Detection and Isolation Technique for Black Hole Attack in Mobile Ad Hoc Networks

Navjotpreet Kaur[1], Er. Maninder Kaur[2]
[1]*Research Scholar,* [2]*Assistant Professor*
[12]*Doaba Institute of Engineering & Technology, Kharar, Punjab*

Abstract- A wireless mobile network comprises of countless spread over a particular territory where we need to take care of at the progressions going ahead there. A mobile hub, for the most part, comprises of mobiles, actuators, memory, a processor and they do have correspondence capacity. These sorts of networks are much powerless against security attacks. Many kinds of active and passive attacks are conceivable in the mobile network. Among all the conceivable active attacks, sinkhole attack is the most widely recognized and destructive attack. This attack debases network execution and prompts denial of service attack. The attack is triggered by the malicious hub which is available in the network. In this work, a novel strategy has been proposed to recognize and disengage malicious nodes from the network which are in charge of triggering the attack. The novel procedure is based on blacklist technique and clustering technique. The exploratory results will demonstrate that proposed strategy detects and separate the malicious nodes from the network proficiently. It will enhance network effectiveness as far as bundle misfortune, defer and expand throughput of the network. NS2 simulator instrument will be utilized as a part of it.

I. INTRODUCTION

The collection of small mobiles that involve computing elements as well is known as the wireless mobile network. The cost of these mobile nodes is very less and they also have very limited amount of energy within them. Thus, the processing capability of these nodes is very less. There are innumerable nodes present within these networks and they are highly distributed. The deployment of such networks is done within various applications [1]. These networks monitor the system or surroundings by measuring physical parameters, for example, moistness, weight and temperature. MANETSs are most appropriate for applications like natural life checking, military order, shrewd interchanges, modern quality control, and perception of basic bases, brilliant structures, circulated apply autonomy, movement observing, inspecting human heart rates, and so forth. [2]. In order to provide energy from a source the battery power is utilized within the mobile nodes. For providing energy, the battery is utilized as an object. However, these batteries cannot be replaced or changed once they run out of energy. This is due to the deployment of mobile nodes in mostly such places in which human reach is almost impossible. Thus, here the proper utilization of energy of batteries is the major concern. For this, various strategies are proposed which can increase the lifetime of the mobile nodes. These systems must also ensure the reduction of throughput or the delay occurring within the network

A. Attacks in MANETs:

Security issue is the main concern in mobile network. These attacks are as follow:

a. **Worm hole Attack:** In this a malicious node, records packets at a particular location in the network and tunnels them to another location. When the control messages are routing are tunneled it create disrupted. It is a network layer attack. The solution to this problem is monitoring the network and flexible routing schemes.
b. **Black hole Attack:** In this attack malicious node captures and reprograms a set of nodes in the network and blocks the packets are received instead of forwarding them towards the base station. Any packet that enters into the black hole region is captured by the malicious node and never reaches the destination node. [4,5]
c. **Denial of Service Attack:** This malicious node in this attack hits on the accessibility of a node and all nodes in the whole of the network. Aim of this attack is to block the services of the mobile nodes [4, 5]. The attacker generally uses battery absorption method and radio signal jamming.
d. **Byzantine Attack:** In this attack, an intermediate compromised node is used for carrying out attacks, some of which are created collision forwarding packets on non-optimal paths, routing loops, and dropping packets selectively which give out interruption or dreadful conditions of the routing services [5].
e. **Jamming:** In this attack the radio frequencies are inferred that is used by the mobile node. Attacker monitors initially in order to verify frequency at which destination node is getting signal from the sender. Attacker transmits the signal on that frequency and powerful enough to disrupt the network [6].
f. **Collision Attack**: In this attack, an attacker attempts to send the data on the same frequency with which other nodes are transmitting the data, so that the packets collide and retransmission is required [7]s.
g. **Man- in- the- middle attack:** In this attack, an attacker sits in between the sender and receiver node. The information being passed by the sender is captured by the attacker sitting

in the middle. In some instances, attacker might masquerade as the original sender to communicate with receiver or masquerade as the receiver to reply to the sender.

h. **Misdirectional Attack:** The content packet is led to a different destination than the original place in this type of attack. The misguidance of the packet is done here by the attacker. The system will degrade due to the increase in time in which the packet should be received. There is a presence of the selfish nodes in the network which misdirect the packets and there is a decrease in the efficiency of the complete system due to this. [1, 2, 7, 8].

i. **Node Replication attack:** The attacker tries to add a malicious node in the network by assigning the malicious node the same Node ID of some existing node in the network.

B. Black Hole Attack in AODV protocol

AODV is an important on-demand routing protocol that creates routes only when desired by the source node. In this process the intermediate node can reply to the RREQ packet only if it has a fresh enough route to the destination [4]. Once the RREQ reaches the destination or an intermediate node with a fresh enough route, the destination or intermediate node responds by unicasting a route reply (RREP) packet back to the neighbor from which it first received the RREQ. After selecting and establishing a route, it is maintained by a route maintenance procedure until either the destination becomes inaccessible along every path from the source or the route is no longer desired. A RERR (Route Errors) message is used to notify other nodes that the loss of that link has occurred. In AODV, the sequence number is used to determine the freshness of routing information contained in the message from the originating node. When generating RREP message, a destination node compares its current sequence number, and the sequence number in the RREQ packet plus one, and then selects the larger one as RREPs sequence number [5]. Upon receiving a number of RREP, the source node selects the one with greatest sequence number in order to construct a route. But, in the presence of black hole when a source node broadcasts the RREQ message for any destination, the black hole node immediately responds with an RREP message that includes the highest sequence number and this message is perceived as if it is coming from the destination or from a node which has a fresh enough route to the destination. The source assumes that the destination is behind the black hole and discards the other RREP packets coming from the other nodes. The source then starts to send out its packets to the black hole trusting that these packets will reach the destination [6]. Thus the black hole will attract all the packets from the source and instead of forwarding those packets to the destination it will simply discard those. Thus the packets attracted by the black hole node will not reach the destination.

II. LITERATURE SURVEY

Juby Joseph et al [1]," Misdirection Attack in MANETS Due to Selfish Nodes; Detection and Suppression using Longer Path Protocol", 2014 There is a lot of use of the wireless mobile networks in fields which have consumers and in industrial and defense areas also it has its involvements. The networks are vulnerable and prone to the attacks of outsiders. It is very commonly found that the attackers attack the security of the networks. The wireless mobile networks are also been attacked by various kinds of outsiders in different ways. The Denial of Service (DoS) attacks have another kind of attack known as misdirectional attacks which mislead the packets of the network. There are various selfish nodes present in the network which perform such activities and they decrease the efficiency of the network. The messages are not forwarded to the intended nodes due to the unexpected behaviors of some nodes.

Dr. G. Padmavathi et.al [2] introduced in their paper "A survey of attacks, Security Mechanisms and Challenges in Wireless Mobile Networks", the security goals for mobile networks, various attacks in wireless mobile networks and the security mechanism related to different attacks. The paper also presented the challenges of mobile networks.

Maan younis Abdullah et al [8], "Wireless Mobile Networks Misdirection Attacker Challenges and Solutions", 2008 There are various challenges that a wireless mobile network faces due to the misdirectional attacks. This type of attack does not allow the packets to be received by the destination address. The packets are transferred to the other location. There is also another type of way of attacking the wireless networks by sending number of useless packets to the network. this acquires a lot of energy and the overall efficiency of the network reduces a lot. The latency also increases when the packets are misdirected. The intruder considers it as his main objective of not allowing the packets to be received on the other end or the destination. The message of its own is send by the attacker on the other end. This is done by avoiding to be noticed by the network. there are solutions provided to these type of problems. The solutions have prevented the attacks to a greater extent and have helped in maintaining the efficiency of the networks.

Roshan Singh Sachan et al [9], "Misdirection Attack in MANETS: Topological Analysis and an Algorithm for Delay and Throughput Prediction", 2012 There are various types of attack that the wireless mobile network faces. There are a lot of instances that have been occurring in which the detection of the attack of DoS and misdirection attacks has not been possible. The node in misled in such a way that the node reaches to any other node except for the destination node. The degradation of performance occurs due to such cases. Here in the article such an attack has been proposed on the topological analysis of the wireless network. An algorithm is proposed which will provide a help for the assistance in throughput and

delaying of the packets**.** Better performance is observed in the tree network topology than in the mesh topology network.

Ju young Kim et.al [7] presented in their paper "A Review of the Vulnerabilities and Attacks for Wireless Mobile Networks" about the investigation of the distinctive vulnerabilities, threats and attacks for Wireless Mobile Networks. Viable administration of the threats connected with remote innovation requires a sound and through appraisal of danger given nature and advancement of an arrangement to relieve distinguished threats. An investigation to network supervisors comprehend and evaluate the different threats connected with the utilization of remote innovation and various accessible answers for countering those threats are talked about. Remote Mobile Networks give a various chances to expanding profitability and minimizing costs. It gives huge focal points to numerous applications that would not have been feasible for the past. The diverse vulnerabilities, threats and attacks that could place MANETSs in a crucial or basic circumstance have been recognized and talked about in their paper. The diverse classifications for these threats are characterized to distinguish a conceivable countermeasure plan pertinent for every risk characterization.

Kalpana Sharma and M K Ghose [4] introduced in their paper "**Wireless Mobile Networks: An Overview on its Security Threats"** that the issue of security is because of the wireless nature of the mobile organizes and obliged nature of resources on the wireless mobile nodes, which implies that security models utilized for conventional wireless systems are not practical. Moreover, wireless mobile systems have an extra helplessness since nodes are regularly set in an unfriendly or risky environment where they are not physically secured. They have introduced the summery of the MANETSs threats influencing diverse layers alongside their protection system. They infer that the guard system introduced just gives guidelines about the MANETS security threats; the definite arrangement relies on upon the sort of application the MANETS is sent for. There are numerous security systems which are utilized as a part of "layer-by-layer" premise as a security tool. As of late specialists are going for integrated framework for security system as opposed to focusing on various layers freely. Through this paper they have attempted to introduce the most widely recognized security threats in different layers and their most likely arrangement.

III. RESEARCH METHODOLOGY

The wireless mobile networks is the decentralized type of network due to which malicious nodes enter the network which trigger various type of active and passive attacks. The blackhole attack is the active type of attack which is triggered by the malicious nodes. The proposed technique is based on to detect malicious nodes which are responsible to trigger blackhole attack in the network. The proposed technique consists of following steps for the detection of malicious nodes :-

1. In the first step, the source node will flood the route request packets in the network. The source node will start the timer to check the time for receiving route reply packets
2. The source check each route reply packet and check which node revert in minimum time with the exceptional high sequence number
3. The node which reply back with the exception high sequence number in minimum amount of time will be put into the blacklist
4. The source will check each node that how many number of packets are re-transmitted by the each node in the network
5. The rating is assigned to each node in the network and node which has maximum trust values will be the most trusted or legitimate node
6. The cluster are formed in the network and node which has maximum trust value will be selected as cluster head and all network data will be transmitted through cluster heads

Algorithms

Step 1: Get current time (Time at which route request message is sent)

Step 2: Get waiting time (WT).

Step 3: While (RT<=WT).

Verification of route reply messages are done by various step verifications.

Step A: Check for malicious node.

i. After getting route replies from intermediate nodes, check the malicious_table for malicious node_id which is formed on the basis of previous traffic.

ii. If node_id is matched with the malicious_table, then discard the route reply.

iii. If node_id is not found in the malicious_table, then go to step ii.

Step B: Check the distance_time value.

i. If distance_time value matches with expected hop count value, then store that value in dt_table and go to step C.

ii. Repeat step2

Step C: Divide the whole network into clusters and select cluster head in each cluster

Step D: Continue the cluster head to cluster head communication in the network.

IV. RESULTS AND DISCUSSION

The proposed technique is implemented in NS2 and compared with the existing techniques in terms of various parameters

Parameter	Value
Terrain Area	800 m x 800 m
Simulation Time	50 s
MAC Type	802.11
Application Traffic	CBR
Routing Protocol	AODV

Data Payload	512 Bytes/Packet
Pause Time	2.0 s
Number of Nodes	19
Number of Sources	1
No. of Adversaries	1 to 3

TABLE 1 Simulation Parameters

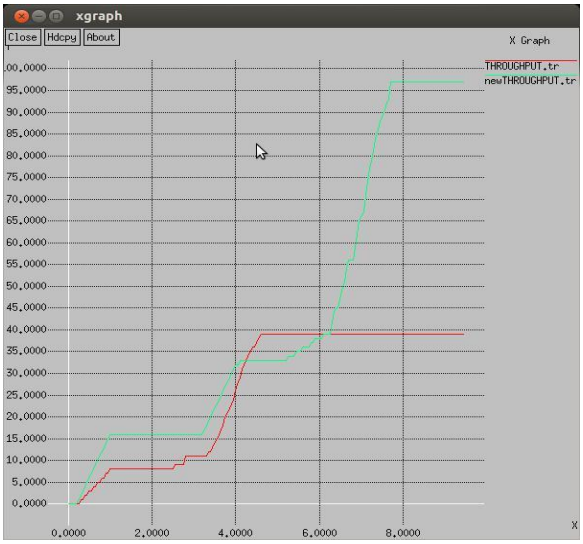

Fig.1: Throughput graph

In above figure 1 red line shows old throughput and green line show new throughput. X-axis show time and y axis shows packets. It concluded that new technique has more throughputs as compared to old technique.

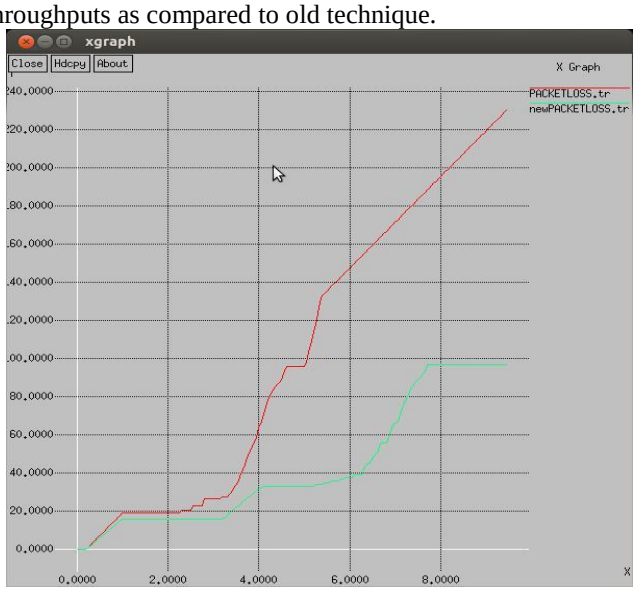

Fig.2: Packet loss Comparison

In above figure 2, red line shows packet loss and green line show new packet loss. X-axis show time and y axis shows packets. It concluded that new technique has less packet loss as compare to new technique. It proves that new technique is better than old technique.

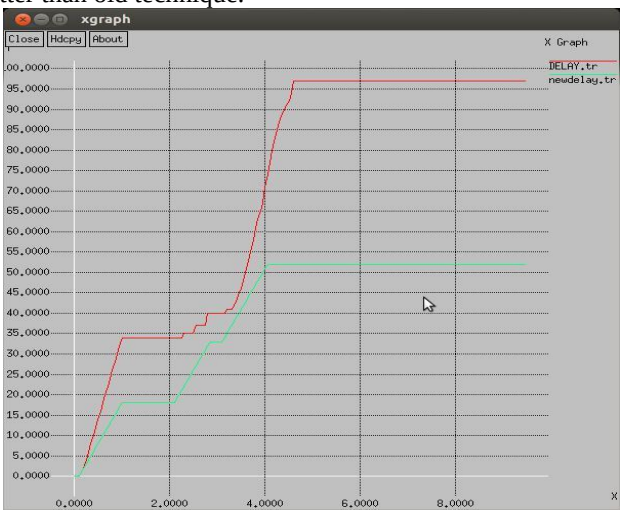

Fig.3: Delay Graph

In above figure 3 the earlier delay is denoted by the red line and the new delay is represented by green line. The time duration and the number of packets are represented on x-axis and y-axis respectively. The delay is reduced within the new proposed method in comparison to the earlier method. This shows improvement within the new technique.

V. CONCLUSION

The wireless mobile networks are the type of network in which mobile nodes can sense environmental conditions and sensed information will be passed to base station. The size of the mobile nodes is very small due to which battery life of the mobile nodes is limited. The wireless mobile networks are the self configuring type of network due to which some malicious nodes may join the network. These malicious nodes are responsible to trigger blackhole attack in the network. In this work, technique is proposed which will detect and isolate malicious nodes from the network. The proposed technique will be based on analysis of the route reply packets in which the nodes reply with the exceptional high sequence number. The nodes which send exceptional high sequence number will be considered as the malicious nodes. To isolate these nodes from the network, technique of clustering will be applied this improvement leads to increase network performance.

VI. REFERENCES

[1]. Juby Joseph, Vinodh P Vijayan," Misdirection Attack in MANETS Due to Selfish Nodes; Detection and Suppression using Longer Path Protocol", 2014 Vol.4

[2]. Dr. G. Padmavathi, Mrs. D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Mobile Networks", International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009, pp. 1-9

[3]. Ju young Kim, Ronnie D. Caytiles, Kyung Jung Kim, "A Review of the Vulnerabilities and Attacks for Wireless Mobile Networks" Journal of Security Engineering, 2014, pp.241-250

[4]. Kalpana Sharma and M K Ghose, "Wireless Mobile Networks: An Overview on its Security Threats" IJCA Special Issue on "Mobile Ad-hoc Networks" MANETs, 2010, pp.42-45

[5]. Kalpana Sharma and M K Ghose, "Wireless Mobile Networks: An Overview on its Security Threats" IJCA Special Issue on "Mobile Ad-hoc Networks" MANETs, 2010

[6]. LV Shaohe, Wang Xiaodong, Zhao Xing," Detecting the Sybil Attack Cooperatively in Wireless Mobile Networks", Computational Intelligence and Security 2008, CIS '08 International Conference on Volume 1Suzhou, pp.442-446, IEEE 2000

[7]. Baviskar B.R, Patil V.N," Black hole attacks mitigation and prevention in wireless mobile network", International Journal of Innovative Research in Advanced Engineering (IJIRAE), Volume 1, Issue 4, pp. 167-169, May 2014.

[8]. Maan younis Abdullah, Gui Wei Hua, Naif Alsharabi, **"**Wireless Mobile Networks Misdirection Attacker Challenges and Solutions", 2008 IEEE 978-1-4244-2184-8/08/

[9]. Roshan Singh Sachan, Mohammad Wazid, D.P. Singh, Avita Kata and R.H. Goudar, **"**Misdirection Attack in MANETS: Topological Analysis and an Algorithm for Delay and Throughput Prediction", 2012 IEEE 978-1-4673-4603-0/12/

[10]. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci. "Wireless Mobile Networks: A survey" Broadband and Wireless Networking Laboratory, School of Electrical and Computer Engineering, Georgia institute of Technology, Atlanta, GA 30332, USA Received 12 December 2001; accepted 20 December 2001, pp . 392-422.