Detection and Prevention of Cooperative Black Hole and Gray Hole Attack In MANET Using DSN and Reverse Tracing Scheme

Benzeer Kaur[1], Harleen Kaur[2]
[1]*Student, Department of Computer Science & Engineering, Baba Farid College of Engineering and Technology, Bathinda, India*
[2]*Asst Prof., Department of Information Technology & Engineering, Baba Farid College of Engineering and Technology, Bathinda, India*

Abstract- MANET is branch of networking that deals with communication from source to destination without any wired infrastructure. Various malicious attacks degrade performance of the network. These attacks are gray hole and Cooperative black hole attacks. In black hole attack the adversary node with the help of routing protocol announces the node that has a valid shortest route. After the establishment of route, the adversary node drops all packets and does not forward packet to destination. Gray hole is that in which node sometimes act as an ordinary node and sometimes act as attacking node. In this paper an approach has been purposed for detection of malicious behavior of the nodes in early route establishment path using DSN flow and CBDS for reverse tracking to detect attack in the network. Purposed approach comprises best detection in MANET prior to various previous detection approaches and this approach is detecting various malicious nodes.

Keywords*:* MANET, Black Hole, Gray Hole, DSN and CBDS

1. INTRODUCTION

1.1 Mobile Ad Hoc Networking (MANET)

The Mobile Ad-hoc Networking (MANET) is a collection and set of independent network. In mobile ad-hoc network mobile devices are connected through various wireless links. The mobile ad-hoc network works on a constrained bandwidth. The network topologies are dynamic and network topology may vary from time to time. Each and every device must act as a router and route their packet for transferring any traffic among each other. This network can operate by itself and incorporate into large area network (LAN).

There are three types of MANET.

1. Vehicular Ad hoc Networks (VANETs)
2. Intelligent Vehicular Ad hoc Networks (In VANETs)
3. Internet Based Mobile ADHOC network (iMANET)

1.2 SECURITY ATTACKS IN MANET:

A. Flooding Attack: The flooding Attack is a denial-of-service attack. The malicious node sends the fake packets in the network and disturbs the normal functioning of the network. Nodes under the flooding attacks are unable to receive or forward any packet and all the packets directed to them will be discarded from network [8].

B. Impersonation: A node may disguise as another node and send fake routing information to some other normal node. A malicious node might gain perceptive information and even provide fake information to other nodes [2].

C. Packet Modifying: The intermediate node changes the contents of packets during transmission. In a message modification attack, some changes are made in the routing messages by the attacker. In Ad-HOC Network nodes are free to move and self-organize, relationships among nodes at some times nodes may include the malicious nodes. These malicious nodes might disturb the random relationships in the network .The malicious node participate in the packet forwarding process, and launch the message modification attacks [8].

D. Worm Hole Attack: A worm hole assail is when two or more suspicious nodes work together to encapsulate and exchange messages between them. A worm hole attack always tunnels the packet to its misbehaving partner node [2]. In a wormhole attack, an attacker receives packets at one point in mobile ad-hoc the network, "tunnels" them to another point in the network. Routing can be disrupted and corrupted when routing control message are tunnels. This tunnel between two colluding attacks is known as a wormhole attack.

E. Sink Hole Attack: In sinkhole Attack, malicious node collect wrong routing information and to produce itself and receives all network traffic in MANET. Gray hole attack and black hole attack are most popular examples of sink hole attack in mobile ad-hoc network [9].

F. Black hole Attack: It is a kind of selfish node that just drops the packets and hence the transmission further. Black hole attack occurs on network layer. Black hole gray hole example of sink hole attack. Black hole is a active type of attack. The black hole attack not send any packet to the destination it drops the all packet. In black hole attack not

any packet send at destination side, black hole node drop all received packets.[9]

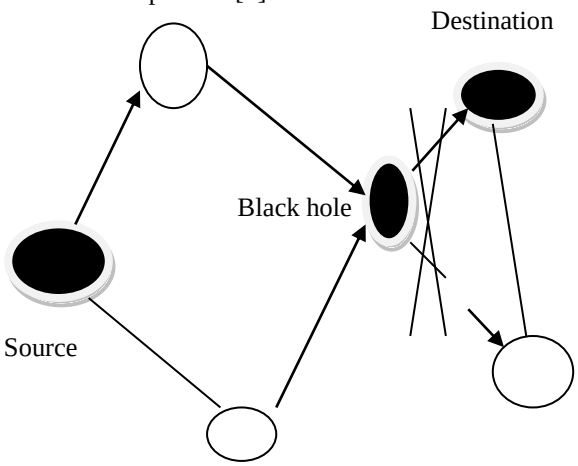

Fig 1: Black hole attack [10]

In Black hole attack, adversary node with help of one of reactive routing protocol announces that it has a valid Shortest route, and once the route is established it drop packets without forwarding to next node.[11]

Internal black hole attack -In internal black hole attack, malicious node which fits in between the routes of given source and destination and drop all packet.

External black hole attack- External attacks occur outside of the network and try to access network traffic or disrupting the process of entire network.

G. cooperative black hole attack: Some times in AODV if in RREP the next hop information is asked then malicious node provide next malicious node as a next hop, when confirmed with the next hop then and next malicious node replies that I am having route to the destination node in the network but actually malicious node don't have any information of routes to destination. This is called a cooperative black hole attack [6].

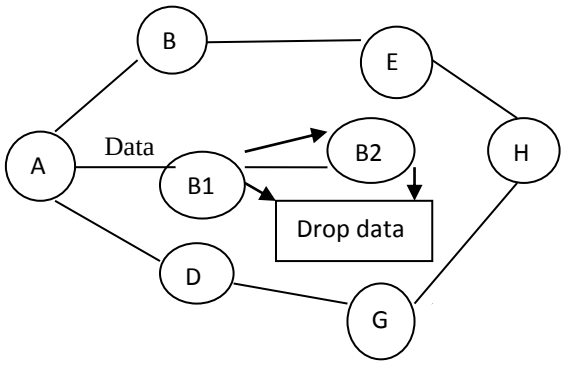

Fig 2: Cooperative Black hole Attack [6]

H. Gray hole attack and Black hole attack**:** Gray hole attack is also a kind of Denial of service attack [1]. Gray Hole attack may occur due to a malicious node. The malicious node selectively drop the packet .So the gray hole attack is called selective forwarding attack. The malicious nodes not drop all packets but just drop part of the packet it is called gray hole attack. Gray hole attack is an variation of black hole attack. It is an active type of attack [5]. If attacker drops the every packet, it is known as black hole attack. The gray hole attack is difficult to detect because node can drop packet due to Congestion and dynamic topology.

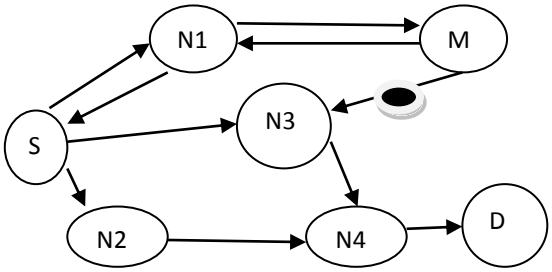

Fig 3: Gray hole attack [6]

Selective forwarding attack is proposed by Karlof and Wagner [4]**.** In black hole attack, adversary node with the help of reactive protocol announces that it has a valid and shortest route and once route is established it drop packet without forwarding to next node .This is called a black hole attack [11].

1.3 Security Requirements in MANETs

1. Availability: Availability means the data assets are accessible to authorized parties at appropriate times. Availability applies to both data and services. It guarantees the survivability of network service despite denial of service attack [7].

2. Confidentiality: Confidentiality ensures that the computer-related assets are accessed only by authorized parties. Protect the information that is exchanging by nodes in a MANET [7].

3. Integrity: Integrity means the assets can be modified only by authorized parties. The assets can be modifying only in authorized way. The Modification includes changing status, selecting and creating message being transferred never corrupted. Integrity guarantees that a message being transferred. The message is not corrupted.

4. Authentication: Authentication indicates that the participants in communication are authenticated and not imitators. The network resources should be accessed by the authenticated nodes.

5. Authorization: Authorization means assigning different access rights to different types of users. For example a network management can only be performed by network administrator [7].

6. Resilience to attacks: It is required to support the network functionalities when a portion of nodes is disconnected or destroyed [7].
7. Freshness: It guarantees that harmful node does not resend previously captured packets.
8. Non repudiation: In non repudiation guarantees that sender or the receiver neither of a message is able to deny the transmission.

II . RELATED WORK

Meenakshi Patel et al. [2] proposed novel automatic security mechanism to detect black and gray hole attack. The SVM is used to defense against malicious attack occurring in AODV.SVM classifies the behavior of the nodes.SVM based system uses PDER, PMOR and PMISR metrics and classifies the nature of nodes. Novel security scheme to detect malicious attack in the MANET .This scheme uses the concept of classification done by SVM. The behavior metrics are used to develop the security system those are easily computed and classify.
Ashok M.Kanthe et al. [5] present effect of black hole, gray hole, packet drop attack that eliminates the network capacity to perform expected function. In MANET the effects of black hole attack, gray hole attack, packet drop attack on AODV protocol under different performance metrics like throughput, packet drop rate and end-to-end delay are studied. The increase in number of malicious nodes decreases the performance of MANET.
Jan von Mulert et al. [3] proposed various security technique .Many attack occur in AODV protocol which disturb the performance of the AODV protocol. The various extensions of AODV like SAODV, ARAN, and SEAODV are used. SAODV uses cryptography approach and digital signature to protect data. The various incentive schemes, directional antennae, packet leashes, localized self-healing communities and a intrusion detection scheme used to detect all these attack. AODV is not secure protocol So SAODV Secure AODV is used to combat all type of attacks.
Renu Sharma et al.[12] proposed ECBDPS scheme. The ECBDPS scheme is used to identify byzantine attacks and prevent them from interrupting data from reaching its destination. Identification of the attack is done on basis of symptoms. The ECBDPS scheme is used to detect and prevent attack in MANET. CBDS does not provide any guarantee about data delivery so ECBDPS scheme is used to detect and prevent attack and used for packet delivery. The ECBDPS ensures better data delivery without any loss.
Ahmad Haghighi [13] proposed a modified cooperation bait detection Scheme. The CBDS technique suffers from false positive rate. In modified CBDS add some operation and reduce false positive rate and improved performance in the terms of throughput delay and energy consumption and decrease routing overhead. The modified CBDS technique detect and prevent black hole and gray hole attack in MANET. The modified CBDS technique improved the performance of DSR protocol.

III. PROPOSED WORK

MANET is the used for forwarding information from source to destination via intermediate nodes. These nodes transmit information from source to destination using various routing protocols. This paper comprised an approach for early detection of gray hole and collaborative black hole attack in MANET's using hybrid approach of cooperative bait detection scheme and DSN based RREP scheme. In the purposed work source node transmit request for data transmission to destination that forward RREQ to adjacent nodes to develop a path from source to destination. In this network malicious nodes reply to route request by defining a greatest destination sequence number to RREP. This causes that malicious node captures a shortest path to forward information from source to destination.
In mobile ad-hoc network the malicious nodes are prevented and detected from participating in the routing operation, using a reverse tracing technique. In this process early detection has been done on the basis of different DSN that has been forwarded by the source node has been matched with reply message DSN so that detection of malicious node can be done using reverse tracking process. In this process dynamic threshold approach has been used that compute dynamic packet delivery ratio that down to a particular threshold value that transmit a alarm to the source node that re- investigate the developed path using initial bait and detect malicious node using reverse tracking process. In this process different malicious node has been detected using collaborative detection approach that works with AODV reactive routing strategy in CBDS Scheme.

On the basis of RREQ and RREP message malicious node is available in the path may forged RREP. Source node does not aware from malicious node available in the network that causes source node selects shortest path that contain malicious node, which attack may then lead to a black hole attack. This attack is called a black hole attack. To resolve this problem, the function of HELLO message is added to the CBDS technique to help each node in identifying which nodes are adjacent nodes within one hop in CBDS technique. This function assists in sending the bait address to detect the malicious nodes and to use the reverse tracing program of the CBDS to detect the exact and correct addresses of malicious nodes. In CBDS technique the baiting RREQ packets are similar to the original RREQ packets, without a destination address is the bait address.

In the process of detection of malicious nodes CBDS is divided into different steps that cover initial bait step and reverse tracking process for malicious node detection.

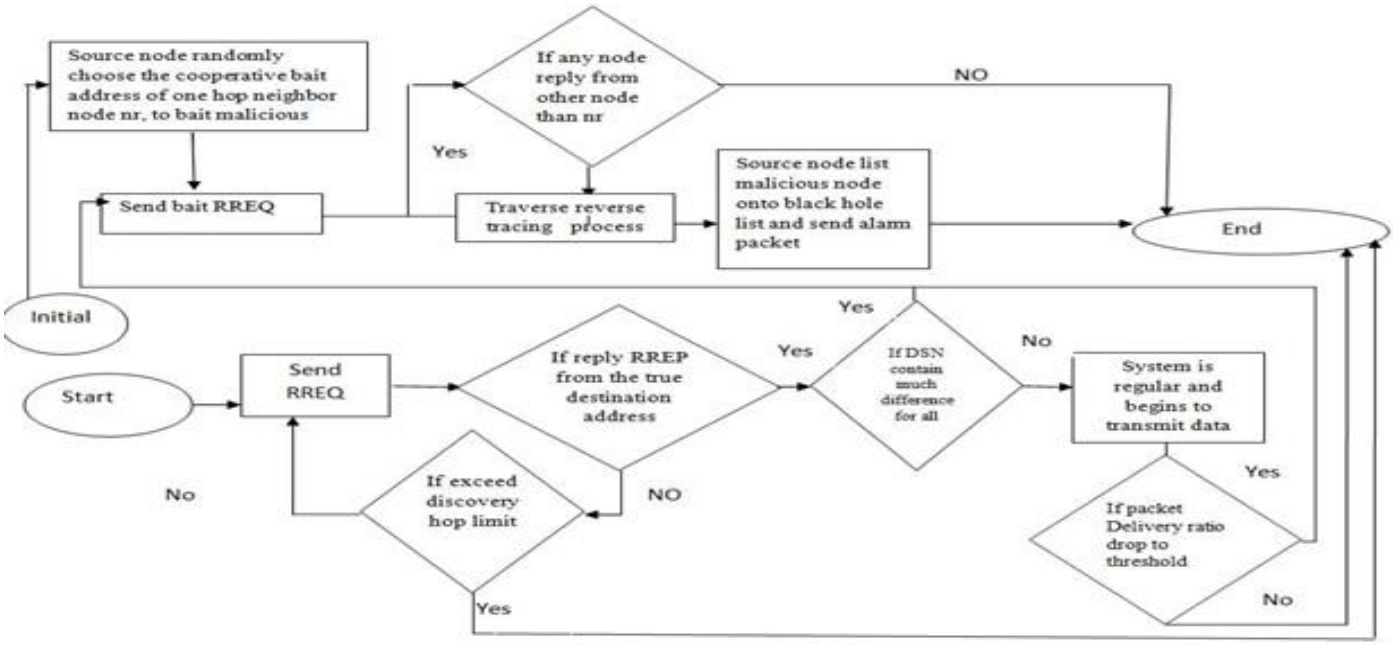

Fig: 4 flow of proposed work

1. Initial Bait Step: The goal of bait phase is detect a malicious node. This technique is generating the destination address of the bait RREQ. In bait phase first send bait route request and after send a RREP if DSN contain much difference for all send bait RREQ because bait route request is used to store the address of one hop neighbor node and used a one hop neighbor node address as a destination address. The neighbor node had not launched a black hole and gray hole attack, after the source node had sent out the RREQ and other nodes reply RREP add a neighbor node. This describe that the malicious node show in the reply routing. The reverse tracing program is used in next step. If DSN is same system working is regular and begin transmit the data. The bait route request sends in our proposed technique.

2. Initial Reverse Tracing Step: In reverse tracing Program is used to detect malicious nodes based on the route reply. If a malicious node has received the RREQ, The malicious node will reply with a false RREP. The reverse tracing operation will be conducted for nodes receiving the RREP. The reverse tracing program gathers unsecure path information and the temporarily trusted zone in the route. To confirm malicious nodes in the route the source node send a test packet in the route and send recheck message in the route and after fed result and send sends back packet to the source node. The source node store the node in the black hole list and send alarm packet in the network inform to other node to terminate operation with this node. In reverse tracing scheme node detected and nodes cooperation stopped.

3. Shifted to reactive defense step: In reactive defense step route is established source to destination. Packet delivery ratio has significantly falls to threshold. The use a dynamic threshold algorithm, the dynamic algorithm control time when packet delivery ratio falls under same threshold.

IV. RESULTS AND DISCUSSIONS

The Mobile ad-hoc network has been used in various areas for data transmission over long distances. In the scenario of mobile ad-hoc network the different types of routing protocols have been used for data communication. There are two types of routing protocols for data communication. 1. Proactive 2.Reactive protocol. Proactive protocols are table driven protocol in MANET that selects the route from the routing table. It is defined by the user. Reactive protocols are on-demand routing protocols in MANET and the used the routing table on demand for data transmission. This protocol selects the shortest path for data transmission. AODV routing protocol used in this work.

Table I: Simulation parameter

Parameter	Description
Area	1500 * 1500
Number of nodes	50
Antenna	Omni
Radio Range	250 m
Queue Type	Drop Tail
Queue Length	250
Routing Protocol	AODV
MAC Type	8.02/11

Simulation Time	200
Mobility Speed	0-20 m/s
Application Traffic	CBR
Packet Size	512
Malicious Nodes	0-40 %

This table represents various simulation parameters that have been defined for MANET communication. In the purposed work various parameters have been analyzed for performance evaluation of purposed work.

In the purposed work simulation has been done using NS 2.35 for simulation of purposed work. In the purposed work detection of malicious nodes have been done through a DSN and CBDS approach. Various performance evolution parameters have been measured in the purposed work for performance evaluation.

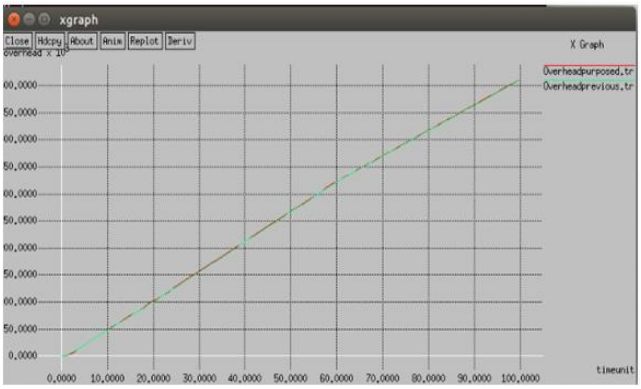

Fig 5: Routing Overhead

This figure is use to represent the overhead in the network.

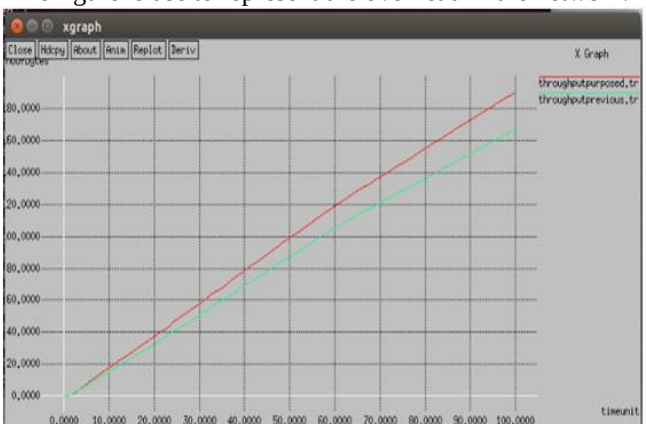

Fig 6: Throughput

Throughput is a average at which data packet is delivered successfully from one node to another through a communication network. It is measured in bits per second.

Throughput = (no of delivered packets * packet size) / total duration of simulation.

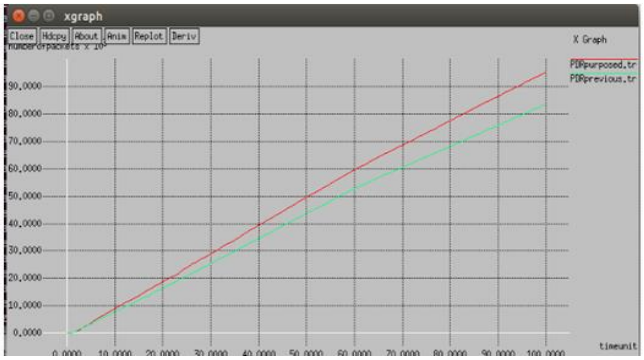

Fig 7: Packet Delivery Ratio

It is the ratio of all the received data packets at the destination to the number of data packets sent by all the sources. It is calculated and dividing by the number of packet received by destination and the no. of packet send through a source.

PDR = (P r / P s) * 100

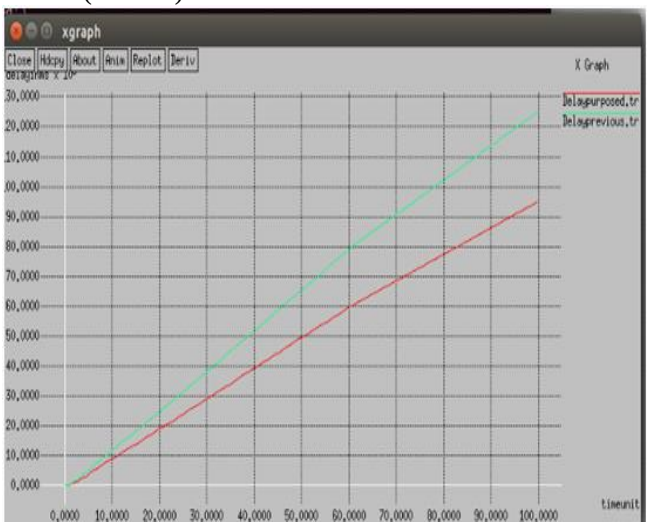

Fig 8: Delay

Delay caused by buffering and through a route discovery, latency, retransmission through intermediate nodes, processing delay in mobile ad-hoc network and propagation delay. It is calculated through a:

D = (T r - T s)

Where, T r is receive time and T s is sent time of the packet.

In the purposed work two different scenarios has been evaluated for performance evaluation if purposed work. On the basis of these scenario in one scenario mobility speed of the nodes in MANET has been varied so that various parameters can be evaluated at different mobility speeds. On the basis of different mobility speed various parameters have been analyzed that has been represented below.

Fig 9: End to End Delay vs Mobility Speed

This graph is use to represent the End to End delay over different modality speed. Data taken at a 0, 2, 4, 6…. Mobility speed.

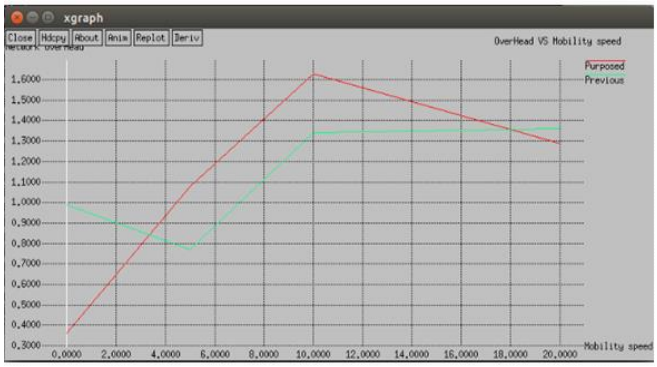

Fig 10: Routing Overhead vs Mobility Speed

This graph is use to represent the Overhead over different modality speed. Data taken at 0,2,4,6… mobility speed.

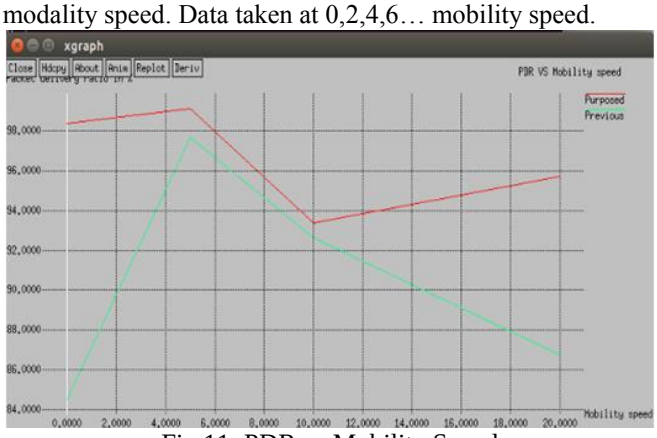

Fig 11: PDR vs Mobility Speed

This graph is use to represent the PDR over different modality speed. Data taken at 0,2,4,6… mobility speed.

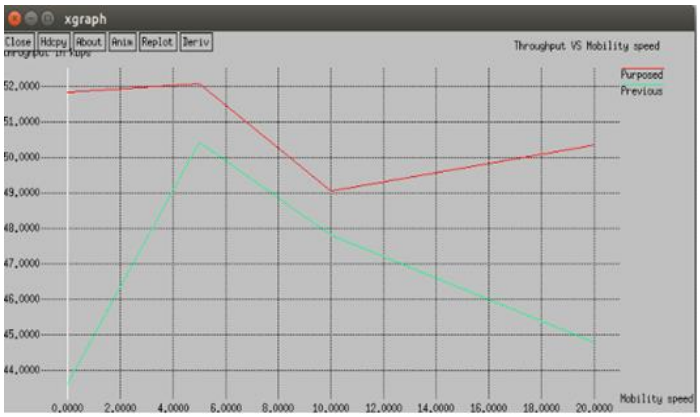

Fig 12: Throughput vs Mobility Speed

This graph is use to represent the Throughput over different modality speed. Data taken at 0, 2, 4, 6. mobility speed.

V. CONCLUSION

Mobile Ad-hoc Network security is the today's biggest challenge. We focused the AODV described the co-operative black-hole attack and gray hole attack in MANET and proposed a feasible solution for detecting and removing them. Our solution is strong for detecting co-operative black-hole, and gray hole attack. In our proposed solution increase packet delivery ratio, decrease end to end delay, and increase throughput and manage overhead from the network.

FUTURE WORK

The CBDS technique can be embedded with some other technique in a different way to yield different yet better results. The Modified a CBDS technique own way and detect and prevent malicious nodes.

REFRENCES

[1] Jiwen CAI, Ping YI, Jialin CHEN, Zhiyang WANG, Ning LIU., "An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network", IEEE International Conference on Advanced Information Networking and Applications, pp. 1550-445, 2010.

[2] Meenakshi Patel , Sanjay Sharma , "Detection of Malicious Attack in MANET A Behavioral Approach", IEEE International Conference Advance Computing (IACC), pp: 388-393, 2012

[3] Jan von Mulert, Ian Welch,Winston K.G. Seah., "Security threats and solutions in MANETs: A case study using AODV and SAODV", Journal of Network and Computer Applications, pp.1249–1259, Elsevier, 2012

[4] Dong Hao, Xiaojuan Liao, Avishek Adhikari, Kouichi Sakurai, Makoto Yokoo, "A repeated game approach for analyzing the collusion on selective forwarding in multi-hop wireless network", pp-2125-2137, Elsevier, 2012

[5] Ashok M.Kanthe, Dina Simunic, and Ramjee Prasad., "Effects of Malicious Attacks in Mobile Ad–hoc

Networks" International Conference on Computational Intelligence and Computing Research, pp. 1-5, 2012

[6] Vani A. Hiremani, Manisha Madhukar Jadhao "Eliminating Co-operative Black hole and Gray hole Attacks Using Modified EDRI Table in MANET", International Conference on Green Computing, Communication and Conservation of Energy (ICGCE), IEEE, pp. 944-948, 2013

[7] Aarti,Dr.S.S. Tyagi "Study of MANET: Characteristics, Challenges, Application and Security Attacks" International Journal of Advanced Research in Computer Science and Software Engineering 3(5), issue 5, volume 3,pp. 252-257, May 2013

[8] Mohd Faisal, M. Kumar, Ahsan Ahmed "ATTACKS IN MANET" IJRET: International Journal of Research in Engineering and Technology, Issue: 10,Volume: 02, eISSN-2329-1163, pISSN-2321-7308 Oct-2013

[9] Nisha Puri, Simranjit Kaur ,Sandeep Kumar Arora., "Performance Analysis of Mobile Ad Hoc Network in the Presence of Sink Hole attack"(IJSER), Issue 3,Volume 1, ISSN:2347-3878,November 2013

[10] Aniruddha Bhattacharyya, Arnab Banerjee,dipayan bose "Different types of attacks in Mobile ADHOC Network: Prevention and mitigation techniques" Department of Computer Science & Engineering, Institute Of Engineering & Management, Saltlake

[11] S.V.Vasantha,DR.A.Damodaram, "Bulwark AODV against black hole and gray hole attack in MANET." IEEE International Conference on Computational Intelligence and Computing Research 978-1-4799-7849, IEEE, 2015

[12] Renu Sharma, Jitender Grover "Mitigation of Byzantine attack using Enhanced Cooperative Bait Detection and Prevention Scheme (ECBDPS),978-1-4673-7231,IEEE, 2015

[13] Ahmad Haghoghi, Kiarash Mizanian and Ghasem Mirjalily "Modified CBDS for defending against collaborative attack by malicious nodes in MANETs" 2nd international conference on knowledge based Engg and Innovation,pp-902-907,Nov 2015

[14] Wikipedia.[online].http://en.wikipedia.org./wiki/wireless_ad_hoc_network

[15] Wikipedia.[Online].http://en.wikipedia.org/wiki/Mobile_ad_hoc_network