Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 8, August 2015, pg.414 – 419

RESEARCH ARTICLE

An Analysis and Prevention of Routing Attacks in Mobile Adhoc Networks

N.Sumathi

Department of MCA & S.N.R.Sons College, Coimbatore

sumathikari73@gmail.com

Abstract— In Mobile Adhoc Networks (MANETs), routing attacks are considered as a serious issue. However, in the presence of malicious nodes, the networks are affected by various kinds of attacks. The malicious node(s) can attack a MANET in different ways, such as sending fake messages several times; fake routing information and advertising fake links to disrupt routing operations. Black hole attacks are significant attacks that need to be addressed in MANETs. Although, significant research has been done to combat black hole attacks, this work successfully attempted to detect and prevent the black hole attacks. The proposed work utilizes sequence number associated with every route to identify and prevent black hole attacks. This work is implemented in NS2 simulator. Simulation results show that the proposed algorithm improves the performance of the network after identifying malicious nodes.

Keywords—Mobile adhoc networks, black hole attacks, routing protocols, malicious node

I. INTRODUCTION

Ad-hoc networking can be applied anywhere where there is little or no communication infrastructure or the existing infrastructure is expensive or inconvenient to use. It allows the devices to maintain connections to the network as well as easily adding and removing devices to and from the network. With the increase of portable devices as well as progress in wireless communication, MANETs are gaining importance with the increasing number of widespread applications. The set of applications for MANET is diverse, ranging from large-scale, mobile, highly dynamic networks, to small, static networks that are constrained by power sources [1, 13].

MANETs do not have a centralized management and control. The absence of management makes the detection of attacks difficult because it is not easy to monitor the traffic in highly dynamic and large scale adhoc networks [3, 5, 13]. Routing algorithm for MANETs usually assumes that nodes are cooperative and non-malicious. As a result, a malicious attacker can become an important routing agent and disrupt network operation by disobeying the protocol specifications. Vulnerability is a weakness in security system [16]. A particular system may be vulnerable to unauthorized data manipulation because the system

does not verify a user's identity before allowing data access. MANETs are more vulnerable than wired networks [9].

MANETs are accessible by both legitimate network users and malicious attackers. Since every node actively participates in the operation of the network, malicious nodes are difficult to detect. However, many researchers are trying to remove main weaknesses of MANET such as limited bandwidth, battery power, computational power, and security [4, 6]. Most of the attacks are focused on the on-demand protocols such as AODV (Adhoc OnDemand Vector) [12], DSR, (Dynamic Source Routing) etc. This article discussed the current routing attacks and preventive measures against AODV routing protocol.

The rest of this paper is organized as follows. The next section discusses existing routing attacks as well as countermeasures against such attacks in MANETs. Section 3 describes the proposed work. Section 4 analyses the experimental results. Finally, in section 5, the paper is concluded.

II. RELATED WORK

Most of the related work focused mainly on providing preventive schemes to protect the routing protocol in a MANET. In flooding attack [10], attacker exhausts the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance. In this approach, each node monitors and calculates the rate of its neighbors' RREQ (Route REQuest). If the RREQ rate of any neighbor exceeds the predefined threshold, the node records the ID of this neighbor in a blacklist. Then, the node drops any future RREQs from nodes that are listed in the blacklist. The limitation of this approach is that it cannot prevent against the flooding attack in which the flooding rate is below the threshold.

In a blackhole attack, a malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. The route Confirmation REQuest (CREQ) and route Confirmation REPly (CREP) is introduced in [11,9] to avoid the blackhole attack. As a special case of a black hole [16], an attacker could create a gray hole, in which it selectively drops some packets but not others, for example, forwarding routing packets but not data packets.

In a link spoofing attack, a malicious node advertises fake links with non-neighbors to disrupt routing operations. A location information-based detection method is proposed [15] to detect link spoofing attack by using cryptography with a GPS (Glopal Positioning System) and a time stamp. In a replay attack [2], a node records another node's valid control messages and resends them later. This causes other nodes to record their routing table with stale routes. Replay attack can be misused to impersonate a specific node or simply to disturb the routing operation in MANETs.

In wormhole attack [7], a pair of colluding attackers record packets at one location and replay them at another location using a private high speed network. The key advantage of this approach is that it can detect the attack at low cost without introducing extra routing traffic, and it does not require modification of the existing protocol. However, false positives are the main drawback of this approach due to the nature of anomaly detection. Such an attack can be prevented by using packet leashes which authenticate the timing information in the packet to detect fake packets in the network [14].

In colluding misrelay attack, multiple attackers work in collusion to modify or drop routing packets to disrupt routing operation in a MANET. This attack is difficult to detect. A conventional acknowledgment-based approach might detect this type of attack in a MANET, especially in a proactive MANET, but because routing packets destined to all nodes in the network require all nodes to return an ACK, this could lead to a large overhead, which is considered to be inefficient [8].

Among these, black hole attack is a common and serious problem that should be addressed. Black hole attack may occur due to a malicious node which is deliberately misbehaving, as well as a damaged node interface. In this case, nodes in the network will constantly try to find a route for the destination, which makes the node consume its battery in addition to losing packets.

III. PROPOSED WORK

When a source node wants to communicate with destination node, it first checks for a fresh route to the destination in the routing table. Otherwise, source node initiates route discovery procedure by broadcasting RREQ control message to all its neighbors. Then the source waits for RREPs (Route Reply) to be received from the destination. Source node selects the RREP which has highest destination sequence number. Destination sequence number is a 32 bit integer associated with every route and used to determine the freshness of a route. Malicious nodes make use of this sequence number and send a false RREP with a very high sequence number. Malicious node now acts as a destination. Hence, source would start sending data packets to this malicious node.

In order to overcome this issue, destination sequence number is compared with threshold. If it is higher, an alert message is broadcasted to all its neighbors and routing table for that node is not maintained. Threshold value is calculated as the average of difference in sequence numbers between routing table and RREP in each time slot. In normal state, each node's sequence number is changed depending on its traffic conditions. When a node receives RREP for the first time, it updates the value of threshold. It is then updated dynamically in regular time intervals.

Figure 1 shows an example of an attack, where attacker F sends a fake RREP to the source node S, claiming that it has a sufficiently fresher route than other nodes. Since the attacker's advertised sequence number is higher than other nodes' sequence numbers, the source node S will choose the route that passes through node E. This work identifies the fake route and searches alternate path to destination.

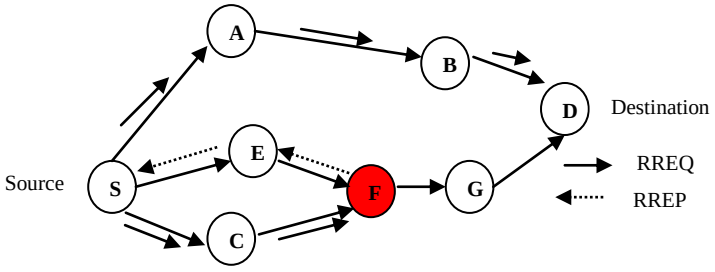

Figure 1: Attack on QoS-AODV Protocol

An example of updating sequence numbers in RREQ and RREP are explained as follows. IP_addr indicates the node which generates RREQ or RREP. Destination sequence number for S is 10. Source node S sets its RREQ and broadcasts. It is forwarded through A, E and C until the destination is reached. Destination D increments the sequence number by one and sends RREP back to source S. But the malicious node F increases its sequence number rapidly as 425210. As a result, route from S to D is deprived by node F.

IV. RESULTS AND ANALYSIS

A network is modeled as set V of nodes that are interconnected by a set E of communication links. V and E change over time when nodes move. Nodes have the maximum transmission range. Each node is equipped with an omni directional antenna. Two nodes are immediate neighbors and an undirected link connecting them exits if they are in the

transmission range of each other. There are several paths between two nodes. The choice of route could be based on the available bandwidth. The simulation results of the proposed method are analyzed.

The simulation time is set as 200 secs for 125 nodes with a grid size of 1000×1000 m. The values chosen for CW_{min} and CW_{max} are 31 and 1023 respectively. These simulation parameters are set as per IEEE 802.11 standard [17]. Figure 2 shows that the number of packets received at 5 nodes. Packets are routed through these five nodes before attack. At the end of 40 secs, 450 bytes are received approximately. Figure 3 shows packets received under attack. Few nodes receive packets abnormally. Those are identified as malicious nodes. Hence this path is blocked and alternate path is selected to transmit the packets.

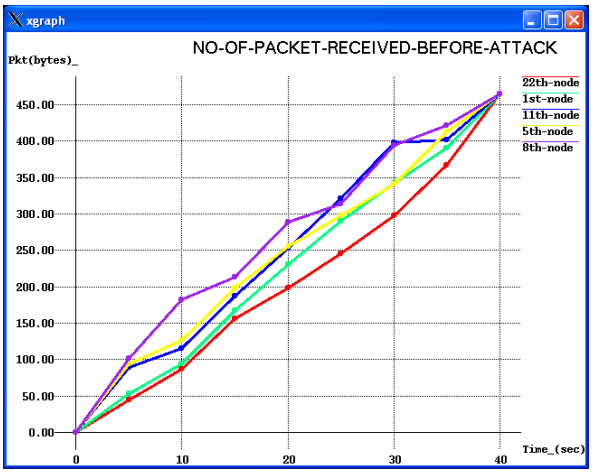

Figure 2: Packets Received Before Attack

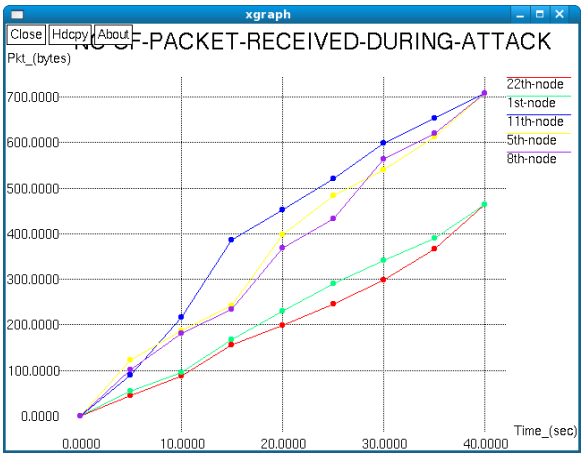

Figure 3: Packets Received During Attack

In order to reduce packet loss and delay, these malicious nodes are identified by checking the abnormal increase in sequence number of RREP control packet. Figure 4 shows packets received after preventing black hole attacks**.** Identifying and controlling malicious nodes during route discovery procedure itself reduces packet loss.

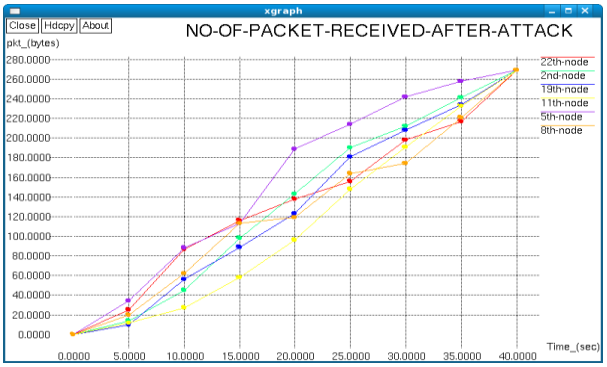

Figure 4: Packets Received After Implementing Attack Algorithm

Malicious attackers exhaust the network resources, such as bandwidth and consume the node's resources, such as computational and battery power and disrupt the routing operation causing severe degradation in the network performance. These attackers are identified and are blocked.

V. CONCLUSIONS

The unique characteristics of MANETs make routing a challenging task. Mobility of nodes cause frequent route failure. As a result of these, an effective routing protocol has to adapt to dynamic topology and designed to be bandwidth constrained. Wireless channel is bandwidth constrained and shared among multiple networking entities. Since MANET has no clear line of defense, it is accessible to both legitimate users and malicious attackers. In order to address this issue, various types of attacks are analyzed. Malicious nodes attack the network which causes packet loss and consume considerable amount of bandwidth. These types of nodes are identified and blocked to improve the available bandwidth. However, adhoc networks present unique advanced challenges, including the design of protocols for mobility management, effective routing, data transport, security, power management, and QoS provisioning. Once these problems are solved, the practical use of MANETs will be realizable.

REFERENCES

[1] Loay Abusalah, Ashfaq Khokhar and Mohsen Guizani, "A Survey of Secure Mobile Ad Hoc Routing Protocols" IEEE Communications Surveys& Tutorials, VOL. 10, NO. 4, Fourth Quarter, 2008.

[2] C. Adjih, D. Raffo and P. Muhlethaler. Attacks Against OLSR:Distributed Key Management for Security. *2nd OLSR Interop/Wksp.*, Palaiseau, France, July 28-29, 2005.

[3] D.P. Agrawal and Qing- An Zeng. Introduction to Wireless and Mobile Systems. BrookdCole-Thomson Learning, 2003.

[4] C. R. Dow, P. J. Lin, S. C. Chen*, J. H. Lin*, and S. F. Hwang. A Study of Recent Research Trends and Experimental Guidelines in Mobile. Ad-hoc Networks. 19th InternationalConference on *Advanced Information Networking and Applications, 2005. AINA 2005,Volume: 1, On page(s): 72- 77 vol.1*.

[5] Elizabeth, M.R. and T. Chai-Keong. A Review of Current Protocols for Ad Hoc Mobile Wireless Networks. IEEE personal communications, Vol.6, No.2, pp. 46-55, April 1999.

[6] Grunde Eikenes and Ole Erik Grostøl. Management of Quality of Service and other functions in mobile Ad Hoc networks. Masters Thesis in Information and Communication Technology Agder University College Grimstad, May 2003.

[7] Y-C. Hu, A. Perrig and D. Johnson. Wormhole Attacks in Wireless Networks. IEEE JSAC, Vol. 24, No. 2, pp. 370-380, February 2006.

[8] B. Kannhavong, H. Nakayama and A. Jamalipour. A Collusion Attack against OLSR-Based Mobile Ad Hoc Networks. *IEEE GLOBECOM '06*, pp.1-5, 2006.

[9] S. Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour and Yoshiaki Nemoto. Detecting Blackhole Attack on AODV-Based Mobile Ad Hoc Networks by Dynamic Learning Method. Proc. Int'l. J. Network Sec., 2006.

[10] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, A. Jamalipour. A survey of routing attacks in mobile ad hoc networks security. In wireless mobile ad hoc and sensor networks, pp. 85-91, October 2007.

[11] S. Lee, B. Han and M. Shin. Robust Routing in Wireless Ad Hoc Networks. Int'l. Conf. on Parallel Processing Workshop, Vancouver, Canada, August 18-21, 2002.

[12] C. Perkins, E. Belding-Royer, and S. Das, "Ad Hoc On demand Distance Vector (AODV) Routing," IETF RFC 3561, July 2003.

[13] Goyal Priyanka, Parmar Vinti, Rishi Rahul, " MANET: Vulnerabilities, Challenges, Attacks, Application", International Journal of Computational Engineering & Management (IJCEM), pp. 32-37, 2011.

[14] L. Qian, N. Song and X. Li. Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks Through Statistical Analysis of Multi-path. IEEE Wireless Communication and Networking Conf. '05, 2005.

[15] D. Raffo, C.Adjih, T.Clausen and Paul Muhlethaler. Securing OLSR Using Node Locations. Proc. 2005 Euro. Wireless, Nicosia, Cyprus, pp. 10-13, April 2005.

[16] B.Wu, J.Chen, J.Wu and Mihaela Cardeiet. A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks. Wireless/Mobile Network Security, Springer, Vol. 17, 2006.

[17] IEEE Std. 802.11, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," 1997.

