network if its fidelity level reaches zero and marked as a malicious node. The main drawback of this solution is the high end-to-end delay specially when the malicious node is far away from the source node.

N. Choudhary [9] introduced a solution that based on sensing the wireless channel. This approach assigns a max trust value to all its neighboring nodes. A node will not do any further communication with a neighbor whose trust value is less than min trust value. When a source node receives a RREP message, it updates its routing table, starts transmitting the data packets and inserts a unique sequence number with each transmitted data packet. When a node forwards a data packet, it sets a timer and listens to the wireless channel in promiscuous mode to ensure that this packet is forwarded by a next hop neighbor. When the timer expires without hearing the retransmission of this packet, the node reduces the trust value for its next hop node. Trust value information is updated and disseminated to other neighboring nodes. If the trust value of a node decreases below min trust value, it will be isolated by all the nodes in the network.

5. Proposed Solution

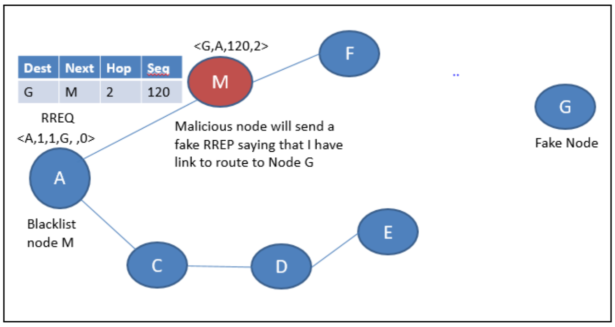


Figure 4: Blackhole Detection

Detection is done with the help of fake RREQ. Fake packet simply means a packet which sender sends to identify the blackhole in which sender starts the communication sending the RREQ with non-existing or virtual node in the network which is unreachable. In figure Node A is sending the packet to Fake node which is unreachable in the network and is represented as G as shown in the Figure 4. After sender generatinging fake RREQ packet, genuine node simply broadcast the RREQ packet to its neighbor nodes whereas malicious node responses with RREP packet for fake RREQ. This reply is useful to detect malicious node. We detect the malicious node with the help of trace file by tracing the path from sender to the destination.Taking into consideration the fact that a black hole node always tries to send a fake a RREP with highest sequence number and also that it cannot fake the unique ID of the destination. Trace file consist of routing information from where certain packet is travelling but not the exact path. Each packet need to be traced using flow ID of the packet. Flow ID gives the information of packet where the packet has visited. After identifying the blackhole node, they are blacklisted. This process is applied in the network till all the blackhole nodes are identified as only one node can be identified at a time. Communication is started once there is no response for the fake RREQ.

6. Simulation Approach

NS-2 simulator [10] is used to simulate under blackhole attack. The parameters used are shown in Table 1. Node mobility was modelled with the random waypoint method. While we examined our proposed mechanism on UDP traffic and the mechanism succeeded in detecting blackhole neighbors and enhancing the network performance , this paper is focused on the results of the proposed mechanism on the UDP traffic only. We examined our proposed mechanism for different number of nodes as 10, 15, 20, 25 and 30 with blackhole nodes as 1, 2, 2, 3 and 3 repectively and different node speeds (0, 5, 10, 15, 20 and 25 m/s) as shown in Table 1. The highest negative impact of malicious nodes usually appears on static networks and this effect decreases as nodes mobility increases. We compare the performance of networks using AODV under blackhole attacks with and without our mechanism. Our blackhole attack model assumes that once a malicious node receives a RREQ packet from any other node, it immediately constructs a fake RREP that includes a randomly generated hop count to spoof other nodes about best route.

Table 1: Simulation Parameters

Parameter	Value
Simulation Time	50 sec
Simulation Area	1200 m x 1200 m
Number of Nodes	10, 15, 20, 25, 30
Number of Malicious nodes	1, 2, 2, 3, 3
Node speed	0 - 25 m/s
Traffic type	CBR

Another network setup was done with 50 nodes varying blackhole nodes from 0 to 5 to observe the effect of malicious node on the network as shown in Table 2.

Table 2: Simulation Parameters

Parameter	Value
Simulation Time	50 sec
Simulation Area	1200 m x 1200 m
Number of Nodes	50
Number of Malicious nodes	1, 2, 3, 4, 5
Node speed	0 - 25 m/s
Traffic type	CBR

Packet Delivery Ratio (PDR): The ratio of packets that are successfully delivered to a destination compared to the number of packets that have been sent out by the sender.

$$\text{PDR} = \frac{\text{Received packets}}{\text{Sent packets}} \tag{1}$$

Throughput: The number of data bits delivered to the application layer of destination node in unit time measured in bps.

End-to-End Delay (EED): The average time taken for a packet to be transmitted across the network from source to destination.

7. Results and Analysis

First of all, comparison of network on normal mode and with a blackhole is done. In this scenario, only one node is taken as blackhole node and simulation was run by setting up the network as in Table 1. The effect of increasing no of nodes with packet delivery ratio is shown in Figure 5. When the no of nodes is less, packet drop ratio aren't observed in both normal and prevented mode. As packet is dropped if network switches path and the result shows if no of nodes increases, packet drop ratio decreases. This is because as the no of node increases and the nodes are mobile, path is varied throughout the simulation and if destination isn't reachable then packet drops significantly. Normally, packet delivery ratio is less in normal mode but it is not the case when number of nodes are 20 due to the reason that the network route wasn't changing even if nodes are mobile after ommitting the blackhole nodes. This literally means that in normal mode blackhole node is participating in the route which is mobile and there was a path switch that result packet drop.In AODV routing protocol,when nodes are mobile better path is searched if link breaks down so it arises PDR.

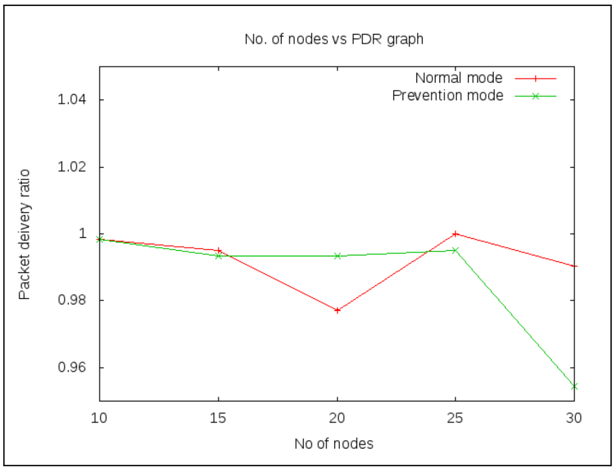


Figure 5: No of nodes Vs Packet Delivery Ratio

The effect of increasing no of nodes with throughput on normal and prevented mode on the network is shown in Figure 6. Throughput is slightly decreasing as the no of nodes increases.

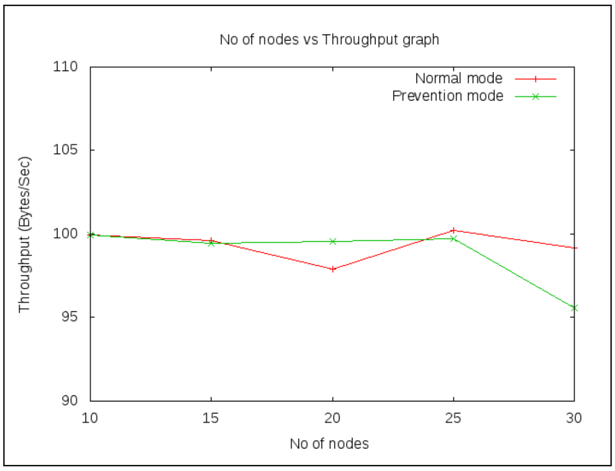


Figure 6: No of nodes vs Throughput

The effect of delay in the network as the no of nodes increased in both prevention and normal mode is presented in Figure 7. Delay increased significantly when we took larger network since the distance between the source and distance is larger is greater.

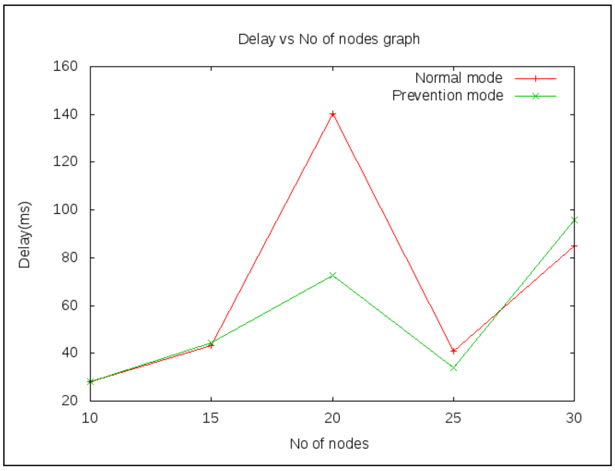


Figure 7: No of nodes vs Delay

The effect of increasing no of blackhole nodes with packet delivery ratio in the network is shown in Figure 8. As the no of malicious nodes increases PDR steeps down but again with high malicious node PDR steeps up. The result is due to the reason that the position of the malicious node plays vital role, if the position of malicious node in the path it has larger impact in the network and if malicious node doesn't lie in the path, malicious node has very less impact on PDR in the network.

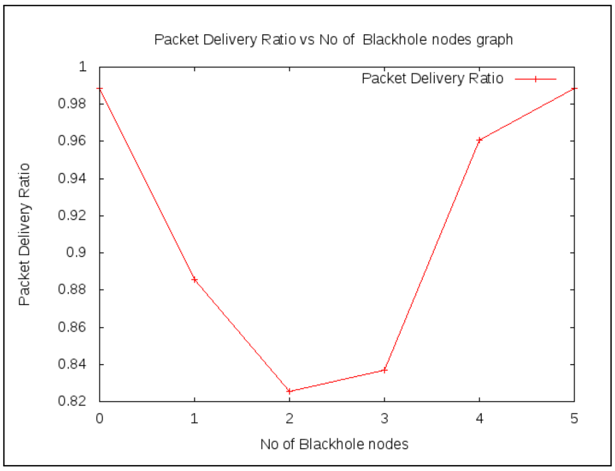


Figure 8: No of Blackhole vs Packet Delivery Ratio

The relation between throughput and increasing no of malicious nodes is shown in Figure 9. The result shows throughput is high when we have no malicious node and 5 malicious nodes. When no of malicious nodes increases, they are filtered out and alternative path is followed and throughput is decreasing.

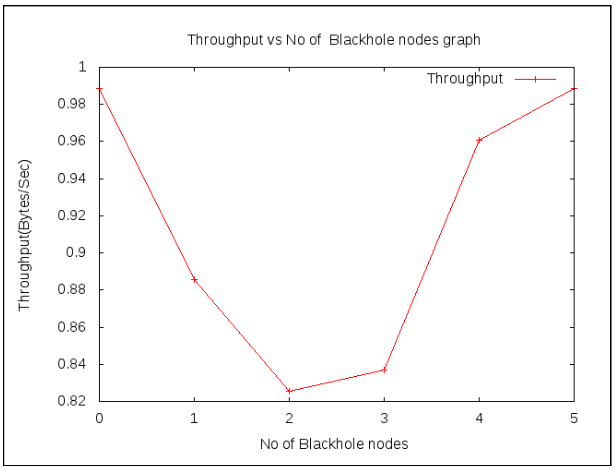


Figure 9: No of blackhole vs Throughput

The effect of delay with number of blackhole nodes is shown in Figure 10. Delay is less when there is no malicious node, with including malicious node it increases significantly and after having high no of malicious nodes delay is approximately equal to the one with no malicious node. This result is due to the reason that malicious nodes are filtered in prevented mode and even after filtering these nodes there exist the appropriate path same as the path without malicious node.

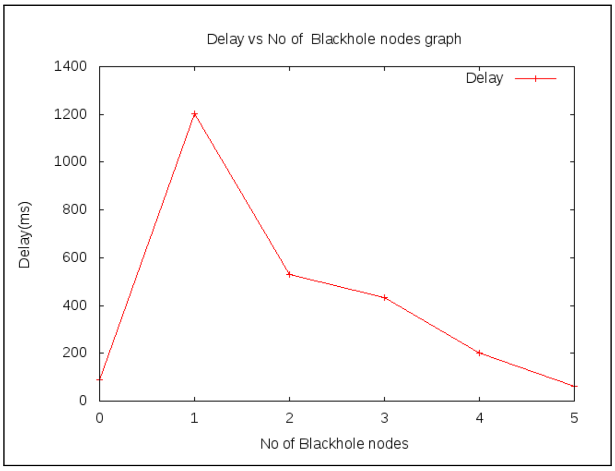


Figure 10: No of Blackhole vs Delay

8. Conclusion

A new concept has been introduced to detect a malicious intruder which is accomplished by complying with the normal protocol behaviour. We introduced a new Blackhole resisting mechanism that can be incorporated into any reactive routing protocol in MANET. The proposed mechanism uses fake RREQ packet that cheats the malicious node to detect it. The mechanism requires additional packets before sending the real packet to check if the network is free of malicious node or not and trace information form where it gets responses. The proposed mechanism succeeded in detecting blackhole nodes within a short time regardless the number of malicious nodes and the time they are participating in the network.

References

[1] L. Tamilselvan and Dr. V. Sankaranarayanan. Prevention of blackhole attack in MANET. In *The 2nd International inproceedings on Wireles Broadband and Ultra Wideband Communications ,IEEE*, 2007.

[2] C. Mihaela M. Pervaiz and Jie Wu. Routing security in ad hoc wireless networks. 2005.

[3] Ashwani Kumar. Security attacks in MANET. In *IJCA Proceedings on National Workshop-Cum-inproceedings on Recent Trends in Mathematics and Computing, RTMC(11)*, 2012.

[4] C. E. Perkins and E. M. Royer. Ad-hoc on-demand distance vector routing. In *2nd IEEE Workshop on Mobile Computing Systems and Applications*, 1997.

[5] K. Satoshi and H. Nakayama. Detecting blackhole attack on aodv based mobile ad hoc networks by dynamic learning method. *International Journal of Network Security*, 2007.

[6] M. Mistry and P. Tandel. Mitigating techniquues of black hole attack in MANET. In *International Proceedings on Trends in Electronics and Informatics*, 2017.

[7] N. Sharma and A. Sharma. The black-hole node attack in MANET. 2012.

[8] M. G. Zapata. Secure ad hoc on-demand distance vector routing. In *SIGMOBILE Mob. Comput. Commun. Rev*, volume 6, pages 106—-107, Jun 2002.

[9] Nidhi Choudhary and Lokesh Tharani. Preventing black hole attack in AODV using timer-based detection mechanism. In *International Proceedings on Signal Processing And Communication Engineering Systems (SPACES)*, pages 1—4, Jan 2015.

[10] *The network simulator ns-2*. http://www.isi.edu/nsnam/ns/.