International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)
Impact Factor: 3.45 (SJIF-2015), e-ISSN: 2455-2585
Volume 3, Issue 10, October-2017

PROTECTING AGAINST MALICIOUS ATTACKS IN MANETS USING COOPERATIVE BAIT DETECTION APPROACH

K.MAMATHA

PG Scholar (DSCE), Dept of ECE, JNTUACEA, Anantapuramu, Andhrapradesh, India

ABSTRACT : Wireless networks are computer networks that are not connected by cables of any kind. Wireless network enables to avoid the costly process of introducing cables into buildings or as a connection between different equipment locations. Numerous examination works have concentrated on the security of MANETs. A large portion of them manage avoidance and location ways to deal with battle individual getting out of hand hubs. In such manner, the viability of these methodologies gets to be weak when numerous noxious hubs plot together to start a community oriented assault, which may result to all the more crushing harms to the network. The absence of any framework included with the dynamic topology highlight of MANETs make these systems very powerless against steering assaults, for example, black hole, gray hole, wormhole a hub transmits a malignant show advising that it has the most brief way to the destination, with the objective of capturing messages.

Key Words: *CBDS, DSR, Gray hole attack, Black hole attack, malicious node, mobile ad hoc network (MANET).*

1 INTRODUCTION

MANET is point to point transmission type where a group of mobile nodes communicate with each other by wireless. MANET plays the role of both host and router. This forms wireless LAN where each node receives data and forwards packets to other nodes. However, the security of this particular network environment has many defects. In addition to the drawback of using radio wave to transmit in nature, there are still many problems, such as limited power, lower computing ability, and dynamic topology which make security of MANET lower than cable network. This uses open medium to communicate where attacker can easily overhear the transmitted messages. The design of previous routing protocol trusts completely that all nodes would transmit route request or data packets correctly, dynamic topology, without any central infrastructure, and lack of certification authorities make MANET are vulnerable to several types of attacks. Black hole is common attack which uses a malicious node to attract all packets (forged RREP) by claiming a fresh and shortest route to the destination and then discards. Gray hole attack, a variant of black hole that selectively discard and forwards data packets which passes through it. Cooperative black hole attacks is the technique where several malicious nodes cooperate with each other and form a group . The drawback is most of detecting methods fail and causes more immense harm to all network. Overcome by setting cooperate node with a stochastic adjacent node. By using the address of the adjacent node as the bait destination address, it baits malicious nodes to reply RREP and detects the malicious nodes by the proposed reverse tracing program. Finally the detected malicious node is listed in the black hole list and notices all other nodes in the network to stop any communication with them. As a result our proposal can reduce packets loss that cause by the malicious nodes and have better packet delivery ratio. The rest of the paper is organized as follows. we introduce the background and related work. The detecting and reverse tracing scheme that we proposed is presented in section. Next, in section we discuss and analysis the simulation results. Finally, the conclusion is depicted in section.

II. RELATED WORK

The security of MANETs deals with prevention and detection approaches to conflict individual misbehaving nodes. The efficiency of these approaches becomes weak when multiple malicious nodes collude together to initiate a collaborative attack, which results in devastating damages to the network. These attacks are highly vulnerable when there is no infrastructure added to the network topology. In blackhole attacks, a node transmits a malicious broadcast informing that it has the shortest path to the destination, with the goal of intercepting messages. In this case, a malicious node (so-called blackhole node) can attract all packets by using forged Route Reply (RREP) packet to falsely claim that “fake” shortest route to the destination and then discard these packets without forwarding them to the destination. In grayhole attacks, the node turns malicious only at a later time thus initially not recognized preventing a trust-based security solution from detecting its presence in the network. It then selectively discards/forwards the data packets when packets go through it.

III. PROPOSED SYSTEM

In this project, a method called "cooperative bait detection scheme" (CBDS) is proposed that effectively detects the malicious nodes that attempt to launch gray hole/collaborative black hole attacks. In this scheme, reverse tracing technique used to detect the malicious node. The address of an adjacent node is used as bait destination address to bait malicious nodes to send a reply RREP message. Nodes detected as malicious are kept in a blackhole list so that all other nodes that participate to the routing of the message are alerted to stop communicating with any node in that list. The advantage of CBDS is it integrates the proactive and reactive defense architectures to achieve the aforementioned goal.

Network Model :

It consider a dense multi hop static wireless mobile network deployed in the sensing field, it assume that each node has plenty of neighbors. When a node has packets to send to the destination, it launches the on-demand route discovery to find a route if there is not a recent route to a destination and the MAC layer provides the link quality estimation service.

Initial Bait: The goal of the bait phase is to entice a malicious node to send a reply RREP by sending the bait RREQ that it has used to advertise itself as having the shortest path to the node that detains the packets that were converted. To achieve this goal, the following method is designed to generate the destination address of the bait RREQ .The source node selects an adjacent node, within its one-hop neighborhood nodes and cooperates with this node by taking its address as the destination address of the bait RREQ. First, if the neighbor node had not launched a black hole attack, then after the source node had sent out the RREQ , there would be other nodes' reply RREP in addition to that of the neighbor node. This indicates that the malicious node existed in the reply routing. The reverse tracing program in the next step would be initiated in order to detect this route. If only the neighbor node had sent the reply RREP, it means that there was no other malicious node present in the network and that the CBDS had initiated the DSR route discovery phase

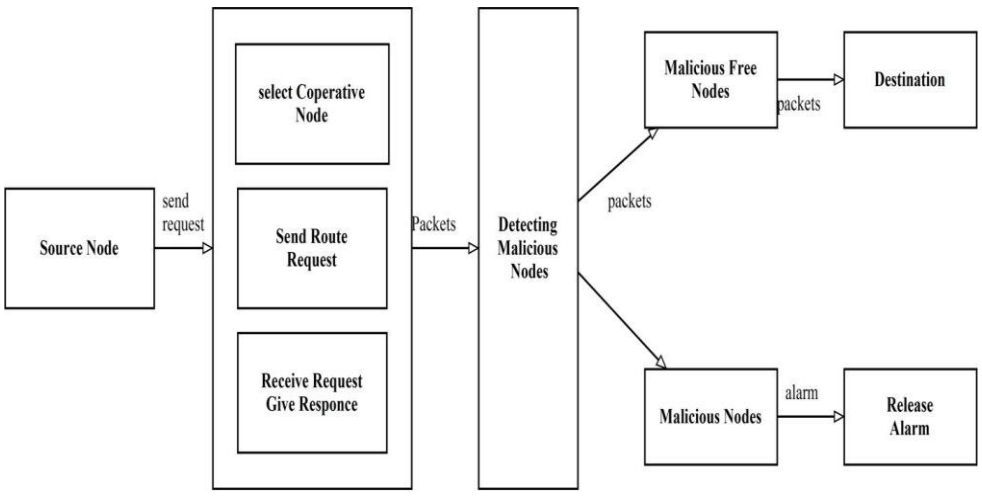
Initial Reverse Tracing: The reverse tracing program is used to detect the behaviors of malicious nodes through the route reply to the RREQ message. If a malicious node has received the RREQ, it will reply with a false RREP. Accordingly, the reverse tracing operation will be conducted for nodes receiving the RREP, with the goal to deduce the dubious path information and the temporarily trusted zone in the route. It should be emphasized that the CBDS is able to detect more than one malicious node simultaneously

When these nodes send reply RREPs..

Shifted to Reactive Defense Phase: When the route is established and if at the destination it is found that the packet delivery ratio significantly falls to the threshold, the detection scheme would be triggered again to detect for continuous maintenance and real-time reaction efficiency. The threshold is a varying value in the range [85%, 95%] that can be adjusted according to the current network efficiency. The initial threshold value is set to 90%. A threshold algorithm is considered that controls the time when the packet delivery ratio falls under the threshold. The network contains malicious node if the descending time is shortened. In that case, the threshold should be adjusted upward else lowering of threshold is done.

Security Module: It is going to use the key value of the message which is going to be sent and then it is added with the encrypted key sent from the source to destination through the intermediate node. Then decryption in the destination by subtracting the encrypted key from the message obtained and then the original message is obtained from the packets sent.

SYSTEM ARCHITECTURE



IV. SIMULATION

The Performance of Cooperative bait detection algorithm (CBDS) is evaluated through NS2 Network Simulator following are the performance metrics used.. A random network is deployed in an area 800m*800m is considered. Number of nodes is varied from 0 to 35. Initially the nodes are placed randomly in the specified area. The simulated traffic is CBR with TCP source and sink.

Table 1. Lists the simulation parameters used for network configuration

PARAMETERS	VALUES
Number of Nodes	35
Mac Protocol	802_11
Propagation Model	Two Ray Ground
Terrain Dimensions	800m*800m
Paket Size	512bits
Traffic	Constant Bit Rate (CBR)
Transport Protocol	TCP & UDP

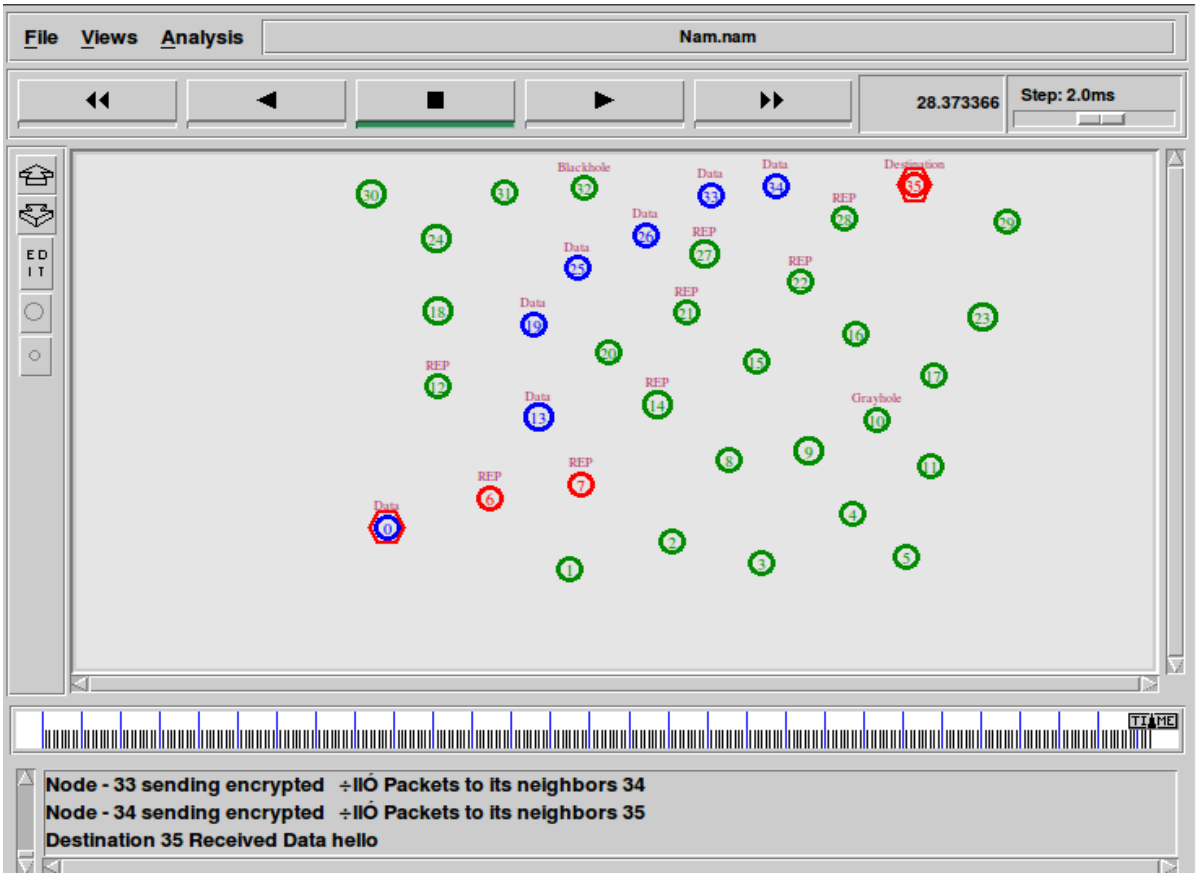


Figure 2: Network Animator Window

In fig2 we have shown the output traced on NAM. NAM stands for Network Animator .This NAM upon receiving the input file having the packet transmission events, draws the network events graphically. In this window we will show the animation of packet transfer, packet drops and mobility.

The overhead graph in Fig:3 is plotted for time v/s control overhead and the overhead is defined as the number of routing packets that is required to select in order to send the packets to one of the relay nodes with minimum number of packets. The control overhead also be named as Normalized Routing Load. We calculate the NRL by using the formula which states that the in NRL of any network and is defined as the ratio of number of routing packets that the source node is allowed to send the relay nodes to the number of routing packets that
has been received by the one of the nearest relay nodes. The formula can be simply given as

NRL= Number of routing packets /No.of received data packets

NRL must be as low as possible in order to decide the routing algorithm and overhead. It just decides the effective usage of network resource and the power consumption for transmission and recession.

The Average delay graph in Fig:4 is plotted for time v/s average delay where the delay is defined as the delay occurred in reaching the destination node of a coded packet between the slot allotted for both sender and receiver as the time elapses between them. The simple formula can be given as average end-to-end delay

AD= last packet transmission time/ number of packets received.

The packet delivery ratio graph in Fig:5 is plotted for time v/s packet delivery ratio and the PDR is defined as the ratio of number of packets sent over received. The formula can be given as:

PDR= packets received/ packets sent.

The Throughput graph in Fig: 6 is plotted for time v/s average throughput and the average through formulated can be given as

*Average throughput: no.of bytes received * 8 / (end time–start time)*

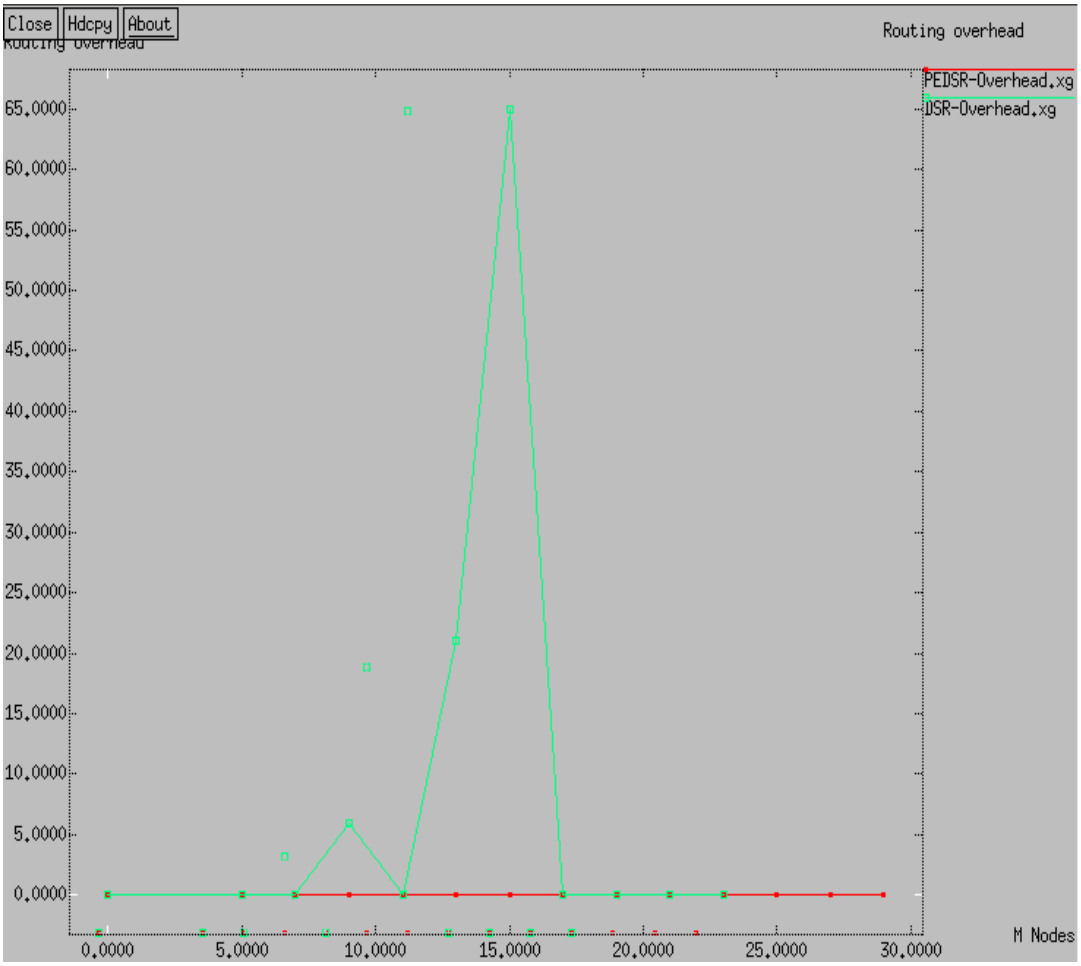


Fig.3. simulation time vs Overhead

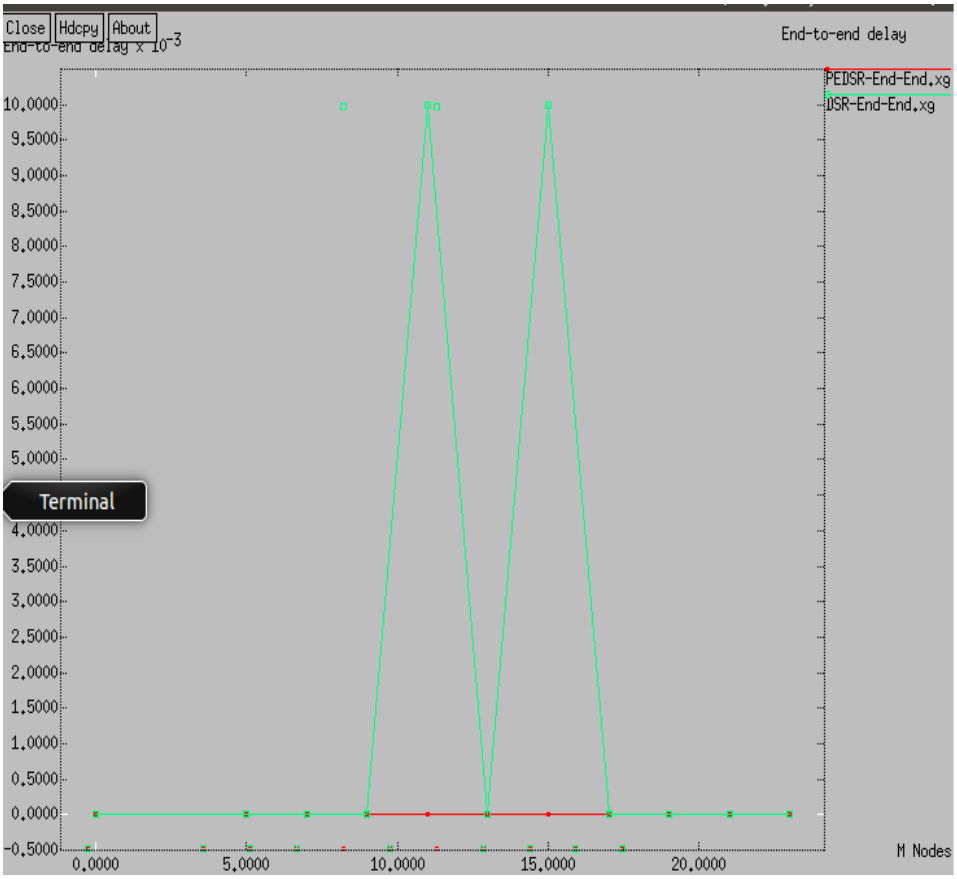


Fig.4. simulation time vs Average dealy

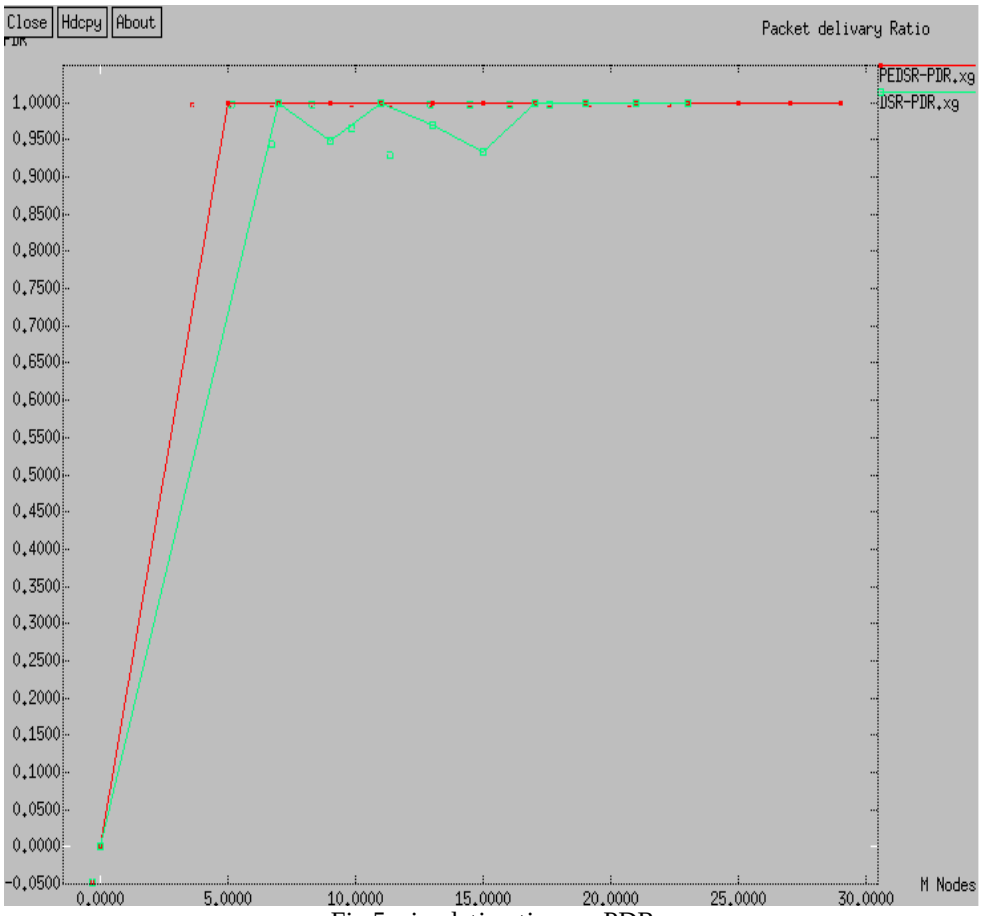


Fig.5. simulation time vs PDR

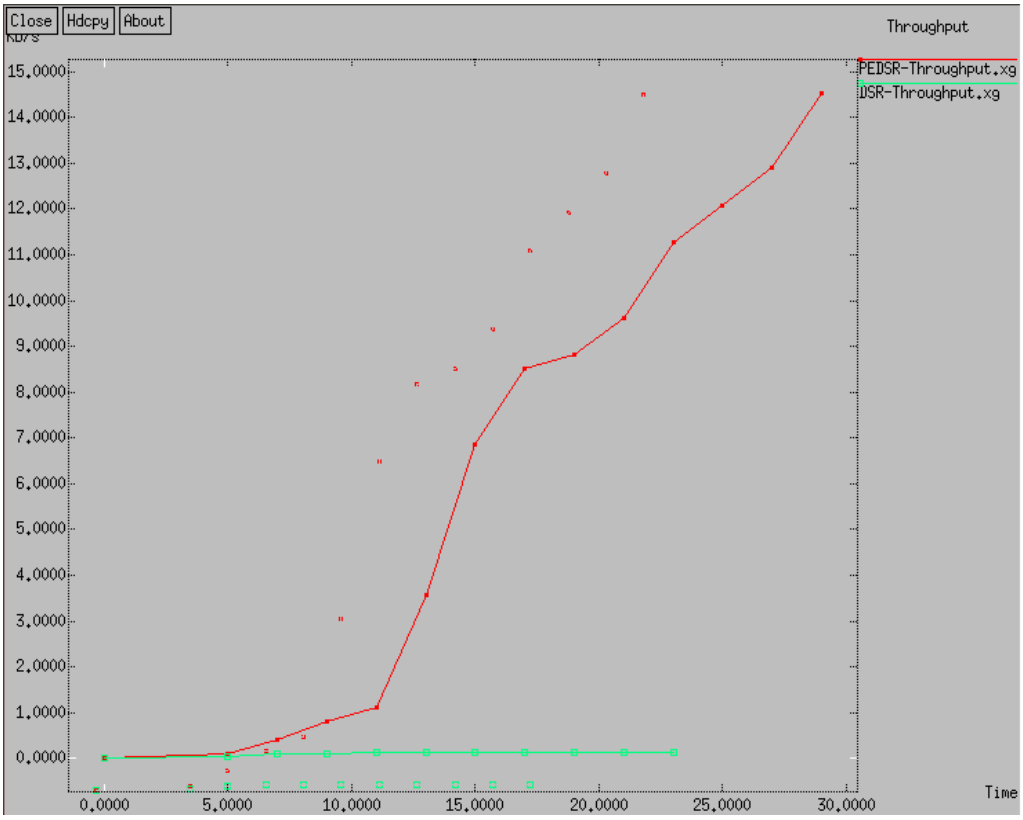


Fig.6.: Simulation time vs Average throughput.

CONCLUSION

The Cooperative bait detection scheme (CBDS) for detecting malicious nodes in MANETs under gray/collaborative black hole attacks. The address of source node selected to adjacent node used as bait destination address to bait malicious nodes to send a reply RREP message, and malicious nodes are detected using a reverse tracing technique. Any detected malicious node is kept in a black hole list so that all other nodes that participate to the routing of the message are alerted to stop communicating with any node in that list. Performance parameters such as routing overhead, packet delivery ratio, throughput and the end to end delay are carried out. Integration of The CBDS with other well-known message security schemes in order to construct a comprehensive routing framework to protect MANETs against miscreants.

REFERENCES

1 Po-Chun Tsou, Jian-Ming Chang, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai *,"* Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach. *Member, IEEE Mar 2015.*

2 .P.-C. Tsou, J.-M. Chang, H.-C. Chao, and J.-L. Chen, "CBDS: A cooperative bait detection scheme to prevent malicious node forMANET based on hybrid defense architecture," in *Proc. 2nd Intl. Conf. Wireless Commun., VITAE*, Chenai, India, Feb. 28–Mar., 03, 2011, pp. 1–5.

3. D. Johnson and D. Maltz, "Dynamic source routing in ad hoc wireless networks," *Mobile Comput.*, pp. 153–181, 1996.

4. I.Rubin, A. Behzad, R. Zhang, H. Luo, and E. Caballero, "TBONE: A mobile-backbone protocol for ad hoc wireless networks," in *Proc. IEEE Aerosp. Conf.*, 2002, vol. 6, pp. 2727–2740.

5. A. Baadache and A. Belmehdi, "Avoiding blackhole and cooperative blackhole attacks in wireless ad hoc networks," *Intl. J. Comput. Sci. Inf. Security*, vol. 7, no. 1, 2010.

6. K. Vishnu and A. J Paul, "Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks," *Int. J. Comput. Appl.*, vol. 1, no. 22, pp. 28–32, 2010.

7. K. Liu, D. Pramod, K. Varshney, and K. Balakrishnan, "An Acknowledgement based approach for the detection of routing misbehavior in MANETs," *IEEE Trans. Mobile Comput.*, vol. 6, no. 5, pp. 536–550, May 2007.

8. Y. Xue and K. Nahrstedt, "Providing fault-tolerant ad hoc routing service in adversarial environments," *Wireless Pers.Commun.*, vol. 29, pp. 367– 388, 2004.

9. W. Kozma and L. Lazos, "REAct: resource-efficient accountability for node misbehavior in ad hoc networks based on random audits," in *Proc. WiSec*, 2009, pp. 103–110.

10. W.Kozma and L. Lazos,"REAct:resource-efficient accountability for node misbehavior in ad hoc networks based on random audits," in *Proc. WiSec*, 2009, pp. 103– 110.