Black Hole Attack Isolation Technique for Mobile Ad hoc Networks

Maneesha Kureshi
Research Scholar
Sirda Group of Institutions
Sundernagar

Er.Poonam Chaudhary
Assistant Professor
Sirda Group of Institutions
Sundernagar

Abstract - The infrastructure-less networks are kind of networks which do not comprise any centralized manager. These central controllers or managers are also recognized as access points. These networks are termed as ad hoc networks as well and are decentralized kinds of networks. Inside this ad hoc network, every node sends information to its subsequent node. This means that all nodes participate in routing process. In this study, a new method has been projected which performs according to blacklist and clustering mechanism. The simulation of projected method is carried out in NS2. It has been scrutinized that projected method gives good performance on the basis of different factors.

I. INTRODUCTION

Network is defined as the association of various computers which are connected to give benefits to one another. The computers are linked for communication purpose and information sharing. In this arrangement, computer systems are gathered for performing interaction among each other. Thus network is a kind of situation, where several computers are congregated and linked with one another for the sharing of information and grant services to other resources as well. The networking tools provide information interaction. During sharing procedure, various software and hardware tools remain present [1]. MANET (Mobile Ad-hoc Network) is a high momentum infrastructure less kind of wireless network which includes several mobile nodes. A random topology is created inside the network because of the connection of all nodes. These nodes act both as router and host. The MANET is a self-configured kind of network which provides suitable communication amid the accessible nodes for information sharing. As these networks are infrastructure less, therefore nodes are free to join or leave the network according to their necessity. Inside MANET, both stationary and lively topologies may occur for the routing protocols. In the ad hoc network, it is also observed that a potential wireless set-up remains present in the absence of central or fixed framework. In the infrastructure-less networks, various issues occur because of their performance. The passage in the network is acknowledged and routed from the intermediary nodes towards the target through the movable nodes of mobile ad-hoc network. Thus according to the service of nodes, network can behave both as router as well as host. During the movement of nodes, the latest connection breakage and re-links taking place inside the network represents power restraint [5].The mobile ad hoc networks have inadequate bandwidth and node movement. Therefore, appropriate consideration and investigation is necessary for different parameters such as the power competence of nodes, topology alterations and untrustworthy interaction inside the network. A number of routing protocols occur within mobile ad-hoc networks. The efficiency of routing protocol is determined on the basis of battery consumption by the contributing nodes. The total quantity of traffic routing is a significant parameter as well..A mobile ad hoc network is also defined as a wireless dispersed network which is self-arranged and comprises multi-hops. The main aim of this network is the detection of a path inside the network. Routing protocols are used for the association and maintenance of the paths present amid the mobile nodes. Inside the network, connection failure and termination of end-to-end path occurs because of the continuous alteration of network topology. The AODV protocol is a significant on-demand routing protocol which establishes paths according to the need of source node. Inside the network, a path detection procedure is commenced when establishment of path is required towards the target. A RREQ packet is delivered to the neighboring nodes inside the arrangement. The demand is auxiliary transmitted to the adjoining nodes. This demand is keep going till the source node or an intermediary node establishes a path towards the destination node which exists beyond the base station coverage area. The unicasting RREP packet sends respond after the arrival of RREQ packet at the target or intermediary node. This RREP is delivered to the primary adjoining node from which the request was received initially. The path continuation process is commenced for the selection and establishment of path. This process continues till the arrival of target from the source node by any route. This means that no additional path is required. The RERR (route error) information is sent for informing other nodes about the link failure.

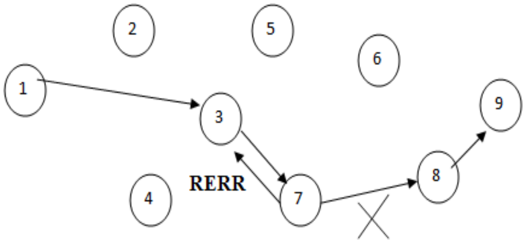

Figure 1 Routing Discovery Process in AODV protocol

The black hole concern occurs in a situation when routing protocol declares itself to be the direct path to the target node. The routing packets are plunged and are not sent to the adjoining nodes too. It is assumed that ‘M’ is the attacker node. During any time period, when node ‘A’ transmits the RREQ packet, the nodes ‘B’ ‘D’ and ‘M’ collect this packet. The routing table of the malicious node ‘M’ is not checkered and thus the request of node ‘E’ is replied arbitrarily. A RREP packet is then forwarded to a node which determines the availability of path. RREP is sent to node ‘A’ from ‘M prior to the acknowledgement of any respond from node ‘B’ and ‘D’. The node ‘A’ claims that path through malicious node ‘M’ is the direct path. Whole information is immersed in such a situation where node ‘A’ propels information to node ‘M’. Therefore, it acts like a ‘Black hole’.

II. LITERATURE REVIEW

Seung Yi, et.al (2012) stated that several accessible joint verification techniques occurred inside the mobile ad hoc networks [12]. In this study, both symmetric and asymmetric key allocation techniques were presented. In this study, PKI (public key distribution) scheme was also revealed as per the symmetric key allocation technique. The researcher proposed a novel approach named as MOCA. This scheme was hybrid and involved both PKI (public key distribution) and asymmetric techniques for joint verification.

Mohammad Al-Shurman, et.al (2004) stated that the mobile ad hoc networks were vulnerable to the black hole intrusion which depleted the system protection. In this study, two explanations were provided in opposition to this intrusion [13]. The primary explanation involved the recognition of more than single path on the way to the target. The next technique involved the utilization of packet series number that included a packet header. The simulation outcomes demonstrated that the second method could authenticate the 75 to 98% of the paths on the way to the target because least holdup cost occurred for every break time inside the network as compared to that which involved AODV routing system.

Pradeep kyasanur, et.al (2005) proposed a novel protocol which was the advanced version of 802.11 DCF protocol [14]. This protocol provided support in the identification of self-centered activities of the nodes inside the wired and ad hoc network topologies. A self-centered node was the one which selected the contentional window (CW) time in such a way that the remaining nodes hanged around for sending the information. This selfish behavior reduced the overall performance of the network. In the presented technique, mainly three mechanisms occurred. In the first mechanism, the receiver gathered knowledge about the occurrence of path diversion from the routing protocol. The contentional window time was provided to the source inside the second mechanism which was castigated. The sender compensated profusion for forwarding information in the specific time period.

Tien-Ho Chen, et.al (2010) conversed the requirement of joint verification inside the wireless sensor arrangements [15]. In this study, a hash-based substantiation protocol identified as DES protocol was proposed as well. A number of different safety procedures were presented in this study for the prevention of different kinds of intrusions occurring inside the system.

Priyanka Goyal, et.al (2011) stated that mobile ad hoc network were extremely popular in every investigational field of wireless sensor networks [16]. The wireless ad hoc network was the most famous and dynamic field of information sharing among all the networks. This network was used in almost all the movable equipments and wireless set-ups. The mobile ad-hoc network was gone through numerous challenges. These challenges were required to be resolved timely. In this study, the main concerns recognized inside the ad hoc networks were conversed in conjunction with the characteristics, groups and liabilities occurring in the mobile ad-hoc networks. A concise demonstration of routing protocols was provided in this study in association with the issues occurring in the mobile ad hoc networks.

DurgeshWadbude, et.al (2013) presented a brief review of ad hoc network which was a multi-hop wireless network. In this network, every node maintained the network connectedness in the absence of centralized framework [17]. Inside the mobile ad hoc networks, locations of nodes were changed dynamically. In these kinds of networks, several protocols were used due to the regular alteration of network topology. Safety was the main challenge of these networks. A number of intrusions occurred inside these networks because of the misconduct of attacker nodes. These intrusions could create issues is packet broadcasting. In this study, a proficient safe AODV routing protocol was presented. The tested outcomes demonstrated that an enhanced safety and functionality level was attained with the help of proposed approach. Inside the network, an improvement was noticed regarding different factors like operating cost, performance and peer to peer holdup. These factors could provide support in the protection of AODV routing protocol in the set-up.

A.S. Bhandare, et.al (2011) presented a concise review of AODV and DSR routing protocols utilized in mobile ad hoc arrangements. In this study, a new approach identified as attack discovery was proposed with the help of irregularity recognition. The proposed approach provided protection against the solitary and manifold black hole intrusions [18]. Through this technique, attacker nodes were secluded from the trustworthy nodes. The discovery and scrutiny of the irregular behaviors of an attacker was executed according to the performed the actions. The system was based on the source relied attack discovery as no centralized mechanism was present over the component for the observation of passage streaming. The fraudulent respond broadcasted from an illegal node could be identified using different factors like hop count, target IP address and timestamp. These networks could be deployed easily. In these networks, a self-defense system was implemented.

Jaydip Sen, et.al (2011) proposed a novel technique for the prevention of mutual black hole intrusion inside the mobile ad hoc networks by utilizing AODV routing protocol [19]. In this scheme, definite throughput level was ensured inside the network. These schemes helped in implementation of safety measures against the black hole intrusion inside the set-up. The tested outcomes demonstrated that the proposed approach increased the packet deliverance proportion. In future, this approach can be made better with the help of definite improvements in order to protect the ad hoc network in opposition to different intrusions.

III. RESEARCH METHODOLOGY

Detecting and removing black hole attack from the network is the major objective to achieve which this research is implemented. When a malicious node enters the network, it forces to generate a path from source node across it causing a black hole attack. The route request packets are flood in the network by the source node in the attack process. Route reply packets are sent as a reply by the nodes that have path to the destination. Although the malicious node does not have a path to the destination, it pretends to do so. It also shows to be having the maximum sequence number. Due to this, a path across malicious node is chosen by the source node. Thus, to detect the malicious nodes from network, certain steps are performed:

1. Mobile nodes are deployed in the network in the initial step.

2. To perform communication in the network, the source nodes and destination nodes are defined.

3. Fake route request packets are flood in the network by the source node.

4. A node will be identified as malicious if it responds to the fake route request packets.

5. If not, the time at which route reply packets are being received is tracked by the source node.

6. A node will be denoted as the least trusted node if it replies back with least sequence number in the minimum possible time.

7. A node that is known to be the least trusted node is then declared as malicious.

8. To isolate the malicious nodes from network, clustering mechanism is applied.

9. Depending upon the location based clustering, a complete network is divided into clusters.

10. A cluster head is chosen as the one node of each cluster that has maximum trust.

11. The cluster head that isolates the malicious node from network is responsible for routing the data to destination.

IV. RESULT AND DISCUSSION

Network Simulator is the outcome of a continuing endeavor of R&D directed by investigators at Berkeley. This is a distinct incident simulator focused on networking exploration. Network simulator 2 is an entity-oriented, distinct incident NS invented at sUC Berkeley. This simulator is in C++ and OTcl (Object-Oriented Tcl) programming languages. This simulator generally utilizes OTcl in form of authority and pattern language. NS is essentially written in C++, with an OTcl predictor as a frontend

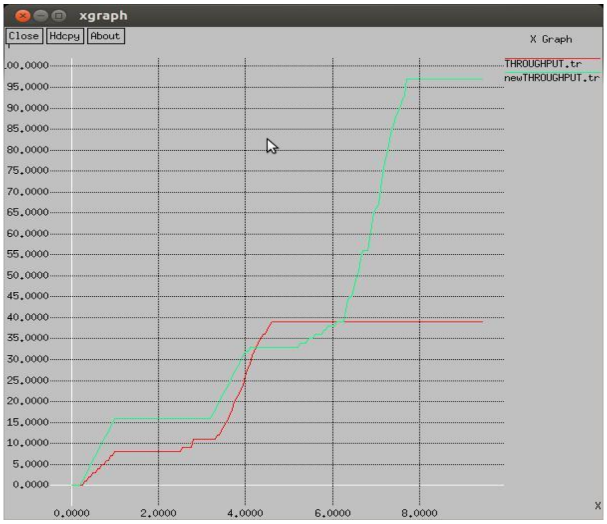

Figure 2 Throughput graph

The figure 2 depicts that the throughput of the presented approach is compared with the existing attack scenario. It is analyzed that when attack is identified and secluded from the set up then throughput is raised in the network.

Table 1: Throughput comparison

Time	**Existing Technique**	**Proposed Technique**
2 seconds	**6 packets**	**16 packets**
6 seconds	**36 packets**	**42 packets**
8 seconds	**43 packets**	**93 packets**

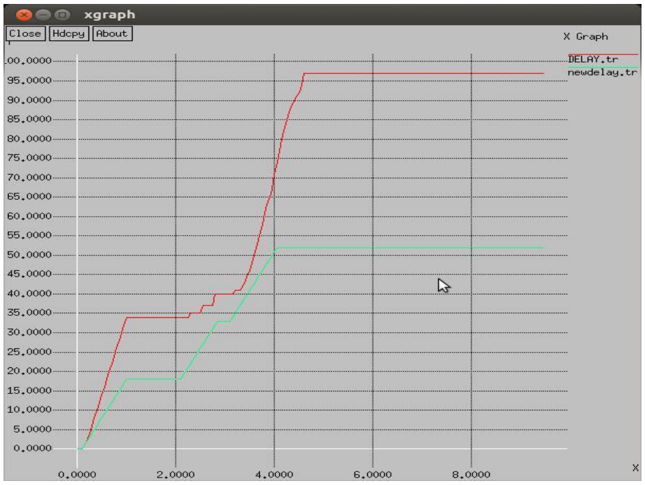

Figure 3 Delay Graph

The figure 3 depicts that the delay of proposed and existing intrusion is compared for the performance analysis. The delay in the network gets reduced when the malevolent nodes is removed from the network.

Table 2: Delay comparison

Time	Existing Technique	Proposed Technique
2 seconds	34 packets	16 packets
6 seconds	70 packets	52 packets
8 seconds	96 packets	55 packets

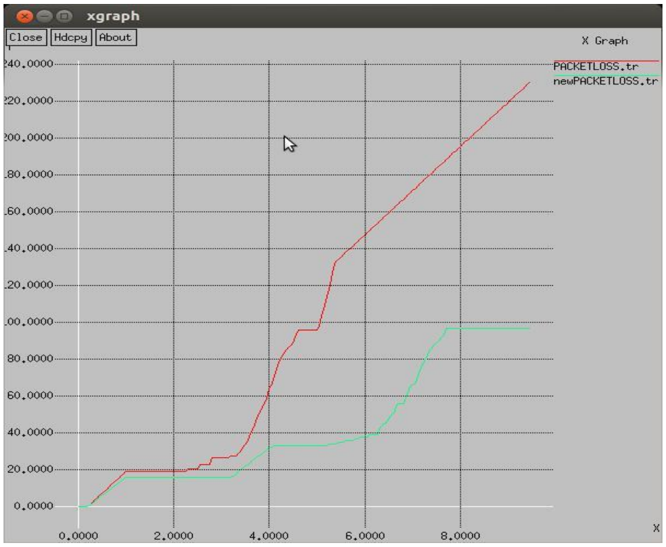

Figure 4 Packet loss Graph

The figure 4 shows that the packet loss of the projected and existing attack scenario is compared to carry out performance analysis. The packet loss in the network gets reduced after the of malevolent from the network.

Table 3: Packet loss comparison

Time	Existing Technique	Proposed Technique
2 seconds	22 packets	18 packets
6 seconds	60 packets	32 packets
8 seconds	140 packets	100 packets

V. CONCLUSION

This study concluded that the MANET is a self configuring wireless network. In this network, movable nodes can enter or depart from the network as per their own wish. The network security is one of the most concerning issue which reduces network functioning. It calculates the trust of the nodes on the basis of several nodes being forwarded. Another clustering method is proposed for the isolation and illumination of harmful nodes. This technique is implemented on the network simulator 2 and outcome are scrutinized in terms of various parametric values.

VI. REFERENCES

[1] Bo Sun Yong, “Detecting Black-hole Attack in Mobile Ad Hoc Networks”, EPMCC, 2004

[2] CaimuTang ,DapengOilver “An Efficient Mobile Authentication Scheme for Wireless Networks”,*IEEE,* 2011

[3] Jacek Cicho,RafałKapelko, Jakub Lemiesz, and Marcin Zawada“On Alarm Protocol in Wireless Sensor Networks*”,IEEE, 2010*

[4] S. Sharmila and G.Umamaheswari, “ Defensive Mechanism of Selective Packet Forward Attack in Wireless Sensor Networks”, *International Journal of Computer Applications (0975 – 8887) Volume 39– No.4, February 2012*

[5] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester, “An Overview of Mobile Ad Hoc Networks: Applications and Challenges”, *IJSER, 2005*

[6] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, “A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks” ,*Springer,2006*

[7] SevilŞen, John A. Clark, Juan E. Tapiador, “Security Threats in Mobile Ad Hoc Networks”, *IEEE, 2010*

[8] Giovanni VignaSumitGwalani Kavitha Srinivasan Elizabeth M. Belding-Royer Richard A. Kemmerer, “An Intrusion Detection Tool for AODV-based Ad hocWireless Networks*”, 2004*

[9] N. Purohit, R. Sinha and K. Maurya, “Simulation Study of Black Hole and JEllyfish Attack on MAnet using NS-3,” *IEEE*, pp. 1-5, 2011.

[10] H. L. Nguyen and U. T. Nguyen, “A Study of Different Types of Attacks in Mobile Adhoc Network,” *25th IEEE Canadian Conference on Electrical and Computer Engineering*, no. 2, pp. 1-6, 2012.

[11] S. Lu, L. Li, K. Y. Lam and L. Jia, “SAODV- A MANET Routing Protocol that can withstand Black Hole Attack,” *IEEE*, pp. 421-425, 2009.

[12] Seung Yi, Robin Kravets, “Key Management for Heterogeneous Ad Hoc Wireless Networks”, 10th IEEE International Conference on Network Protocols (ICNP’02) 1092-1648, n.d.

[13] Mohammad Al-Shurman et.al, “Black Hole Attack in Mobile Ad Hoc Networks”, ACM, 2004

[14] Pradeep kyasanur “Selfish MAC layer Misbehavior in wireless networks”, IEEE on Mobile Computing, n.d .2005

[15] Tien-Ho Chen and Wei-Kuan, Shih, “A Robust Mutual Authentication Protocol for Wireless Sensor Networks”ETRI Journal, Volume 32, Number 5, October 2010

[16] Priyanka Goyal, VintraParmar and Rahul Rishi, “MANET: Vulnerabilities, Challenges, Attacks, Application”, IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011 ISSN (Online): 2230-7893 2011

[17] DurgeshWadbude, Vineet Richariya, “An Efficient Secure AODV Routing Protocol in MANET”International Journal of Engineering and Innovative Technology (IJEIT) ISSN: 2277-3754 Volume 1, Issue 4, April 2012

[18] A. Bhandare and S. Patil, “Study of Protocols (AODV, DSR) of MANET and Black Hole Attack in AODV,” ISOR Journal of Electronics and Communcation Engineering, pp. 50-53, 2011.

[19] J. Sen, S. Koilakinda and A. Ukil, “A mechanism for Detection of Cooperative Black Hole Attack in Mobile Adhoc Network,” International conference on Inteligent Systems, Modellingand Simulation, pp. 338-343, 2011.

[20] P. K. Singh and G. Sharma, “An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET,” IEEE International conference on Trust, Security andPrivacy in Computing and Communcation, pp. 902-906, 2012.