Detecting and Preventing Attacks in MANET

Jasleen Arora
GTBKPC, Chhapianwali,
Malout, Punjab, India

Paramjeet Singh
GZSCETPTU campus,
Bathinda, Punjab, India

Shaveta Rani
GZSCETPTU campus,
Bathinda, Punjab, India

ABSTRACT
MANET network is a type of decentralized network and is high vulnerable network which requires secure communication.A significant security issue in manet is to protect the network layer from malicious nodes that misbhaves often to obtain the data that is not broadcasted for them i.e gray hole attacks aka selective forwarding attack that leads to denial of service attack(DoS) .In this paper The overall objective is to find the nodes which frequently misbehaves and based upon their miss ratio they will be eliminated from the network. The proposed strategy does not allow unauthorized nodes to access the data frames multicast by the initiators. The proposed strategy is designed and implemented in MATLAB using mathematics toolbox. The experimental results have shown significant improvement in detecting the malicious nodes.

General Terms
Attacks in MANET.

Keywords
Gray hole attack, Miss ratio, Multicasting

1. INTRODUCTION
MANETS (Mobile Adhoc Networks): Mobile means moving and adhoc means temporary without any infrastructure [8]. So, mobile adhoc network 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 [2]. The nodes themselves are responsible for creation, operation and maintenance of the network. Each node in the MANET is equipped with a wireless transmitter and receiver, with the aid of which it communicates with the other nodes in its wireless vicinity. The nodes which are not in wireless vicinity, communicate with each other hop by hop following a set of rules (routing protocol) for the hopping sequence to be followed [5]. **Characteristics of MANETs** [8] [5] [11]**:**

Cooperation: If source node and destination nodes are out of range of each other then the communication between them takes place with the cooperation of other nodes. This is known as mutihop communication.

Limited Bandwidth: The bandwidth available for mobile ad-hoc networks is generally very low.

Resource Constraints: MANETs have low power capacity, computational capacity, memory etc. In order to achieve reliable communication between nodes, these resource constraints make the task more enduring.

Dynamic Topology: In MANET, nodes are mobile nodes as a result the network topology may change rapidly and unpredictably and connectivity among the terminals may vary with time. The nodes dynamically establish routing among themselves as they move about, forming their own network on the fly.

Energy Constraint Operation: The nodes in MANET are portable devices and are dependent on batteries.

Lack of Fixed Infrastructure: In MANETs there is no fixed or central infrastructure as a result it is not possible to establish centralized authority to control the network. Due to the absence of centralized authority network management and security are scarcely applicable to MANETs.

Autonomous Terminal: In MANET, each mobile terminal is an autonomous node, which may function as both a host and a router. Besides the basic processing ability as a host, the mobile nodes can also perform switching functions as a router. So, endpoints and switches are indistinguishable in MANET

Distributed Operation: As there is no background network for the central control of the network operations, the control and management of the network is distributed among the terminals. The nodes involved in a MANET collaborate among themselves and each node acts as a relay as needed, to implement security and routing.

Fluctuating Link Capacity: In MANETs, one end-to-end path can be shared by several sessions. The channel over which the terminals communicate is subject to noise, fading, and interference, and has less bandwidth.

Lightweight Terminals: Nodes in MANET have less CPU processing capability, small memory size and low power storage.

Rest of the paper is Structured as follow, Section II discusses different types of attacks in Manet,

section III gives a brief literature review and current state of art related to prevention and detection attack.

section IV intriduces our proposed methodology to detect malacious nodes attack in Manet, section V present simulation results and performance evaluation of the method and finally section VI concludes the paper.

2. ATTACKS IN MANETS [5] [6] [12]:
Due to dynamic topology, distributed infrastructure less nature of MANETs and lack of centralized authority, ad- hoc networks are vulnerable to compromise and are suspectible to denial of service attacks(DoS) attacks. MANETs are susceptible to both passive and active malicious attackers. A passive attacker listens to the channel and may access the packet containing secret information. The action of active attacker includes injecting packets to invalid destinations in the network, deleting packets, modifying contents of the packet etc. [5].

Various types of attacks in MANETs are:

2.1.Flooding Attack [5]: The attacker node floods the network with bogus route creation packets to fake (non-existing) nodes or simply sends excessive route advertisements to the network. The purpose is to overwhelm the routing-protocol implementations, by creating enough

routes to prevent new routes from being created. Proactive routing protocols, as they create and maintain routes to all possible destinations are more vulnerable to this attack.

2.2. Sleep Deprivation Attack [5]: In this attack, the attacker keeps the resources of the specific nodes engaged in routing decisions by continually requesting for either existing or non-existing destinations. The nodes remain busy in processing and forwarding these packets thereby consuming batteries and bandwidth and obstructing the normal operation of the network.

2.3. Impersonation Attack [5]: In this attack, the attacker node impersonates a legitimate node, joins the network undetectably and starts sending false routing information.

2.4. Black Hole Attack [5] [6]: In this attack, a malicious node falsely claims as having shortest route to the destination with the aim to absorb the transmitted packets from source to the destination and thereby dropping the packets instead of forwarding them.

2.5. Node Isolation Attack [5]: In this attack, the attacker node isolates a given node from communicating with other nodes in the network by preventing link information of specific node from being spread to the whole network. Thus, other nodes will not be able to get link information to establish link to the target node and hence will not be able to send data.

2.6. Routing Table Poisoning Attack [5]: In this, the attacker node generates and sends fictitious traffic in order to create false entries in the routing tables of participating nodes. The attacker may also inject a RREQ packet with highest sequence number that causes all legitimate RREQ packets with lower sequence numbers to be deleted. This type of attack can result in selection of non optimal routes, creation of routing loops, bottlenecks etc.

2.7. Wormhole Attack [5] [6]: Wormhole attack involves cooperation between two attacker nodes. For example, consider the following network:

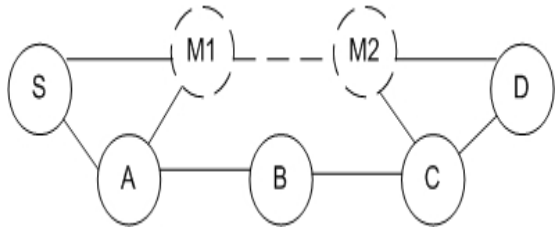

Figure 1: Example of Wormhole Attack.

The source S chooses to route the data packets by S, M1, M2, D instead of S, A, B, C, because it is the shorter route but in reality, attackers use a longer route S, M1, A, B, C, M2, D since that the link between M1 and M2 is unreal.

2.8. Location Disclosure Attack [5]: In this type of attack, the attacker is able to discover the location of anode and structure of a network by using traffic analysis techniques.

2.9. Gray Hole Attack [6]: In this type of attack, the attacker on intercepting packets forwards a portion of packets and blocks the others.

2.10. Message Tampering Attack [12]: In this type of attack, the attacker node alters the contents of the routing messages either by deleting some bytes or adding few bytes to it and forwards them with falsified information. This is an intentional malicious activity by the intermediate malicious nodes.

3. LITERATURE SURVEY

A. Boomarani Malany et al [1] have studied and compared various routing protocols for their better understanding and implementation. The comparison results are graphically presented and explained. Vishnu k. et al. [2] have proposed a technique for detection and removal of cooperative balck/gray hole attack in mobile adhoc networks. According to their technique, a backbone network of trusted nodes is established over the adhoc network. The source node periodically requests one of the backbone nodes for a restricted IP address. Whenever a node wants to make a transmission, it sends RREQ in search of destination as well as in search of restricted IP simultaneously. As the black/ gray hole nodes send RREP, they reply with RREP for the restricted IP also. If any node responds positively with RREP to restricted IP then malicious node detection procedure is invoked.

G.S. Mamatha et al. [3] have proposed a scheme to identify parallely different types of attacks in MANETs. Identification and prevention of malicious nodes causing packet dropping and message tampering attacks is done using a semantic security mechanism. The scheme is based on three modules: sender module, intermediate node module and receiver module. A simple acknowledgement approach with two way communication: a semantic security mechanism to generate hash code and principle of flow conservation to identify the threshold value for packet dropping is used. Anju K. Gupta et al. [4] have given an overview of a wide range of existing protocols focusing on their characteristics and functionality. The protocols are compared based on routing methodologies and information used to make routing decisions.

Sudhir Agarwal et al. [5] have presented an overview of routing protocols, the known routing attacks and the proposed countermeasures to these attacks. Ahmed Nabet et al. [6] have proposed an efficient secure routing protocol, ASRP, to ensure the routing security in adhoc networks. ASRP is used to provide powerful security extensions to reactive AODV protocol based on modified secure remote password protocol and Deffie- Hellman (DH) algorithm. Radhika Saini et al. [7] have presented the malicious behavior of the node and security solution to defend such behavior. Security solutions include cryptography, protocols, Intrusion Detection System (IDS) and Trusted Third Party (TTP).

Robinpreet Kaur et al. [8] have presented different routing protocols proposed in literature and comparison among these protocols through simulations based on certain parameters like throughput, routing overhead, average delay, packet delivery ratio and scalability. Rajib Das et al. [9] have proposed an algorithm for analyzing and improving the security of AODV protocol against black hole attack. According to proposed algorithm, an additional route to the intermediate node is established that replies the further request message to check whether the route from the intermediate node to the destination node exists or not. Shashank Khare et al. [10] have proposed a Secure Ad- hoc On- Demand Distance Vector routing protocol (SAODV) against black hole attack in MANETs. According to the proposed solution, the requesting node without sending the DATA packets to the reply node at once has to wait till other replies with next hop details from the other neighboring nodes is received. After receiving the first request it sets timer in the 'TimerExpiredTable', for collecting the further requests from

different nodes. It will store the 'sequence number', and the time at which the packet arrives, in a 'Collect Route Reply Table' (CRRT). The time for which every node will wait is proportional to its distance from the source. It calculates the 'timeout' value based on arriving time of the first route request. After the timeout value, it first checks in CRRT whether there is any repeated next hop node. If any repeated next hop node is present in the reply paths it assumes the paths are correct or the chance of malicious paths is limited.

Onkar V. Chandure et al. [11] have proposed a mechanism for the detection and prevention of gray hole attack in mobile adhoc network using AODV protocol. According to the proposed mechanism, each node in the network maintains DRI table containing entries for its neighboring nodes. Based on entries in DRI table, suspected node is checked using cooperative node and when level of suspicion about the suspected node increases, a Malicious Node Detection procedure is activated. Shobha Arya et al. [12] have proposed an algorithm for detecting malicious nodes in mobile adhoc networks. The proposed algorithm uses encryption, acknowledgement and principle of flow conversion approach for security against four attacks namely packet eavesdropping, message tampering, black hole attack and gray hole attack. Arnab Banerjee et al. [13] have proposed a routing scheme named Administrator and Trust Based Secure Routing (ATSR) in MANETs. The proposed scheme provides secure routing by using parameter, trust, an integer value, that helps in the selection of administrator inside the network for routing. It also implements message confidentiality and integrity.

4. PROPOSED ALGORITHM:

In the present work we have proposed a new algorithm which instead of detecting the attack it prevents the attack. Also in network lifetime some parameters are set-up based upon which we can check whether a given node i is malicious or not. Following are the proposed algorithm's steps.

Step1: Initialize the network

Step2: Base station multicast the data frames to some nodes.

Step3: Some nodes try to access the data frames

Step4: if the node i which is trying to access data is the one of the nodes to whom frames are multicast then hit is count else miss will be count.

Step5: after every 5 intervals we will check malicious nodes:

If node.miss_ratio>threshold

It is malicious will be removed from the network.

Else continue the step 2.

5. SIMULATION RESULT AND PERFORMANCE EVALUATION

To validate the proposed work we have select a node initiator i.e. base station which multicast data randomly to 5 nodes out of 15 fifteen. 4 different nodes try to access the packets. According to their behavior hit/miss is count. Figure 2 is showing the experimental set-up. It is showing the initial configuration of the network in which there is initiator, cluster head and 15 other nodes are shown. All 17 nodes are adhoc in nature and they continue change their position during the simulation of the proposed scenario.

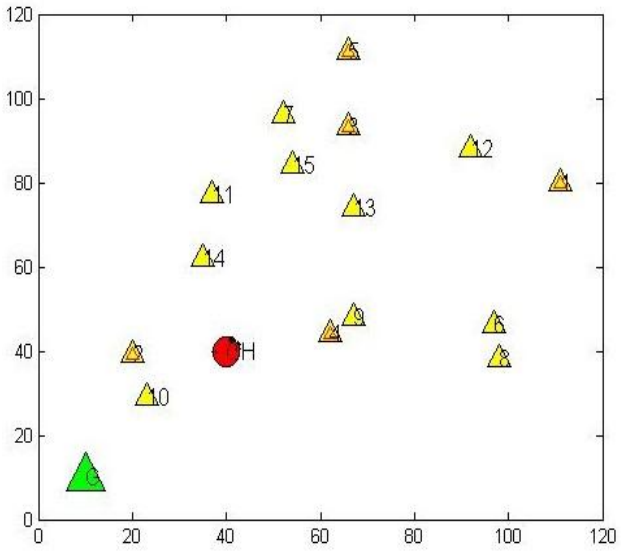

Figure 2: Initial configuration of the Experimental set-up

Figure 3 is showing the network configuration when initiator multicast data to some nodes in the network. Initiator sends data firstly to the cluster head then cluster head is responsible for sending the data to the other nodes.

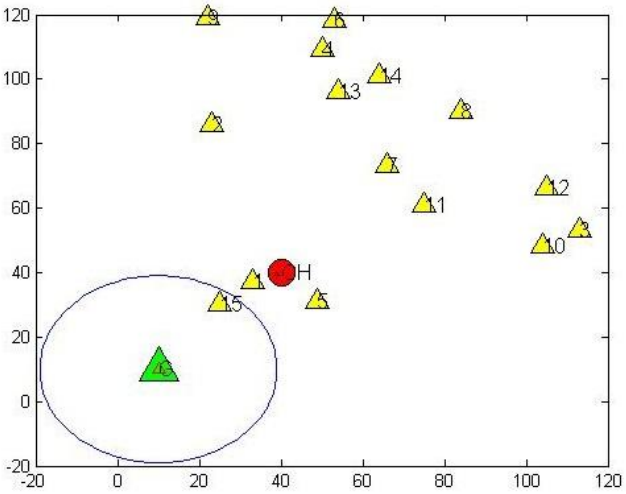

Figure 3: Multicasting data to Adhoc nodes

Figure 4 is showing the network configuration when authorized nodes send acknowledgement to cluster head that they successfully receives the sent data.

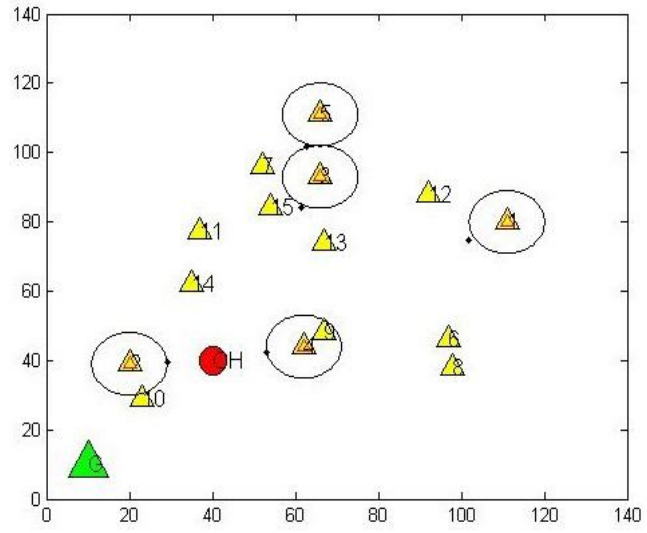

Figure 4: Authorized nodes sending acknowledgement to initiator

Performance evaluation

We have run the simulation 20 times with 10 frames multicasting at each round. We have randomly select authorized and attacker nodes and note down their overall hit ratio and miss ratio using the gap between total hits and total tries. By selecting the threshold value as intrusion detector function. Table 1 is showing the miss evaluation of the 15 nodes that are part of the network. Based upon the miss ratio, some nodes has been declared as malicious.

Table 1 Malicious evaluation

Node	Misses	Miss ratio	Malicious
1	20	0.1	No
2	30	0.15	No
3	35	0.17	No
4	15	0.07	No
5	15	0.7	Yes
6	0	0	No
7	45	0.22	Yes
8	0	0	No
9	0	0	No
10	74	0.37	Yes
11	41	0.2	Yes
12	20	0.1	No
13	45	0.22	Yes
14	3	0.01	No
15	21	0.1	No

Figure 5 is showing the misses evaluation. It is clearly shown the misses of each node is almost different and even some nodes are even has not tried even a once to access non-authorized data. Number of misses lies between 0 to 200 as maximum tries are 200. It is found that the node 10 has attempted quite more un-authorized accesses.

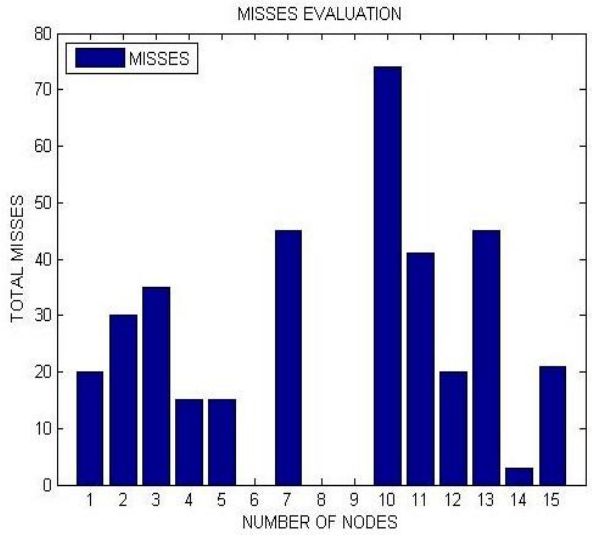

Figure 5: Misses evaluation

Figure 6 is showing the miss ratio evaluation. Each node having miss ration more than or equal to 2 is declared as malicious.

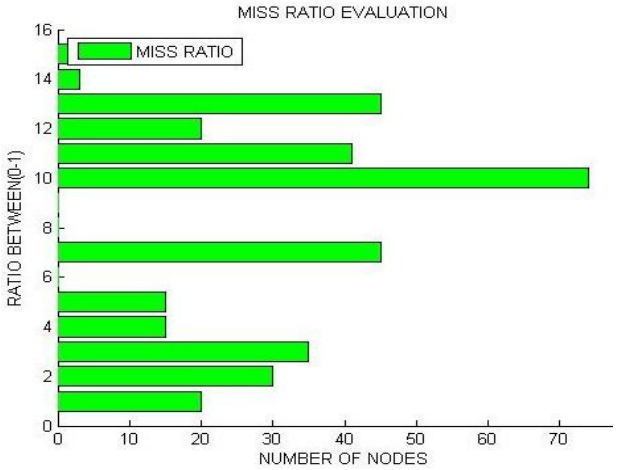

Figure 5: Miss Ratio evaluation

Simulation Parameters

Following parameters are used for experimental setup.

Table No. 2 Simulation Parameters.

SR. NO.	**SIMULATION PARAMETER**	**VALUE**
1	Simulator	MATLAB
2	Protocol	AODV
3	Simulation Time	Depends On Packet Transferred
4	No. of Nodes	15
5	Max. No. Of attacker nodes in one simulation	5
6	Simulation area	140*140 (Varies)
7	Pause	1 Sec.

6. CONCLUSION AND FUTURE WORK

By conducting the survey and evaluating the problems of existing attack preventing techniques it has been found that most of the work done so far is on detecting the attacks not preventing the attacks. However some of the researchers have

proposed quite efficient techniques to handle different kind of attacks. The proposed strategy has ability to prevent grayhole attack. The developed algorithm will allow only genuine nodes to access the data frames. By conducting the suitable experiments we have seen that the proposed algorithm has successfully detect the intruders and based upon their miss ration it has also declare them as malicious or genuine node. However in this research work only grayhole attack is considered in near future some more attacks will be considered for accurately justify the proposed work for different kind of voices. Even selecting the threshold is an critical task, so in future some systematic way other than used will be taken under consideration.

7. ACKNOWLEDGMENT:

I would like to thank my guide Prof (Dr.) Paramjeet Singh and Prof (Dr.) Mrs. Shaveta Rani for their consistent guidance and support in the accomplishment of this research work entitled "Prevention and Detection of Attacks in Manet". I am also thankful to my family and friends who keep encouraging me to complete my work in time.

8. REFERENCES:

[1] A. Boomarani Malany, V. R. Sarma Dhulipala and RM. Chandrasekaran, "Throughput and Delay Comparison of MANET Routing Protocols", Int. J. Open Problems Compt. Math, Vol. 2, No. 3, ISSN 1998-6262, September 2009.

[2] Vishnu K and Amos J Paul, "Detection and Removal of Cooperative Black/Gray Hole Attack in Mobile ADHOC Networks", International Journal of Computer Applications, Vol. 1, No. 22, 2010.

[3] G.S. Mamatha and Dr. S. C. Sharma, "A Highly Secured Approach against Attacks in MANETs", International Journal of Computer Theory and Engineering, Vol. 2, No. 5, October 2010.

[4] Anuj K. Gupta, Harsh Sadawarti and Anil K. Verma, "Review of Various Routing Protocols in MANETs", International Journal of Information and Electronics Engineering, Vol. 1, No. 3, November 2011.

[5] Sudhir Agrawal, Sanjeev Jain and Sanjeev Sharma, "A Survey of Routing Attacks and Security Measures in Mobile Ad-hoc Networks", Journal of Computing, Vol. 3, ISSN 2151-9617, January 2011.

[6] Ahmed Nabet, Rida Khatoun, Lyes Khoukhi, Juliette Dromard and Dominique Gaiti, "Towards Secure Route Discovery Protocol in MANET", Conference Publication, August 2011.

[7] Radhika Saini and Manju Khari, "Defining Malicious Behaviour of a Node and its Defensive Methods in Ad Hoc Networks", International Journal of Computer Applications, Vol. 20, No. 4, April 2011.

[8] Robinpreet Kaur and Mritunjay Kumar Rai, "A Novel Review on Routing Protocols in MANETs", Undergraduate Academic Research Journal, Vol. 1, ISSN: 2278-1129, 2012.

[9] Rajib Das, Dr. Bipul Syam Purkayastha and Dr. Prodipto Das, "Security Measures for Black Hole Attack in MANET: An Approach", International Journal of Engineering Science and Technology, Vol. 3, No. 4, pp-2832-2838, ISSN: 0975-5462, April 2012.

[10] Shashank Khare, Manish Sharma, Namrata Dixit and Sumit Agarwal, "Security in Routing Protocol to Avoid Threat of Black Hole Attack in MANET", VSRD International Journal of Electrical, Electronics and Communication Engineering, Vol. 2 (6), pp- 385-390, ISSN: 2231-3346, 2012.

[11] Onkar V. Chandure and V.T. Gaikwad, "Detection and Prevention of Gray Hole Attack in Mobile Ad- Hoc Network using AODV Routing Protocol", International Journal of Computer Applications, Vol. 41, No.5, ISSN: 0975- 8887, March 2012.

[12] Shobha Arya and Chandrakala Arya, "Malicious Node Detection in Mobile Ad- Hoc Networks", Journal of Information Operations Management, Vol. 3, pp- 210-212, ISSN: 0976-7754, January 2012.

[13] Arnab Banerjee, Dipayan Bose, Aniruddha Bhattacharyya, Himadri Nath Saha and Dr. Debika Bhattacharyya, "Administrator and Trust Based Secure Routing in MANET", International Conference on Advances in Mobile Network, Communication and its Applications, 2012.