ijecs open access www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume - 3 Issue -8 August, 2014 Page No. 7420-7430

Detection and Prevention Of Black Hole Using Clustering In MANET Using Ns2

Gurnam Singh, Gursewak Singh
Department of CSE (PITK) [1], Department of CSE (LPU) [2]
Email: gurnam.karwal@gmail.com[1], gursewak_garcha@yahoo.com[2]

ABSTRACT

A MANET contains wireless mobile nodes that communicate together without any need of infrastructure of network as well as any central base station. This is the reason it is widely used in area that has a limitation of infrastructure and even we can form huge group of people with fruitful communication through the use of mobile nodes in the MANET. Nodes in the MANETS are autonomous and managed by itself in the absence of infrastructure. Mobile ad-hoc networks are exposed to numerous attacks due to (a) dynamic behavior. (b) In MANETS, any node can join and leave the network at any time. Black node is a malicious node that drops the packets in the network by giving the false replay for any route request and also it does not contains any path for destination. The existing method identifies the black hole attack based upon the sequence number in the RREP message.
Here the proposed method eradicates the malicious black hole node at distributed level. For the implementation of our methodology NS2 tool is used. The overall results by the simulation increases the detection rate of malicious node and that leads to the increase in network performance by lowering the rate of packet drop ratio.

Keywords —ad-hoc, Black hole, MANET routing protocols, AODV, cluster, Security.

INTRODUCTION TO MANETS

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. The communication and connectivity is done from node to node by forwarding packets among themselves. The protocols used for packet forwarding in MANET are dynamic source routing, destination sequenced distance vector and ad-hoc on demand distance vector. Due to non-availability of network infrastructure and autonomous behavior of nodes, network is vulnerable to many attacks. Most commonly found attacks are black hole attack, man in middle attack, Denial of Service attack, Impersonation, Eavesdropping, black hole attack, gray hole attack.

AODV is a source initiated on-demand routing protocol. Every mobile node maintains a routing table that maintains the next hop node information for a route to the destination node [1]. Black hole leads to serious loss in the network by receiving the packet and dropping the received packets that has to receive by the destination.

INTRODUCTION TO AODV

As the name describes AODV forms the route from source to destination and between the intermediate nodes when there is demand for forwarding packets using MANETS. AODV (Ad-hoc On-demand Distance Vector) is a reactive routing protocol, yet it is fundamentally an improvement ofDSDV routing protocol which is proactive protocol [2]. Route discovery process takes place onlywhen required. AODV can handle low, moderate, and relatively high mobile rates, together with a variety of data traffic loadings. However, it makes no provisions for security.

In Route Discovery Process of AODV there are three types of messages: Route Request (RREQ), Route Reply (RREP), and Route Error (RERR) messages.

- RREQ- It is basically the broadcast request to find the route to a required destination node. Thus it helps to create a route discovery process by broadcasting Route Request message to its neighbouring nodes. The neighbouring nodes save the path where RREQ request is transmitted. After that it verifies the new or fresh route to the desired node in the routing table by the use of RREQ request [3].
- RREP- when the node finds a fresh path for destination then a route reply message is unicasted to the originator of the RREQ if the receiver is either the node using the requested address or is having a valid route to the requested address.
- RRER-it helps to keep eye on link status of the next hopin the appropriate route. RERR message is broadcasted to whole nodes whenever the breakage in the link is found. This is also called route maintenance.

Advantages:

- Connection set up delay is less
- Destination sequence numbers are used to find the latest route to the destination.
- On-demand route establishment with small delay
- Link breakages in active routes can be efficiently handled

Disadvantages:

- Periodic beaconing leads to bandwidth consumption
- Intermediate routes can lead to inconsistent routes if the source sequence number is old.
- Multiple RERR packets in response to single RREQ packet may lead to heavy control overhead

1.2 INTRODUCTION TO BLACK HOLE ATTACK

A black hole is a malicious node that falsely replies for any Route Request (RREQ) without having active route to specified destination and drops all the receiving packets [4]. A Black Hole node has two properties: (a) the node enters in AODV by represent itself as a valid route for destination. Then it starts receiving the packet from the valid node (b) drops the packet containing valuable information.

- **Single Black Hole Attack:** In single black hole attack only one malicious node attack on the route [5]. When the source node broadcast RREQ message then the malicious node takes an advantage of vulnerabilities of AODV protocol. It responds with high sequence number to its preceding node in the path. Thus source node assumed malicious node as a destination node and start the process of data forwarding. The malicious node then drop all the packet received.

- **Co-operative Black Hole Attack: T**he number of malicious notes is more than one in the network [6]. The overall result of cooperative is complete decrease in throughput and increase in packet drop ratio in the network. Thus for better security and better performance in MANETS it is very important to eradicate the Cooperativeattack.

LITERATURE REVIEW

Table 1. Literature Summary Table

TITLE	OBJECTIVE	METHODOLOGY	DISADVANTAGES
Antony et al. [7]	Prevention of single and co-operative Black hole attack.	MN-ID broadcasting method is used. In this method once the malicious node is identified, the particular node id is transmitted to the entire network whether the malicious node take part in two or more path packets does not move towards the malicious node because whole nodes in the network should know about the malicious node.	Delay in identifying black hole attack this leads to packet loss
Deng et al. [8]	Prevention of single black hole attack	Any node on receiving a RREP packet, cross check with the next hop on the route to the destination from an alternative path. If the next hope either does not have a link to the destination then that node is considered as a malicious node.	Failed to detect cooperative black hole attack nodes
Weerasinghe et al. [9]	Detection and Prevention of single black hole attack	DRI table keeps track of whether or not the nodes did data transfers with its neighbor or not.	1. Delay in identifying black hole attack this leads to packet loss. 2. Overhead of keeping DRI table by all the nodes
Neelam et al. [10]	Avoiding black hole attack	Assign unique id number to all the normal nodes exist within AODV. And transfer the data only via that path.	Failed to avoid black hole node if black hole node exist within AODV path.
ketan chavda et al. [11]	Removal of black hole attack	This method identifies the black hole node that found between the source and destination based upon the sequence number in the RREP message.	• Detection of malicious node which is not in the path from source to sink • Failed to select black hole node in case of two exceptionally high sequence number.

1. ASSUMPTIONS AND METHODOLOGY

3.1 ASSUMPTIONS:The whole methodology is based upon the following assumption to analyses the network performance with and without the effect of malicious node at distributed levels.

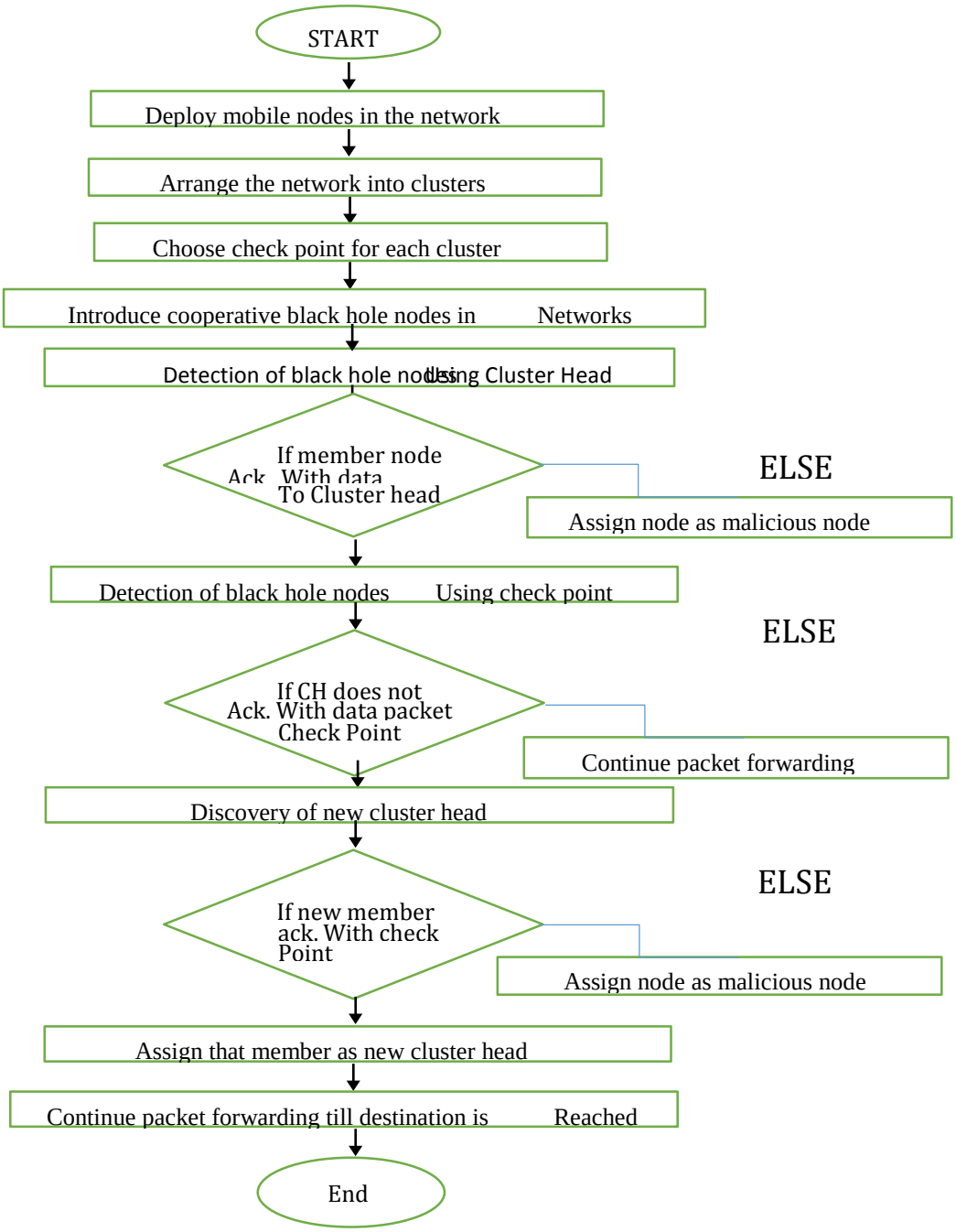
1. Malicious node does not acknowledge withdata packet in the network.
2. Black hole node will receive the packet but instead of forwarding the packet it will drop all the received to lower the packet delivery ratio and network efficiency.
3. Check points are the nodes which is randomly chosen for each cluster and is used to detect malicious cluster head.

3.2 METHODOLOGY:For the performance analyses of network with and without the entry of malicious nodes, distributed clustering approach is proposed. For that firstly deploy the nodes in the networks. Then arrange the network into different clusters, after that assign the check point for each cluster randomly. Introduce the cooperative black hole nodes in the network.

The Detection is done at two levels:

- ***Detection of malicious nodes using Cluster Head*** **-** The detection of cooperative black hole nodes within each clusters are done with the help of CH. Here, if any member of the cluster does not acknowledge with Cluster Head then it is treated as a black hole.
- ***Detection of malicious nodes using check points - It*** helps to detect whether cluster head is black hole node or not. When the CH does not acknowledge to check point then treat those CH as a malicious node. Check points then starts the discovery process of new CH. In this way the all the cooperative malicious nodes are detected within the entire network and improves the network performance as well.

FLOWCHART FOR IMPLEMENTATION:



2. IMPLEMENTATION AND ANALYSIS

4.1 SIMULATION PARAMETERS

Table 2. Simulation Parameter Table

Parameter	Value
Simulator	NS-2
Version	NS 2.34
Number of Nodes	110
Channel	Wireless channel
Traffic Type	CBR
Routing Protocol	AODV
MAC Type	802.11 MAC Layer
Packet Size	512 bytes
Antenna Type	Omnidirectional

4.2 METRICS FOR SIMULATION

Throughput ratio: It is defined as a rate at which message is successfully delivered between a source and sink. It is measured as bits per second. More is the throughput ratio more will be the performance of the network.

Packet delivery ratio: It helps to predict the drop rate of packet. It is basically the ratio of the total number of data packets received by the sink to the total number of data packets sent by the source node. Similar to the throughput ratio, the value of packet delivery ratio must be high for better network performance. Its higher ratio leads to the decrease in drop rate of packet.

Attack Detection Rate: Rate that defines number of black hole node detected with the total number of black hole nodes taken.

4.3 SIMULATION SCENARIO USING NS2

- **Deployment of nodes in the network**

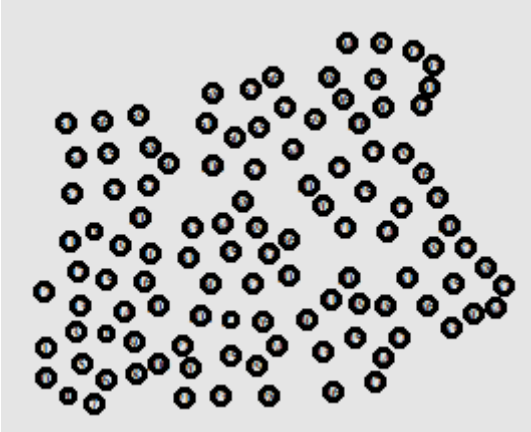


Fig 1.Deployment of Nodes

- **Arrangement of network into clusters and assignment of cluster head and check points for each clusters:** Red colored outlined nodes are the check pints for each clusters and each clusters contains 10 nodes and 1 check point.

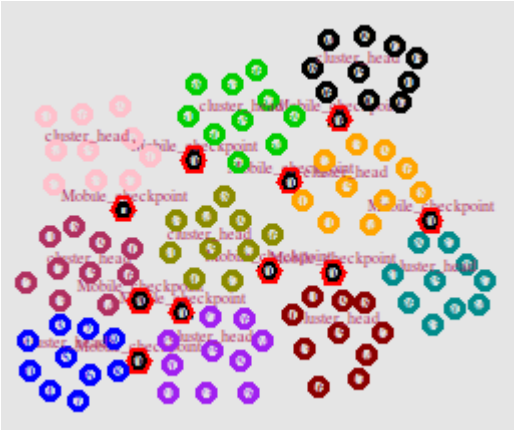


Fig 2. Assignment of Network into Clusters

- **Detection of black hole nodes at luster head and check point level for each clusters:** All red colored nodes are the cooperative black hole nodes detected in the network**.**

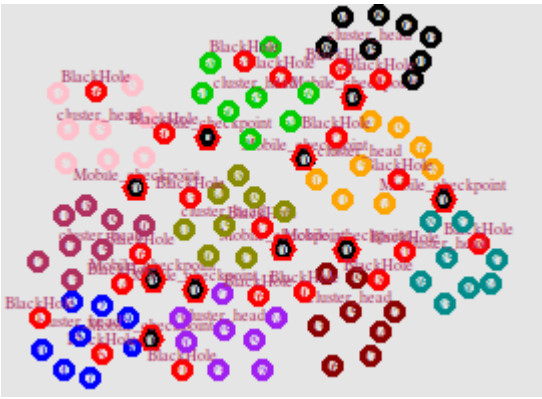


Fig 3. Detection of Malicious Nodes using Cluster Head

- **Sending data via new protected path after detecting all cooperative black hole nodes**

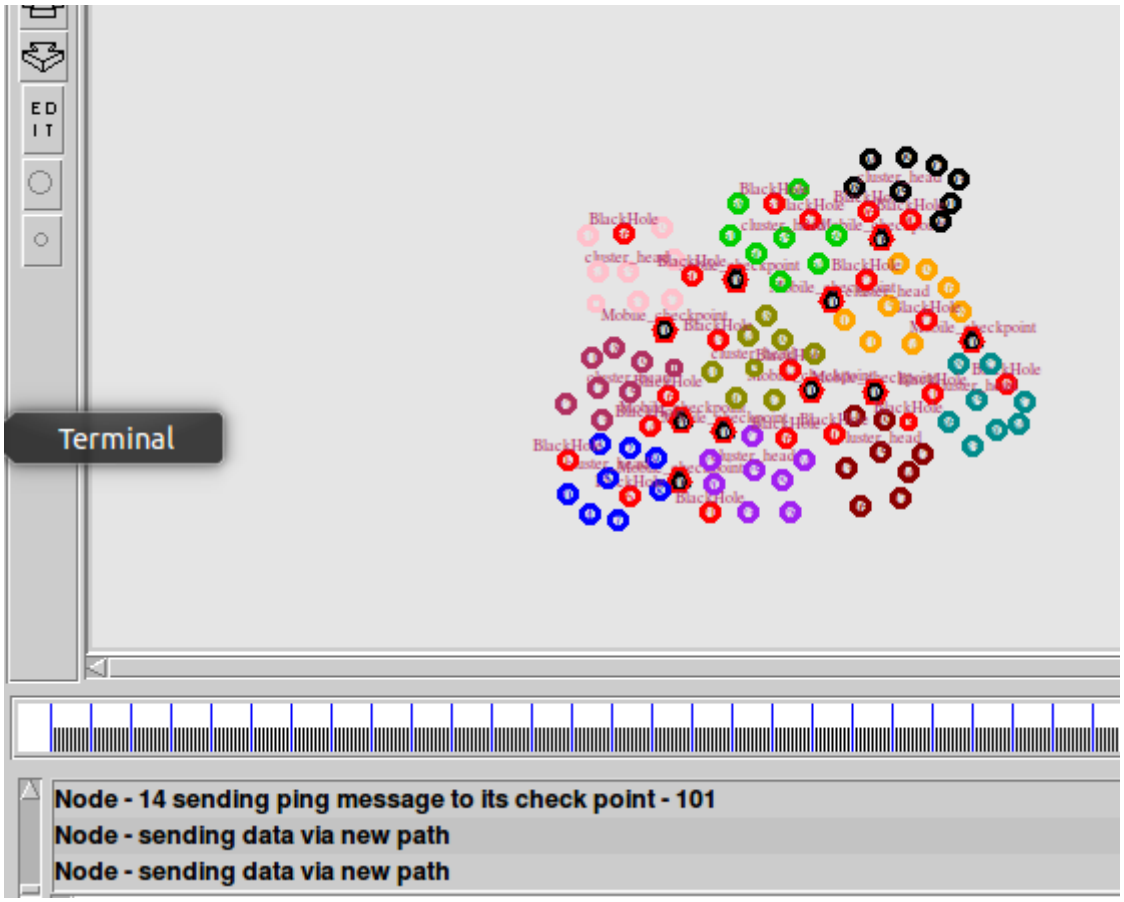


Fig 4. Data Forwarding Using Protected and Safe Path

4.4 RESULTS AND COMPARISON

The proposed methodology is compared with the existing approach of safe route method based upon the sequenced number of route reply message on the basis of throughput, packet delivery ratio and attack detection rate.

- **Packet drop Ratio Graph:** Under normal circumstances packet drop rate is zero percent. When the attack is launched its value goes to peak and after prevention of black hole attack drop rate start decreasing at rapid rate.

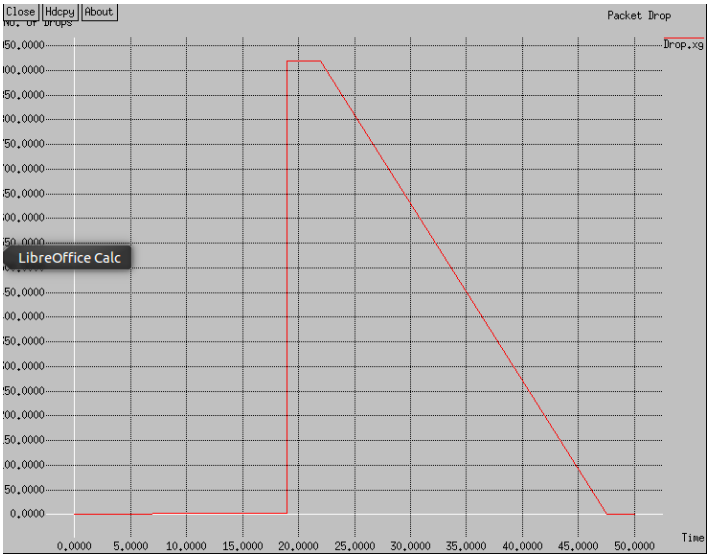


Fig 5. Packet Drop Ratio Graph

- **Packet delivery Ratio Graph:** By the proposed methodology the PDR value is increased by 5% in comparison with safe route method based upon sequence number as PDR value according to their method was 20%.

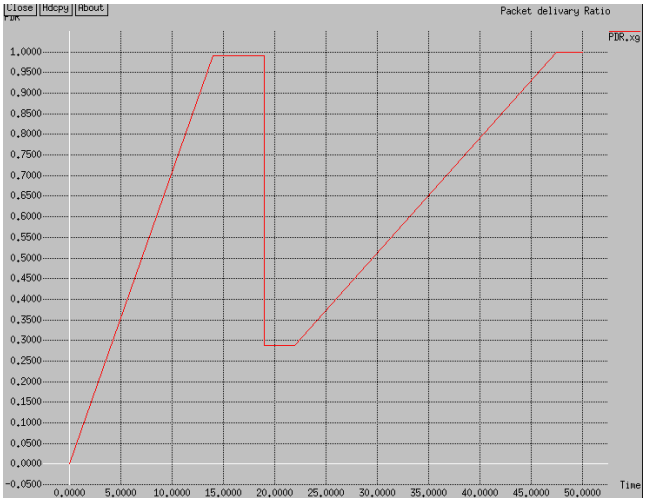


Fig 6. Packet delivery ratio graph

- Throughput graph: the throughput value by the proposed methodology of clustering is 38 % under attack occurrence condition which is greater than 33% of safe route method based upon sequence number.

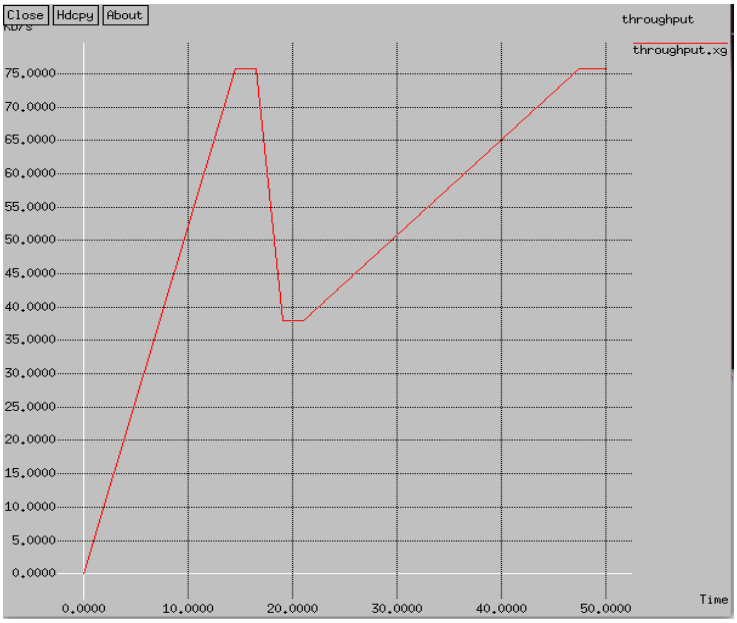


Fig 7. Throughput ratio graph

- **Attack Detection Rate Graph:**It defines the overall detection rate of black hole nodes in entire network. The detection rate is about .95

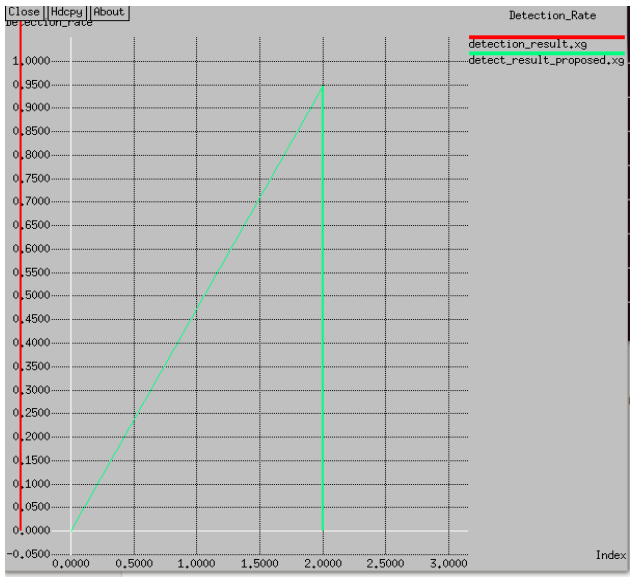


Fig 8. Attack Detection Ratio Graph

3. CONCLUSION AND FUTURE WORK

Black hole attack is hazard to AODV. In the existing approach of safe route method based upon the sequence number they are only able to detect the malicious node that occurs between the route of source and destination instead of detecting black hole nodes in the whole network. Our approach successfully detects the malicious nodes in the entire network and simulation results are predicted to be more efficient than the existing approach of safe route method with high packet delivery ratio as well as high detection rate of black hole nodes. In future we try to apply this approach for prevention of gray hole attack using dynamic clustering.

4. REFERENCES

1. Gurung, Shashi, and Krishan Kumar Saluja. "Mitigating Impact of Blackhole Attack in MANET." Int. Conf. on Recent Trends in Information, Telecommunication and Computing, ITC. 2014.

2. Abusalah, Loay, AshfaqKhokhar, and Mohsen Guizani. "A survey of secure mobile ad hoc routing protocols."*Communications Surveys & Tutorials, IEEE*10.4 (2008): 78-93.

3. Akhlaq, Monis, et al. "Addressing security concerns of data exchange in aodv protocol."*World Academy of Science, Engineering and Technology*16 (2006): 29-33.

4. Sowmya, K. S., T. Rakesh, and P. HudedagaddiDeepthi. "Detection and Prevention of Blackhole Attack in MANET Using ACO."*International Journal of Computer Science and Network Security*12.5 (2012): 2124.

5. Goyal, Priyanka, VintiParmar, and Rahul Rishi. "Manet: Vulnerabilities, challenges, attacks, application."*IJCEM International Journal of Computational Engineering & Management*11.2011 (2011): 32-37

6. Khin, Ei andThandarPhyu. "Comparative Analysis of Black Hole Attack Solutions in AODV Protocol."*IJCCER*1.2 (2013): 21-25.

7. Devassy, Antony, and K. Jayanthi. "Prevention of Black Hole Attack in Mobile Ad-hoc Networks using MN-ID Broadcasting."

8. Deng, Hongmei, Wei Li, and Dharma P. Agrawal. "Routing security in wireless ad hoc networks." *Communications Magazine, IEEE* 40.10 (2002): 70-75.

9. Weerasinghe, and Kriti. "Discovering a secure path in MANET by avoiding black/gray holes." *International Journal of Recent Technology and Engineering (IJRTE) ISSN*: 2277-3878

10. Sanjay Ramaswamy, Huirong Fu, Neelam , ”Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks”. In Proceedings of 2003 International Conference on Wireless Networks (ICWN’03), Las Vegas, Nevada, USA, pp. 570-575.

11. Chavda, Ketan S., and Ashish V. Nimavat. "Master of Computer Engineering, CU Shah College of Engineering and Technology, Wadhwancity." Computing, Communications and Networking Technologies (ICCCNT), 2013 Fourth International Conference on. IEEE, 2013

AUTHORS 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 area of interest are wireless sensor network, network security protocols design and Mobile and Ad-hoc Network and Data Structure.

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.