Available online at: http://www.ijmtst.com/vol6issue06.html

International Journal for Modern Trends in Science and Technology

ISSN: 2455-3778 :: Volume: 06, Issue No: 06, June 2020

An Efficient & Secure Timer Based baiting Approach to Detect Black Hole Attacks in MANET

Shifana Begum[1] | Ramzeena[2] | Riha Kabeer[2] | Sneha H[2] | T A Ayun[2]

[1]Assistant Professor, Dept. of CSE, Srinivas School of Engineering, Mangalore, Karnataka, India.

[2]UG Student, Dept. of CSE, Srinivas School of Engineering, Mangalore, Karnataka, India

To Cite this Article

Shifana Begum, Ramzeena, Riha Kabeer, Sneha H and T A Ayun, "An Efficient & Secure Timer Based baiting Approach to Detect Black Hole Attacks in MANET", *International Journal for Modern Trends in Science and Technology*, Vol. 06, Issue 06, June 2020, pp.:29-32; https://doi.org/10.46501/IJMTST060607

Article Info

Received on 21-April-2020, Revised on 21-May-2020, Accepted on 25-May-2020, Published on 01-June-2020.

ABSTRACT

Mobile Ad hoc Network (MANET) is a type of wireless networks that provides numerous applications in different areas. Security of MANET had become one of the hottest topics in networks fields. MANET is vulnerable to different types of attacks that affect its functionality and connectivity. The black-hole attack is considered one of the mostwide spread active attacks that degrade the performance and reliability of the network as a result of dropping all incoming packets by the malicious node.

Black-hole node aims to fool every node in the network that wants to communicate with another node by pretending that it always has the best path to the destination node. AODV is a reactive routing protocol that has no techniques to detect and neutralize the black-hole node in the network. In this research, we enhanced AODV by integrating a new lightweight technique that uses timers and baiting in order to detect and isolate single and cooperative black-hole attacks. During the dynamic topology changing the suggested technique enables the MANET nodes to detect and isolate the black-hole nodes in the network. The implementation of the proposed technique is implemented using java.

KEYWORDS: *Wireless sensor networks, Quality of service, Multipath routing, OQoS-MRP.*

DOI: https://doi.org/10.46501/IJMTST060607

I. INTRODUCTION

Wireless communication network could be controlled by a central infrastructure that controls communication between nodes in the network, or it could be an infrastructure-less which is called Ad hoc Networks. Mobile Ad hoc Network (MANET) is an application of the Wireless Adhoc Network (WANET) that connects mobile nodes to each other. In MANET, nodes do not rely on a central node to coordinate the communication or to carry data between them; instead of that, they work together to carry data between nodes that cannot reach each other directly. In other words, nodes may work as a bridge between the sender and the receiver node when sender and receiver are not in the same coverage. The mobility of the nodes leads to a dynamic changing in the network topology. MANET routing protocols are designed to be adaptive to any dynamic topology changes[1].

MANET energy is one of the most important connectivity factors, as each node in the network has a limited amount of energy; consequently. MANET connects nodes to each other using a wireless link, where bandwidth is considered an important network property. The bandwidth of the wireless links is much lower than the wired links. Wireless links signal can be affected by a noise, interference from another signal, or fading [2]. MANET is vulnerable to different types of attacks and threats. Since MANET uses wireless links to connect nodes together, data may be viewed or modified by an unauthorized user and that is called eavesdropping threat. MANET has no central infrastructure that controls the communication between nodes, so nodes rely on themselves to deliver data to the destination node. Thus, a malicious attacker node may alter the connection link or drop the forwarded data. Denial of Service (DoS) attack is considered one of the most serious threats to MANET, in which a malicious attacker node drains the battery of other nodes by requesting them to forward a huge amount of data. Attacks in MANET are divided into active and passive attacks.

In active attacks, the attacker nodes work to affect the MANET operation, by dropping the forwarded data, altering the connection links, ordraining the nodes batteries. In passive attacks, the attacker nodes only eavesdrop on the communication between nodes without affecting the communication operation between them [3]. Black-Hole Attack- It is an active attack type where the attacker node claims that it has the shortest route to any desired node in the network even if it does not have any route to it; consequently all the packets will pass through it and this enables the black-hole node to forward or discard packets during the data transmission. Normal nodes trust any reply for the requests that they broadcast and black-hole node takes the advantage of this and keeps replying to any request claiming that it has the shortest path to the desired node. Normally nodes start discovery phase in order to find a path to the destination node. The source node broadcasts a request to the destination node, any node receiving this request checks if it has a fresh path to the destination node. When black-hole node receives this request it immediately sends a reply to the broadcaster claiming that it has the freshest and the shortest path to the destination node. Source node believes that reply because there is no mechanism to verify that the request is from a normal node or from a black-hole node. Source node starts forwarding packets to black-hole node hoping to deliver these packets to the destination node, then black-hole node starts to drop these forwarded packets.

II. LITERATURE SURVEY

In [8], the developed baiting technique depends on the own node id. The detection of black-hole node starts by broadcasting a bait request to all adjacent nodes. The bait request contains source sequence number (SSN) and source id; when source node receives replies it checks if there is a reply that has a higher DSN than its own SSN; this indicates that the reply came from a black-hole since there is no node in the network should have a higher DSN than SSN of the source node. After the detection of the black-hole node in the network, source node broadcasts a black-hole alarm to all adjacent nodes to notify them. The limitations of this technique are that a smart black-hole node can check if the received RREQ asks for a route to the same source of the RREQ, then it simply does not reply to that request. Also, smart black-hole node can use the black-hole alarm and starts broadcasting false black-hole alarms to isolate selective nodes in the network.

In[9,10],they developed a technique which depends on using Cooperative Bait Detection method Scheme (CBDS). In CBDS the detection of a black-hole is divided into three phases Bait, Reverse Trace, and Reactive Defense. In Bait phase source node selects one of its neighbors randomly and sends a bait request using its id. In Reverse Trace phase a list of the suspicious nodes is created from the RREP of the bait RREQ, then the neighbour nodes enter in promiscuous mode to detect if there is an attacker node in the path. For each black-hole node detected in the network, a black-hole alarm is broadcasted to neighbour nodes. In Reactive Defense phase source node checks if the PDR is lower than a determined threshold, then it runs Bait phase again.

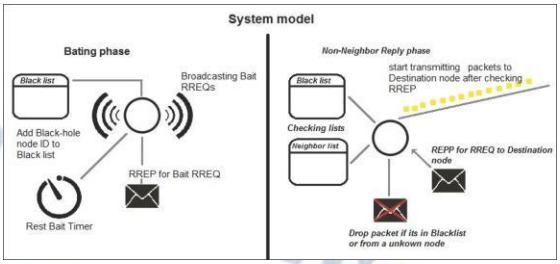
In[11],the developed scheme depends on using a fake id to bait a black-hole node. Source node starts by broadcasting a bait request that contains an id that does not exist in the network. The black-hole node will reply to that bait RREQ due to its normal behavior which replies to any RREQ in the network calming that it has the best path. The developed scheme is implemented in DSR so they modified the RREQ and RREP header in order to determine the black-hole node within the path. An

alert is broadcasted to neighbor nodes when a black-hole node is detected. Source node keeps checking if there is a decrease below the determined threshold; it then starts the baiting again. The limitations of this scheme are that it increases the size of the control packets (RREQ and RREP) which leads to increase in the overhead in addition to the black-hole alerts that can be used by a smart black-hole to isolate nodes in the network.

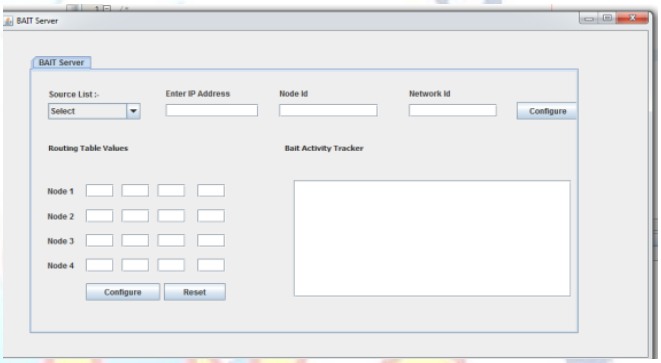
III. PROPOSED SYSTEM

The proposed technique is developed to resist smart black-hole attacks by employing timers and baiting messages (see Figure 2). The proposed technique consists of two phases: Baiting and Non-neighbor Reply. In Baiting phase each node has a bait-timer, the value of the timer is set randomly to B seconds, and each time the timer reaches B it creates and broadcasts a bait request with a randomly generated fake id. Depending on the natural behavior of a black-hole node when it receives any route request it responds with a reply claiming that it has the best path even if it does not exist. When the black-hole receives the baited request it sends a reply to the source node claiming that it has a route; when the source node receives the reply it immediately considers the node which responded as a black-hole and adds it to the black-hole list because it claimed to have a route to a fake node. In the bait request, the value of TTL (Time-To-live) is set to one in order to avoid congesting the network with fake requests. As in a native AODV when any node wants to communicate with another in the network it broadcasts RREQ to the destination node. In Non-neighbor Reply phase each node knows its adjacent nodes because of the hello message broadcasting process.

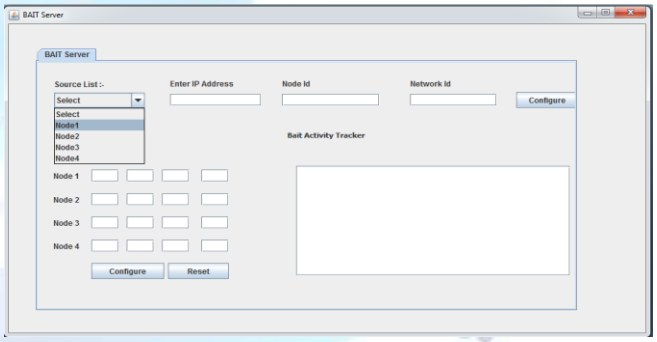
When the source node receives a reply it checks the id of the Node With the Shortest Path (NWSP) if it is in the black-hole list; then it discards the reply; otherwise it checks if the id exists in the neighbor list by comparing the ID with ones in the neighborlist; if NWSP is not a neighbor node then the source node discards that reply to avoid any communication with unknown nodes. The proposed technique provides a self detection and isolation for any black-hole node which enables the connectivity between MANET nodes. The suggested technique does not use the black-hole alarm in order to prevent any smart black-hole node from using this feature by broadcasting false alarms. We set the TTL of the bait request to one to avoid congesting the network by bait requests and responses. The randomness in both fake id and bait-timer will prevent the black-hole node from identifying any pattern to counter this technique. No over head and special packets are used which make it a light weight technique.



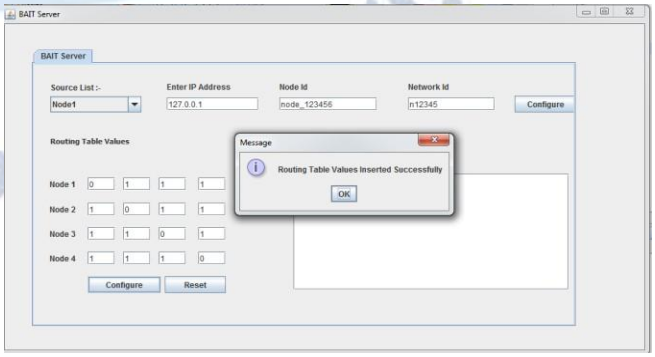
IV. RESULTS AND DISCUSSION



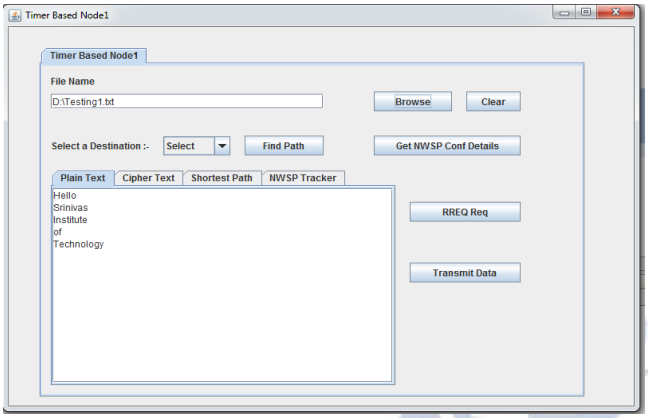
Selecting source node in the bait server



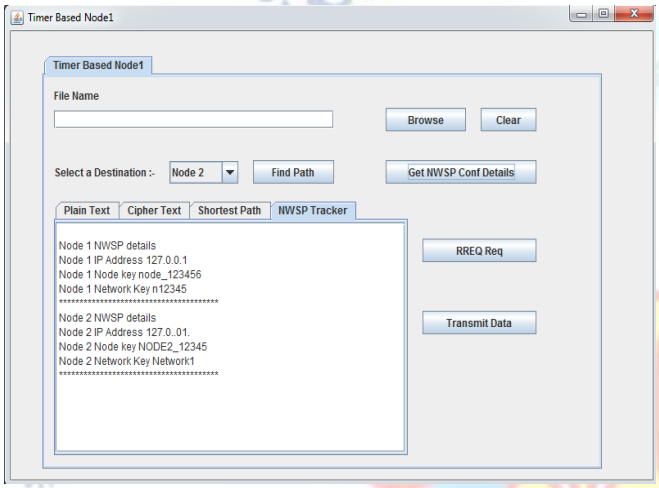
selecting node and configuring



Routing tables Inserted successfully



Getting plain text of text files



Data is getting in NWSP tracker

V. CONCLUSION

The black-hole attack is considered to be one of the most serious attacks that affect the operation of MANET. The detection and isolation of any black-hole nodes in the network are considered an essential task to prevent network collapse. In this research, we introduced a smart black-hole detection and isolation technique that should be considered in constructing and developing any black-hole fighting protocols or techniques. The proposed TBBT integrates both timers and baiting techniques in order to enhance black-hole detection capability while preserving Throughput, End-to-End Delay, and Packet Delivery Ratio. The simulation results of the proposed technique showed that the End-to-End Delay, Throughput, and Packet Delivery Ratio are very close to the native AODV. As a future work, we aim to enhance the proposed model in order to increase the Throughput and Packet Delivery Ratio also to decrease the End-to-End Delay.

REFERENCES

[1] S. Mirza and S. Z. Bakshi, "Introduction to MANET,"International Research Journal of Engineering and Technology,vol.5,no. 1,pp.17– 20,2018.

[2] V. Goyal and G. Arora, "Review paper on security issues in mobile adhoc networks," International Research Journal of Advanced Engineering and Science, vol. 2, no. 1, pp. 203–207, 2017.

[3] M. M. Alani, "MANET security: A survey," in Proceedings of the 2014 IEEE International Conference on Control System, Computing and Engineering (ICCSCE), pp. 559–564, Penang, Malaysia,November2014.

[4] A. Joshi, "A review paper on black hole attack in MANET," International Journal of Advance Research in Computer Science and Management Studies ,vol.4,no.5,pp.16–21,2016.

[5] A. K. S. Ali and U. V. Kulkarni, "Comparing and analyzing reactive routing protocols (aodv, dsr and tora) in QoS of manet," in Proceedings of the 7th IEEE International Advanced Computing Conference, IACC 2017,pp.345–348, Hyderabad, India, January2017.

[6] L. Prashar and R. K. Kapur, "Performance analysis of routing protocols under different types of attacks in MANETs," in Proceedings of the 5th International Conference on Reliability,Infocom Technologies andOptimization,ICRITO2016,pp.405–408,Noida,India,September2016.

[7] H. Moudni, M. Er-Rouidi, H. Mouncif, and B. El Hadadi, "Performance analysis of AODV routing protocol in MANET under the influence of routing attacks," in Proceedings of the 2nd International Conference on Electrical and Information Technologies, ICEIT2016,pp.536– 542, Tangiers, Morocco, May 2016.