International Journal of Multidisciplinary Approach and Studies

ISSN NO:: 2348 – 537X

Collaborative Attack Detection in MANET using MD5 Grid Positioning BDS

Pooja Kundu* & Neeti Kashyap**

** M.Tech. Student, NCU (Formerly ITM University), Gurgaon.*
*** Assistant Professor, NCU (Formerly ITM University), Gurgaon.*

ABSTRACT:

Mobile ad hoc network (MANET) is in great demand now a days due to its special characteristics. Such networks are very useful in remote areas and in case of a disaster. Characteristics of MANET like dynamic topology, absence of centralized governing authority, limited battery power and bandwidth lead to several issues. Security is one of the major concerns in MANET because existing routing protocols for wireless networks do not provide a secure communication.. Various intrusion detection techniques are designed to be used to deal with the issue of malicious nodes in the network. Out of several attacks, collaborative attacks are hard to combat. Collaborative attacks are those attacks where more than one node participates in detection. In this paper, we have proposed a new algorithm MGBDS, which can be used to detect collaborative attacks. The proposed algorithm uses the grid positions of nodes with the help of grid positioning technique and MD5 algorithm to generate a message digest of destination node's address. The proposed algorithm in this paperis based on DSR (Dynamic source routing) protocol. Route request packet of DSR is modified to provide better performance as well as security towards collaborative attacks. MGBDS revamps the packet delivery ratio and a decrement in end to end delay is observed with a considerable percentage. The proposed work is analyzed by comparing it with collaborative bait detection scheme (CBDS) and DSR. Results of the simulation show that MGBDS outperforms the conventional algorithm DSR and CBDS with different thresholds.

Key words: MANET, intrusion detection, MD5, Grid-based, Black hole attack, collaborative attacks.

I. INTRODUCTION

Mobile ad hoc networks (MANETs) are popular and have application in various fields for communication. There significant progress in the market is because of their characteristics like no dependency on a centralized station, dynamic topology and ease to set up whenever required. Many situations arise when they are proven quite useful such as conference rooms, natural disasters, wars, etc. Although there are many advantages of these networks, there are some problems too. Nodes do not have boundaries to follow and can freely move inside and outside the network. There is a battery constraint so routing protocols are required to be power aware and energy efficient in routing. Existing routing protocols are not well equipped to detect security attack especially when attacks are collaborative in nature. When an attack is caused by insider node then it becomes hard to detect. Also when nodes show cooperation with other nodes which are their neighbours to attack the network (Collaborative attack) then it becomes really hard to detect which nodes are acting selfishly and which nodes are helping the selfish node.

In this paper a new algorithm called MGBDS is proposed which helps to detect collaborative attacks and black hole attack. Grid positions of the nodes are used to find out their actual position according to the virtual grids. MD5 algorithm is used to provide an additional layer of security. MD5 is well known for generating a message digest which is not so easily decoded. MGBDS is based on a one of the standard routing protocols, dynamic source routing (DSR) protocol and provides a modification of the existing algorithm.

The rest of the paper is divided into following sections. Section II introduces the related work in the field of detection of collaborative attack, DSR, MD5and grid positioning of nodes. Performance analysis and simulation results are conferred in section IV and in section V the conclusion of the paper is presented.

II. RELATED WORK

Attacks in MANETs can be differentiated into different types with different categories. Attacks in which network's traffic is compensated or is harmed are called active attacks. On the other hand, in passive attacks network is observed by the malicious node but is not distorted. A malicious node can act alone or in a group to affect the network and act selfishly. [1] Several techniques have been devised to protect the information flowing in the network. In this paper our major concern is towards detecting a multiple node attack, a collaborative black hole attack.

A. Black Hole Attack

Mobile ad hoc networks are prone to attack by malicious nodes. Existing routing protocols do not have any mechanism to find out whether the node is malicious or not. A node may start dropping packets when it is acting selfish to save its own battery power or does not want to relay data packets. [2] When malicious nodes are helped by other nodes then the attack is called a collaborative attack. In collaborative black hole attack, a node sends reply packet to the source node claiming that it can establish a route to the destination but in actual packets are being dropped by that node. The malicious node acts as a selfish node because it does not have enough battery power.[3]

In [4] a cooperative bait detection scheme (CBDS) is used to defend against collaborative black hole attack and gray hole attack. It combines both the approaches namely reactive and proactive mechanism to detect intrusion. The scheme works in three steps. DSR is used a base protocol. First and second steps are proactive. Malicious nodes are detected by the defence mechanism using bait node and reverse tracing step. An adjacent node's address is chosen as a bait address so that the malicious node replies to it and gets detected. In third step the algorithm shifts to reactive phase. A dynamic threshold value is maintained which is increased or decreased with respect to number of nodes causing attack or are potential attacker, malicious nodes. When the packet delivery ratio increases, threshold value is decremented by 0.01. The threshold value is incremented by 0.01 when the packet delivery ratio is decreased.

A hierarchical technique, HSRBH is proposed in [5] which use a secure routing scheme against the black hole attack. Nodes are arranged in a well-defined hierarchy in this technique and are also divided into groups. Each node is part of one of the four groups and each group has a group head. Concept of symmetric key is used to find a secure root, such that black hole

attack can't take place. Sharing of keys is done by group leaders in inter-groups and by neighbouring nodes in intra-groups.

Conventional routing protocols for wireless networks can be modified in order to become robust against attacks in the network, with scalability. GAODV [6] is such an attempt. AODV [7] protocol is modified to provide security against black hole and collaborative black hole attacks. Simulation results show that GAODV outperforms AODV in the presence of black hole attack. Another technique proposed in [8] by H. Weerasingheis an improvement over AODV protocol and prevents cooperative black hole attack. Two new parameters are added further request and further reply, which are modifications of route request and route reply of AODV. Also, a routing information table is maintained. Routing of packets is done by trusting the intermediate nodes for relaying packets to the destination, which have transferred the packets previously also. Routing information table contains information about which nodes have transferred the packets and which nodes have not done so. This information can be used to label a node as trustworthy.

B. Grid-based Routing

Many researchers are showing interest in finding the position of nodes in MANETs to route packets in the network. A node can have knowledge of its positions as well as of neighboring nodes. Node's location can be found out with the help of GPS with no extra cost. The position of node can be used for routing packets. In Grid-based routing protocols, a node is recognized by an identifier and its geographic location. When both the values are available, it makes a routing protocol to work efficiently. Network is divided into grids i.e. two-dimensional areas. [9][10]

Location of nodes can be finding out by global positioning system and with recent developments in technology, the hardware and software have become cheaper to detect location of nodes in MANET. EGBB-AODV [11] uses the grid based positioning of nodes to broadcast route request in the network. Flooding of packets and need of rebroadcasting of the request for nodes is prevented by this technique. Grids have gateway nodes which are responsible for rebroadcasting of route request packets.List of such gateway nodes is maintained dynamically at each node. The grids are fixed geographically and packets of route request are broadcasted grid by grid.

C. Security using Hash Key

Some research work has already been performed and discussed to make routing protocols secure with the help of hash key, message digest and other cryptography algorithms. Message digest (MD) with secret key is used in [12] to secure AODV (Ad hoc on-demand distance vector) routing protocol. It is shown that with the help of this scheme nodes start consuming lesser power and there is reduction of overhead. Messages are made secure to transmit in a network by using hash functions in [13]. Also denial of service attack is prevented.

Collaborative packet drop attacks are prevented by the technique proposed in [14] by using a hash based function. A DSR [15] protocol is used in this technique to find out the identity of nodes in the routing path by the source node. Random number and symmetric key are shared among the intermediate nodes by the source node. The procedure of auditing will start when there is a decrease in the packet delivery ratio.

Our proposed work is based on using message digest (MD5) and improving DSR. DSR is a reactive routing protocol which means that it finds the route to the destination when it is requested or required. In dynamic source routing (DSR)[15] protocol a source node broadcasts route request packet in the network. The nodes which have route to the destination replies with a RREP (route reply). Each data packet has an address to the destination in their header. DSR does not provide any mechanism for secure communication. The main concern is to find and establish a route with the help of intermediate nodes to the destination node. Route caches are maintained at each node. If a route is available in the cache then no update is required. Routing overhead is less in case of DSR. If there are many routes to the destination then one of them is chosen but there is no method to do so, any route can be selected and is used.

III. PROPOSED METHODOLOGY

In our proposed work, we are concerned about sending the data packets through a validated path that does not have any malicious nodes. Our work has merged MD5 (message digest) and grid–positioning technique.

- MD5
- Grid-positioning of nodes

The network is divided into virtual two-dimensional grids. Each node has 2-D coordinates in a plane which represents its position in the network. The coordinate value tells about the actual position of the node, which we will refer to as the grid value. When the source node is willing to find and establish a route to the destination and it needs help of intermediate nodes, it broadcasts the route request packet along with the grid value of the destination. Grid values can be found out with the help of GPS or any other such technique with minimum overhead.

A. MGBDS

Our proposed work, MGBDS (MD5 Grid-positioning Bait Detection Scheme) uses a neighbouring node's address as a bait to detect the malicious node. Bait is selected randomly. The bait chosen is a fake destination. A hash function is applied to the destination node's address and a digest is generated with the help of MD5. Hash function is chosen such that the rate of collision is less. The generated digest is added to the RREQ (route request) message. In this way we have proposed a modification of DSR protocol with a modified header of the packet. The mechanism of DSR-route request is modified to MGBDS-route request (MGBDS-RREQ). Figure-1 presents the format of secure MGBDS-RREQ message format. A message digest is added to the header along with the other fields.

MGBDS-RREQ is broadcasted in the network with a fake destination address. Nodes send route reply (RREP) if they have a route to the fake destination. A malicious node or a group of malicious nodes also send a RREP with no intention of sending the packet to the destination. Nodes cannot decrypt the digest of the destination. RREPs when reach the source node, the address is compared with the digest.

Type	Flags	Hop Count
Broadcast Id		
Source Address		
Destination Address		
Route List		
Message Digest Of Destination Address		

Fig.1.Secure MGBDS-RREQ Message Format

Path containing such nodes is not selected for sending the data packet. The node which claims to have a path to the destination is declared as malicious and is listed in a list of malicious nodes. All other nodes in the network are made informed about the new entry in the list of malicious nodes.

B. Algorithm

Working of our proposed scheme is explained in Figure 2. Network is divided into virtual grids and there are different nodes- source node, destination node, malicious nodes and intermediate nodes. Source node, S broadcasts the modified route request packet in the network. RREQ contains message digest of destination address, D and other information regarding the routing of the packet.

Each node maintains a route cache locally like conventional routing protocol, DSR. Nodes which have route to the intermediate nodes or to the destination node reply with a RREP (route reply) message. Malicious node, M also replies with RREP (route reply) by declaring that it can help to send the data packet and establish a route to the destination. The route with the minimum number of hops is chosen for transferring data packets to the destination node.The route cache maintained at each node is used. Malicious node fails to decode the message digest of the destination address. The only destination address known to the M is which is present in the encoded form. M claims about having a route to the destination but in actual it is sending a false reply. When S compares the destination address present in the route reply packet sent by the M with the destination address present at the cache, it declares the path a-b as malicious path because of unmatched addresses. Malicious path is not chosen as the route to the destination. Since we are using the concept of DSR, RREP contains the route through which the packet has come. So that route is not chosen to send data packets. On the other hand route p-q-r-s is chosen to send the data packets because it is the valid route and it passes the validation test by S.

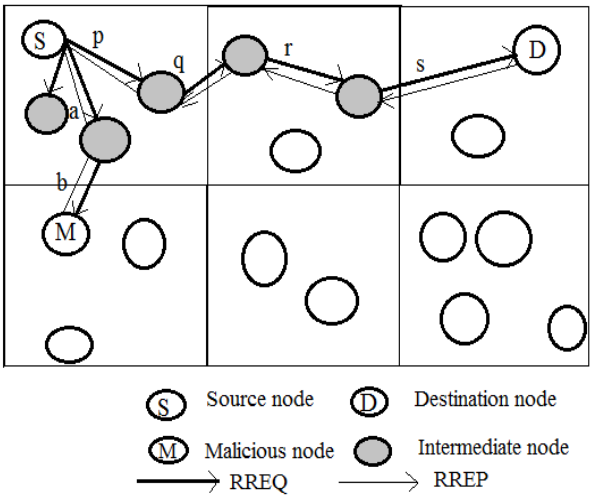

Fig.2. Working of MGBDS

Validation test is a crucial step in MGBDS scheme.MD5 helps to encrypt the destination address in such a way that none of the malicious node is able to decode it.

Algorithm of MGBDS is as follows:

1. Create grids virtually in the network area.

2. Create message digest of the randomly generated destination address.

3. Add the digest to the broadcasting RREQ.

4. Intermediate node when sends RREP, destination address in the RREP is compared with hashed destination address at source node.

5. If addresses match

then route is validated

6. Else

route has malicious nodes

route is discarded

IV. PERFORMANCE EVALUATION

Proposed algorithm results are compared with CBDS (with different thresholds) and DSR with respect to different performance metrics. Different scenarios are considered using MATLAB simulator. A 100*100 area having 100 nodes is simulated with 11mbps data rate. Malicious nodes ratio is taken from 0% to 40% and their mobility is varied to compare the throughput, PDR, End-to-end Delay and overhead of MGBDS with CBDS and DSR. Parameters chosen for simulation using MATLAB are shown in table 1.

TABLE I

Parameters	Values
Total number of nodes	100
Routing protocols	DSR, CBDS, MGBDS
Simulation area	100*100
Radio range	250 m
Channel data rate	11 mbps
Packet size	128 bytes
Malicious nodes	0-40 %
MAC protocol	IEEE 802.11
Traffic model	CBR
Pause time	0 s

A. **Performance Metrics**

Metrics which are used for analyzing and investigating the performance of the proposed work in comparison to CBDS and DSR are as follows:

1. **Packet Delivery Ratio**: PDR can be calculated is the ratio with the number of packets which have been originated by the source node as a numerator in the formula and the number of packets which have been actually received by the destination node as the denominator in the formula. Higher the PDR, higher is the efficiency and correctness of the algorithm.

2. **Routing Overhead**: It is calculated as the ratio of the control packets sent in the route to the data packets sent to the destination node by the source node.

3. **Average End-to-End Delay**: It is the average time taken by the data packet to travel from source node to the destination node is called the average delay. End-to-End delay should be minimized for effective communication.

4. **Throughput**: It helps to measure the success rate of the algorithm by calculating sum of the number of data packets received by the destination node within a specified time period. An algorithm is scalable and flexible if its throughput increases or is not decreased with the increment in the number of mobile nodes in the network.

B. **Simulation Results**

Figure 2 shows PDR for MGBDS with respect to CBDS with different thresholds and DSR. It is clear that MGBDS shows a great improvement in delivering a packet to the destination. When the mobility of the nodes increases the PDR is improved by 59% in case of MGBDS with respect to CBDS with threshold 95% and by 60% with respect to CBDS with threshold 85%. CBDS with threshold 85% shows worst performance in terms of PDR. In case of MGBDS, as the mobility of nodes increases the PDR increases with a great extent.

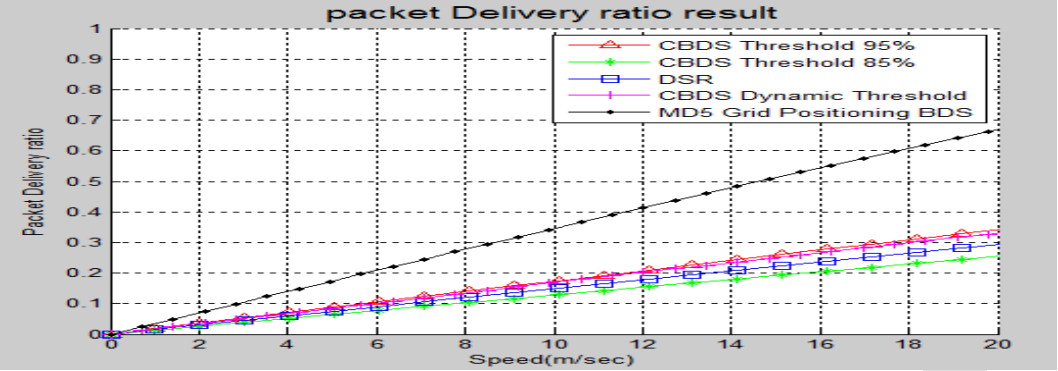

Fig. 2 Packet Delivery Ratio vs. speed of node

Figure 3 shows Routing Overhead vs. Malicious Nodes Ratio. With the increase in number of malicious node ratio to the number of the nodes in the network, the number of control packets has to be increased to detect the number of malicious nodes. In MGBDS, routing overhead remains low when the increase in the number of malicious nodes is simulated in lesser value but when the malicious nodes increases, the routing overhead also increases in comparison to CBDS and DSR. Even the CBDS algorithm with threshold 95% shows high routing overhead. The increase in routing overhead can be compensated by the increase in PDR. The trade-off is done between increased packet delivery ratio and increased routing overhead.

Figure 4 shows average end-to-end delay with 100 nodes in the network. MGBDS has lesser end-to-end delay as compared to CBDS with different thresholds. DSR is better in terms of delay than MGBDS until the number of nodes is low. As there is increment in the population of nodes, DSR starts showing increase in delay while transferring packets and MGBDS shows better performance than others.

Throughput of the proposed work is evaluated under two scenarios:

- **Varying number of nodes**: The consequence of varying the number of nodes on throughput is shown in Figure 5. It is illustrated that when the number of nodes grows MGBDS always shows higher throughput than the other schemes used for comparison, while DSR shows the lowest throughput. Scale on y-axis is n*10, where n is the number of nodes. For 10 nodes, CBDS and MGBDS show almost comparable throughput. But when the number of nodes is 50, MGBDS shows throughput of 98% whereas CBDS with threshold 95% shows throughput of 95%, CBDS with threshold 85% shows throughput of 88% and DSR shows throughput of 84%.

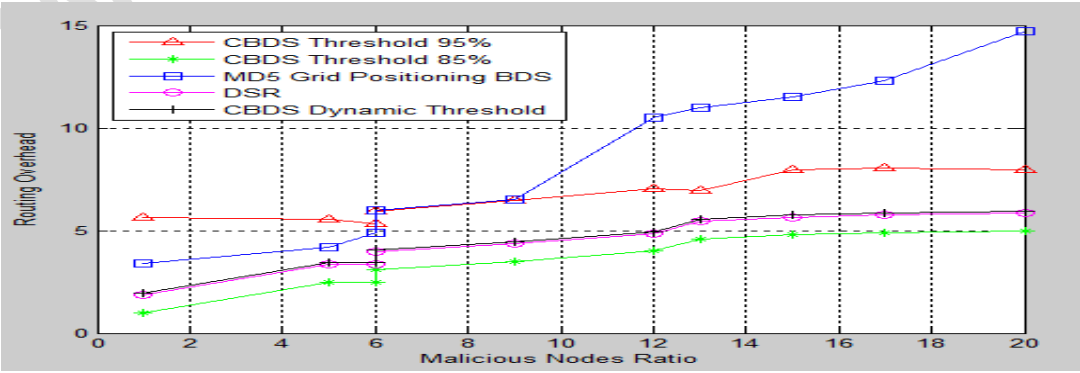

Fig. 3 Routing Overhead vs. Malicious Nodes Ratio

- Varying speed of nodes: In Figure 6 throughput with respect to varying speed of nodes is depicted. There is an improvement of 83% in throughput in comparison to CBDS 95% and improvement of 86% in comparison to CBDS 85%. As the speed of the nodes (in m/sec) increases, there is a marginal improvement in throughput of the proposed scheme, MGBDS compared to the throughput of CBDS and DSR. MGBDS shows throughput of 996 bits/sec when the speed of the mobile nodes in the network is 10 m/sec whereas CBDS with dynamic threshold shows throughput of 756 bits/sec and DSR shows throughput of 380 bits/sec at the same speed of nodes.

By analyzing the results, it is evident that MGBDS shows improvement in PDR, throughput and End-to-end Delay with routing-overhead trade-off. The proposed work outperforms CBDS with dynamic thresholds, CBDS with 85% threshold, CBDS with 95% threshold and conventional routing protocol DSR.

V. CONCLUSION

In MANET, nodes have limited radio frequency range. Nodes rely on each other so that they can transfer packets. There is no restriction on entry or exit from the network. Conventional routing protocols are more concerned for finding the path with minimum number of hops or a stable path rather than the security. Security is compromised. Security is a major concern in mobile ad hoc network. Packet delivery in such networks should be done in such a way that no malicious node can attack the network.

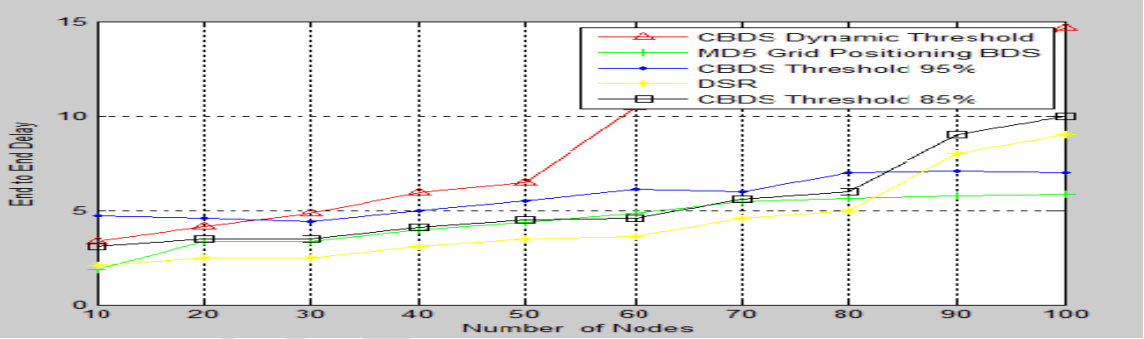

Fig.4 End-To-End Delay Vs. Number Of Nodes

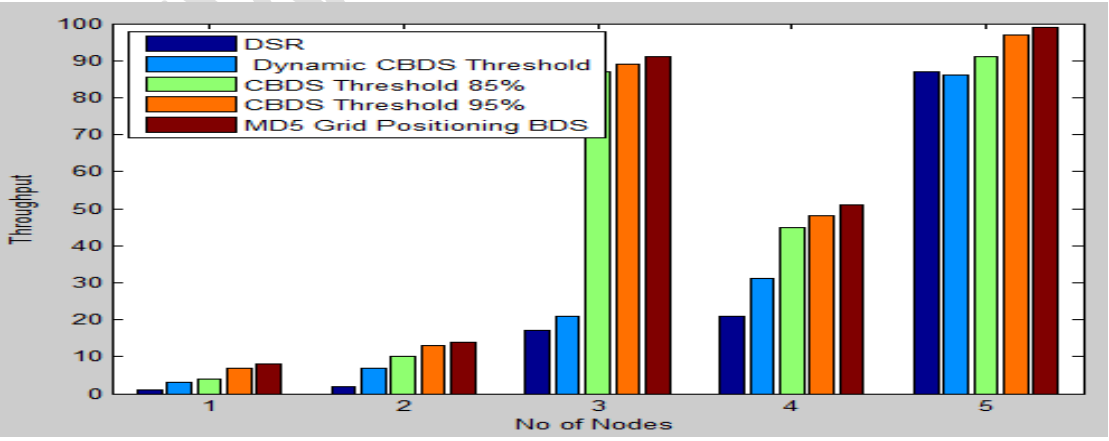

Fig.5: Throughput vs. number of mobile nodes

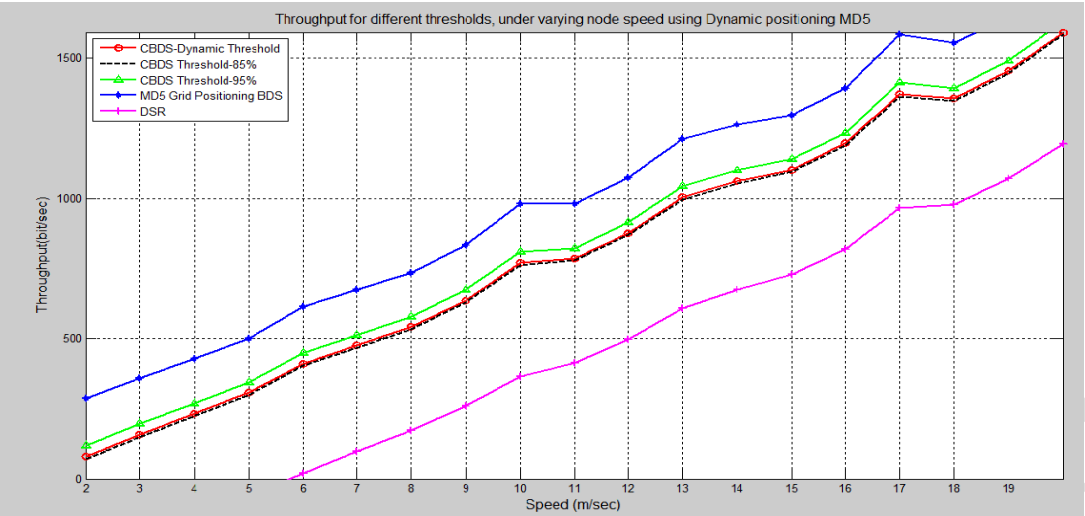

Fig.6: Throughput vs. varying node speed

A node can act as a malicious node depending upon its motive and resources left. There is risk of various types of attacks. There can be a single source attack or multiple nodes attack. Collaborative attacks are harder to detect and deal with because more than one node is involved.

The proposed algorithm (MGBDS) is a new intrusion detection scheme which uses the technique of MD5 and grid positions of nodes. Nodes attacking the network in collaboration are detected and the path suggested by these nodes is declared invalid for packet delivery. It is an improvement over bait detection scheme. DSR is chosen as a base routing algorithm. Our proposed algorithm is compared with DSR and CBDS. The results prove that our proposed algorithm shows better results as compared to CBDS with different thresholds and DSR. There is a trade-off between packet delivery ratio and routing overhead. Average throughput of MGBDS is 84.4% higher with respect to the CBDS. Also results show that MGBDS outperforms DSR in throughput and PDR.

REFERENCES

i. Kundu Pooja, Neeti Kashyap, and Neha Yadav. "Literature Survey on Intrusion Detection Systems in MANETs." Information Systems Design and Intelligent Applications. Springer India, 2016. 357-366.

ii. Kärpijoki, Vesa. "Security in ad hoc networks." Helsinki University of Technology (2000).

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

iv. Chang, Jian-Ming, et al. "Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach. "Systems Journal, IEEE 9.1 (2015): 65-75.

v. Yin, Jian, and Sanjay Kumar Madria. "A hierarchical secure routing protocol against black hole attacks in sensor networks." Sensor Networks, Ubiquitous, and Trustworthy Computing, 2006. IEEE International Conference on. Vol. 1. IEEE, 2006.

vi. Dhurandher, Sanjay Kumar, et al. "GAODV: A Modified AODV against single and collaborative Black Hole attacks in MANETs." Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on. IEEE, 2013.

vii. Perkins, C. (1997) Ad Hoc on Demand Distance Vector (AODV) Routing. IETF Internet Draft, Work in Progress.

viii. Weerasinghe, Hesiri, and Huirong Fu. "Preventing cooperative black hole attacks in mobile ad hoc networks: Simulation implementation and evaluation." Future generation communication and networking (fgcn 2007). Vol. 2. IEEE, 2007.

ix. Shahab Kamali, Jaroslav Opatrny, "A postition Based Ant Colony Routing Algorithm for Mobile Ad-hoc Netwroks," Academy Publisher, Journal of Networks, pp. VOL. 3,NO. 4, 2008.

x. W.-H. Liao, Y.-C. Tseng, J.-P. Sheu, "Grid: A Fully Location-Aware Routing Protocol for Mobile Ad Hoc Networks," Telecommunication Systems, vol. 18, pp. 37-60, 2001.

xi. Touzene, Abderezak, and Ishaq Al-Yahyai. "Performance Analysis of Grid Based AODV Routing Algorithm for AD Hoc Wireless Networks."International Journal of Communications, Network and System Sciences8.13 (2015): 523.

xii. Lakhtaria, Mr Kamaljit, et al. "Securing AODV for MANETs using Message Digest with Secret Key." Nettork Security & Its Applications (IJNSA) 1 (2009): 111-116.

xiii. Ravilla, Dilli, and Chandra Shekar Reddy Putta. "Enhancing the Security of MANETs using Hash Algorithms." Procedia Computer Science 54 (2015): 196-206.

xiv. Wang, Weichao, Bharat Bhargava, and Mark Linderman. "Defending against collaborative packet drop attacks on MANETs." 2nd International Workshop on Dependable Network Computing and Mobile Systems (DNCMS 2009)(in Conjunction with IEEE SRDS 2009), New York, USA. Vol. 27. 2009.

xv. Johnson DB, Maltz DA (1996) Dynamic Source Routing in Ad Hoc Wireless Networks. In: Imielinski T, Korth H (eds) Mobile Computing, vol 353. Kluwer Academic Publishers, pp 153–181.