ISSN No. 0976-5697

Volume 6, No. 6, July - August 2015

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Removal of selective Black Hole Attack with Alarm System by DSR Algorithm

Gurbir Singh
M.Tech Computer Science
Punjab Technical University, India

Nitin Bhagat
AP, M.Tech Computer Science,
Department of CSEm PTU, India

Abstract: In mobile ad hoc network, each node acts as a router to set up a route and transfer data. It is more open to security problems. When a node wants to transfer data, packets are transferred through the intermediate nodes. Thus, searching and setting up a route from a source node to a destination node is an significant task. There are several routing protocols. The existing routing protocols are optimized to perform the routing process without considering the security problem. Black hole attack is one of the routing attacks in which, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose data it wants to capture. DSR is the most suitable routing protocols for the MANETs and it is less vulnerable to black hole attack as compared to AODV. Alarm technique is been proposed which is based on the fake route request packets to detect and alarm black hole attack in MANET.

Keywords: Malicious node, Ad hoc, detection and prevention of Blackhole Attack, routing, Blackhole Attack.

I. INTRODUCTION

An ad hoc network [1] is a wireless network without any fixed infrastructure. It is a group of mobile hosts without the required involvement of any offered infrastructure or centralized access point such as a base station. There are various challenges that are faced in the Ad hoc environment. AODV is an on demand routing network protocols which is specially design for Ad hoc network.

Ad hoc network offer great flexibility, higher throughput, lower operating cost and better coverage because of collection of independent nodes. Mobile ad hoc networks consist of mobile nodes, which can communicate with each other and nodes can enter and leave the network anytime due to the short transmission range of MANETs [2, 3], routes between nodes may consist of one or more hops. Thus each node may either work as a router or depend on some other node for routing. Figure 1 shows a simple ad hoc network with three mobile hosts using wireless interfaces. Host A and C are out of range from each other's wireless transmitter. When exchanging packets, they may use the routing services of host B to forward packets since B is within the transmission range of both of them.

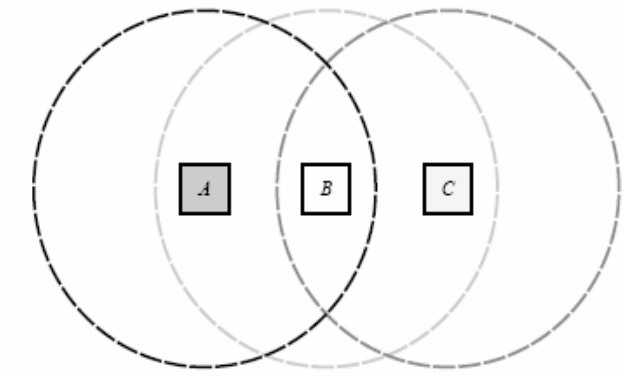

Figure 1. Mobile Ad hoc network with 3 mobile nodes [10].

Routing protocols for Mobile Ad hoc networks can be broadly divided into two distinct categories, namely proactive (table-driven) routing protocols and reactive (on-demand) routing protocols. In Proactive routing protocols, each node maintains up-to-date routing information to every other in a number of routing tables & routes can quickly established without any delay. Reactive or on-demand routing protocols are designed to overcome the increased overhead problem in proactive protocols. Unlike proactive protocols, reactive protocols create a route only when desired [10].

Mobile Ad-hoc Networks (MANETS) have seen tremendous growth in recent years. It is a new paradigm of communication in which there is no fixed infrastructure. Nodes within the radio range of each other can communicate directly over the wireless link, while those that are far apart use other nodes as relays. Routing protocols are the cornerstone of MANET. In the past few years, much research efforts have been focused on this area and many different kinds of routing protocols have been put forward in the literature, such as Wireless Routing Protocol (WRP) [4], Dynamic Source Routing protocol (DSR), Ad hoc On Demand Distance Vector protocol (AODV) and Location Aided Routing. However, from the beginning of its design, almost none of the routing protocols specify security measures, but the nature of wireless ad hoc networks makes them very vulnerable to malicious attacks compared to traditional wired networks.

II. PREVIOUS WORK

Selective blackhole attack constantly has a blow on routing algorithms. It uses sequence number to select the shortest route in routing protocols such as AODV, DSR or DSDV. Normally, a selective blackhole node is reduced to an suitable extent in AODV protocol as referred by Can Erkin [8]. The Justification is given by the concept of rejecting the first two RREP packets send to the source node because mostly the selective black hole node sends its RREP in one of the first two RREP to the source node. Hence it is efficient in detecting Black Hole Attack in AODV protocol.

Dr. Sankarnarayanan [5] proposed another efficient approach based on AODV protocol. It said that usually a source does not send its RREP, only after receiving the first RREP. It waits until all the neighboring nodes to send their RREP. The source sends its reply to the node which has the distance of two from the source node. It also proposed

another method to detect Cooperative Blackhole attack based on the update of the fidelity level. Initially, all nodes are provided with a fidelity level, and sends RREQ to all nodes.

Then it selects a node with higher fidelity level. The level exceeds the threshold value to pass the packets. An ACK is sent from the destination node. The source node adds one to the fidelity level. It subtracts one if no ACK is received. This indicates the possibility of the presence of the blackhole node and sense there may be a loss of data packets before it reaches the destination node.

Nikayama [6] proposed a dynamic learning method to detect a selective black hole node. It is required to observe if the characteristic change of a node exceeds the threshold within a period of time. If yes, this node is judged as a selective black hole node, other-wise, the data of the latest observation is added into dataset for dynamic updating purposes. The characteristics observed in this method include the number of sent RREQs, the number of received RREPs and the mean destination sequence number of the observed RREQs and RREP. However, it does not involve a detection mode, such revising the AODV protocol or deploying IDS nodes, thus, it does not isolate selective black hole nodes. Luo [6] added an authentication mechanism into the AODV routing protocol, by combining hash functions, message authentication codes (MAC), and a pseudo random function (PRF) to prevent lack hole attacks.

Djahel [6] proposed a routing algorithm based on OLSR (Optimized Link State Routing) to prevent the attack of cooperative selective black holes, by adding two control packets, namely 3 hop_ACK and HELLO_rep. Mahmood and Khan [7] also surveyed recent research papers involving selective black hole attacks on MANETs, and described seven previous methods, and analyzed their advantages and disadvantages.

In [9], IDS nodes are deployed in MANETs to identify and isolate selective black hole nodes. An IDS node observes every node's number of broadcasted RREQs, and the number of forwarding RREQs in AODV, in order to judge if any malicious nodes are within its transmission range. Once a selective black hole node is identified, the IDS node will send a block message through the MANET to isolate the malicious node [8].

Mobile Ad-Hoc Networks has the ability to deploy a network where a traditional network infrastructure environment cannot possibly be deployed. In our approach, we have analyzed the behavior and challenges of security threats in mobile Ad-Hoc networks and implemented the promiscuous mode in a better way. Although many solutions have been proposed but still these solutions are not perfect in terms of effectiveness and efficiency. If any solution works well in the presence of single malicious node, it cannot be applicable in case of multiple malicious nodes. After referring many approaches, applying promiscuous mode after the detection of selective black hole attack would surely decrease the rate of loss in data packet. Moreover, the promiscuous mode is applied only for nodes that were attacked rather for applying for all the nodes. Hence loss of energy is surely avoided. We will enhance our work to stop even the initial data packet loss by applying the promiscuous mode to Proactive routing protocols.

Network Simulation 2 is applied for the detection and isolation of selective black hole nodes. In the area 1000 X 1000 m, 75 normal nodes executing the AODV routing protocol were randomly distributed, and few malicious nodes, to perform selective black hole attack. Randomly chosen pairs for data communication send 5 kb UDP-CBR per second. Speed of the nodes moving in a range between 0 and 20m/s. Pause times of the nodes are of 0 s, 5 s, 10 s and 15 s were considered. Pause time is defined as the time taken by node to move from one place to another [9].

III. PROPOSED SCHEME

In MANET, nodes are self configuring. So it can move freely in any direction. There is no central controller in this type of network. Security is of much concern. Different types of attacks are possible in it. There are internal attacks and external attacks. Internal attack affects the network within. Any malicious node can do such type of attack. External attacks affect the network on the outside. The black hole attack is the most common type of attack which is triggered by malicious node present in the network. In this work, new technique has been proposed which detect the malicious node and isolate it from the network which is responsible for triggering the black hole attack. The basic idea to detect and isolate malicious node from the network is by using fake route request packets. In our proposed methodology, source node which wants route to destination will Alarm fake route request packet in Upstream and Downstream network. The fake route request packets contain the IP address of the node which doesn't exist in the network. The malicious node will reply back to source with the route reply packet. The node which reply with the route reply packet is detected as the malicious node and it is isolated from the network. To isolate malicious node from the network, source again Alarm route the genuine route request packets in the network. The source gets various route replies and from the route reply various available paths are there. Source never select that path in which the malicious node exists which is been detected in fake route request packets. The proposed technique will implemented in network simulator version 2 and results will be analyzed graphically by taking various network parameters like throughput and delay.

IV. PROPOSED ALGORITHM

Start

a. Deploy mobile ad hoc network with finite number of mobile nodes

b. Source node flood the network with the fake route request packets to detect malicious node

c. If (Any mobile reply with route reply packet)

{

That node will be detected as malicious node

}

Else

{

Source assume that no malicious node exist in the network

}

d. The source Alarm the genuine route request packets in the network

e. Source gets various route reply packets

If (Malicious nodes==exists)

{
Source will not select the path in which Malicious node exists
}
f. Secure and shortest path is selected between source and destination
End

V. RESULTS ANALYSIS

A. Delay Graph:

In this graph delay is more in new proposed than the existing system. Red lines shows less delay of old system and Green lines shows more delay in new system. This is happened because we are first searching the malicious node by sending the fake route request packet.

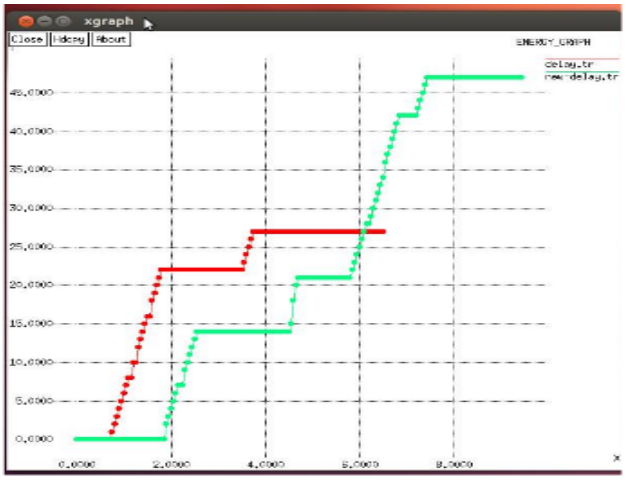

Figure 2. Delay Graph.

B. Throughput Graph

As the packet dropped is prevented in this work. So throughput of the proposed system is more than existing system. Red line shows old throughput and green line shows new throughput.

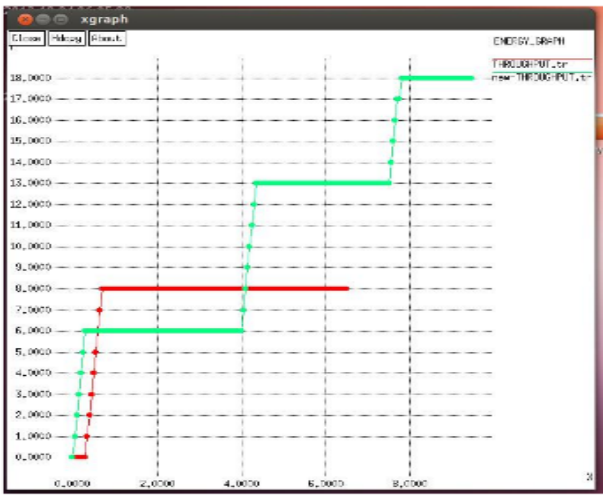

Figure 3. Throughput Graph.

VI. CONCLUSION

In this paper, we conclude that due to the self configuring nature of the mobile ad hoc network type of inside and outside attacks are possible which degrades the network performance. Among all the security attacks black hole attack is the most common and denial of service attack. In this paper, Alarm technique is been proposed which is based on the fake route request packets to detect and alarm black hole attack in MANET. The proposed technique will be implemented in network simulator version 2 and results will be analyzed graphically by taking various network parameters like throughput and delay. The results show that this technique is more efficient than the previous technique.

VII. REFERENCES

[1] Mohammad AL-Shurman, Seon-Moo Yoo, Seungiin Park, “Black Hole Attack in Mobile Ad Hoc Networks” ACMSE, April 2004.

[2] Y. C. Hu, D. B. Johnson, A. Perrig, “Sead: Secure efficient distance vector routing for mobile wireless ad-hoc networks” IEEE, 2002, pp. 3–13.

[3] X. Wang, T. liang Lin, J. Wong, “Feature Selection in Intrusion Detection System over Mobile Ad-hoc Network” Technical Report, Computer Science, Iowa State University, 2005

[4] S. Murthy, J. Garcia-Luna-Aceves, ”An efficient routing protocol for wireless networks,” ACM, vol. l, pp. l83-197, 1996.

[5] A. Hasswa, M. Zulker, H. Hassanein, “Routeguard: an intrusion detection and response system for mobile ad hoc networks,” Wireless and Mobile Computing, Networking and Communication, volume 3, August 2005, P336-343.

[6] Soufine Djahel, Farid Nait-Abdesselam, Ashfaq Khokhar, “An Acknowledgement-Based Scheme to Defend Against Cooperative Black Hole Attacks in Optimized Link State Routing Protocol” IEEE, pp. 2780-2785, 2008.

[7] N. Komnios, D. Vergados, C. Douligeris, “Detecting unauthorized and compromised nodes in mobile ad hoc networks” Elsevier, volume 5, No. 3, pp. 289-298, 2007.

[8] Semih Dokurer, Y. M. Erten, Can Erkin Acar, “Performance Analysis of Ad-hoc Networks under Selective black hole Attacks” IEEE, pp.148-153, 2007.

[9] T. Manikandan, S. Shitharth, C. Senthilkumar, C. Sebastinalbina, N. Kamaraj, “Removal of Selective Black Hole Attack in MANET by AODV Protocol” International Journal of Innovative Research in Science, Engineering and Technology, Volume 3, Special Issue 3, March 2014.

[10] Pooja Jaiswal, Dr. Rakesh Kumar, “Prevention of Black Hole Attack in MANET” International Journal of Computer Networks and Wireless Communications, Vol. 2, No. 5, October 2012.