www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-6, Issue-2, April 2018
Review Paper

Int. J. Sc. Res. in
Network Security
and Communication

ISSN: 2321-3256

A Review of Vulnerabilities and Attacks in Mobile Ad-Hoc Network

Shailja Sharma

Computer Science, Career College, Bhopal, India

Received: 06/Mar/2018, Revised: 19/Mar/2018, Accepted: 12/Apr/2018, Published: 30/Apr/2018

Abstract- MANETs has become an important technology in recent years because of the rapid proliferation of wireless devices. MANETs are highly vulnerable to attacks due to the open access medium, dynamically changing network topology and lack of centralized monitoring point. The various attacks against mobile nodes are flooding, black hole, warm hole, packet dropping and Byzantine attack as well as Collaborative attacks i.e. human attackers or criminal organizations etc. We have addressed the Vulnerabilities and attacks in MANETs in this paper.

Keywords- MANET, Protocols, Attacks, Security Issues

I. INTRODUCTION

A Mobile Ad hoc Network (MANET) is a self-organized wireless short-lived network consisting of mobile nodes. The mobile nodes communicate with one another by wireless radio links without the use of any pre-established fixed communication network infrastructure. Typical MANET nodes are Laptops, PDAs, Pocket PCs, Cellular Phones, Internet Mobile Phones, and Palmtops. These devices are typically lightweight and battery operated. The mobile nodes are vulnerable to different types of security attacks than conventional wired and wireless networks.

Ad-Hoc networks have no infrastructure where the nodes are free to join and left the network. The nodes are connected with each other through a wireless link. A node can serve as a router to forward the data to the neighbors' nodes. Therefore this kind of network is also known as infrastructure less networks. These networks have no centralized administration. Mobile ad hoc networks (MANETs) are one of the examples of ad hoc networks. Therefore, security in Mobile Ad-Hoc Network is the most important concern for the basic functionality of network. The availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANETs often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANETs against the security threats.

II. RELATED WORK

Mobile ad-hoc Networks (MANETs) are an appealing technology that has attracted lots of research efforts over past years. Although the principle of wireless, structure-less, dynamic networks is attractive, there are still some major flaws that prevent commercial expansion. Security is one of these main barriers; Having a secured transmission and communication in MANET is a challenging and vital issue due to the fact that there are various types of attacks that the mobile network is open to. In order to secure communication in such networks, understanding the liable security attacks to MANET is a great task and concern. MANETs suffer from a variety of security attacks and threats such as: Black Hole Attack, Wormhole Attack, Sybil attack, Routing Attacks, Denial of Service (DoS), flooding attack, impersonation attack, selfish node misbehaving, and so forth [1-2]. MANET is open to vulnerabilities as a result of its basic characteristics like: no point of network management, topology changes vigorously, resource restriction, no certificate authority or centralized authority, to mention a few [3-5].

Previous studies show that there are different categories of attacks on MANET [2-6] such as on the basis of source (Internal and External attacks), on the basis of behavior (Passive and Active attacks), and the Routing and Packet Forwarding attacks. Some of these attacks are termed as single attacks while some are referred to as attacks on multiple nodes and are malicious. In this work, we plan to make investigation on the multiple node attacks against MANET and provide a new categorization of multiple node attacks. In addition, based on the characteristics of these attacks, we will present a proper definition of such attacks in MANET. After that, the simulations of different network sizes are performed to see the impact on MANET's performance with and without collaborative attack. Finally, the various mitigation plans for collaborative attacks will be discussed, analyzed and highlighted

III. VULNERABILITIES IN MANET

Vulnerability is a weakness in security system or Wireless System. 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 is more vulnerable than wired network. Some MANETs vulnerabilities are as follows [1-4, 7-9]:-

a. Wireless Links: First of all, the use of wireless links makes the network susceptible to attacks such as eavesdropping and active interference. Unlike wired networks, attackers do not need physical access to the network to carry out these attacks. Furthermore wireless networks typically have lower bandwidths than wired networks. Attackers can exploit this feature, consuming network bandwidth with ease to prevent normal communication among nodes.

b. No predefined Boundary: In MANETs, we cannot exactly define a physical boundary of the networks. The nodes work in a nomadic environment where they are allowed to join and leave the wireless network. As soon as an adversary comes in the radio range of a node it will be able to communicate with that node.

c. Scalability: Due to mobility of nodes, scale of ad-hoc network changing all the time. So scalability is a major issue concerning security. Security mechanism should be capable of handling a large network as well as small ones.

***d. Resource availability*:** Resource availability is a major issue in MANETs. Providing secure communication in such changing environment as well as protection against specific threats and attacks, leads to development of various security schemes and architectures. Collaborative ad-hoc environments also allow implementation of self-organized security mechanism.

e. Lack of Centralized Management Facility: Ad hoc networks do not have a centralized piece of management machinery such as a name server, which lead to some vulnerable problems. Now let us discuss this problem in a more detailed manner First of all, the absence of centralized management machinery makes the detection of attacks a very difficult problem because it is not easy to monitor the traffic in a highly dynamic and large scale ad hoc network. Second, lack of centralized management machinery will delay the trust management for the nodes in the ad hoc network. Third, important algorithms in the mobile ad hoc network rely on the cooperative participation of all nodes and the infrastructure.

f. Cooperativeness: In MANETs, all routing protocols assume that nodes provide secure communication. But some nodes may become malicious nodes which disrupt the network operation by changing routing information etc.

g. Infrastructure less: MANETs is an infrastructure less network, there is no central administration. Each device can communicate with every other device, hence it becomes difficult to detect and manage the faults. In MANETs, the mobile devices can move randomly. The use of this dynamic topology results in route changes, frequent network partitions and possibly packet losses.

***h. Limited power supply*:** The nodes in mobile ad-hoc network need to consider restricted power supply, which will cause several problems. A node in mobile ad-hoc network may behave in a selfish manner when it is finding that there is only limited power supply.

i. Dynamic topology: Dynamic topology and changeable nodes membership may disturb the trust relationship among nodes. The trust may also be disturbed if some nodes are detected as compromised. This dynamic behavior could be better protected with distributed and adaptive security mechanisms.

j. Bandwidth Constraint: Variable low capacity links exists as compared to wireless network which are more susceptible to external noise, interference and signal attenuation effects.

***k. Adversary inside the Network*:** The mobile nodes within the MANETs can freely join and leave the network. The nodes within network may also behave maliciously. This is hard to detect that the behavior of the node is malicious. Thus this attack is more dangerous than the external attack. These nodes are called compromised nodes.

IV. ATTACKS IN MANET

Securing wireless ad-hoc networks is a highly challenging issue. Understanding possible form of attacks is always the first step towards developing good security solutions. Security of communication in MANET is important for secure transmission of information. Security means protecting the privacy (confidentiality), availability, integrity and non-repudiation. Security implies the identification of potential attacks from unauthorized access, use, modification or destruction. Earlier, various attempts have been made by various researchers [10-13] to classify the attacks on various layers. A complete picture of attack types on layers is helpful for the effectively mitigations of these attacks.

a) Passive Attacks: Some important passive attacks are: Snooping Attacks, Eavesdropping Attacks, Traffic Analysis Attacks, and Traffic Monitoring Attacks.

Snooping Attack is also known as masquerade or impersonation or spoofing Network attack. In this attack, a single malicious node attempts to take out the identity of other nodes' in the network by advertising false/fake routes. It then attempts to send packets over network with identity of other nodes making the destination believe that the packet is from original source [14]. The eavesdropping attack is a serious security threat to a wireless sensor network (WSN) since the eavesdropping attack is a prerequisite for other attacks. Traffic analysis is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted. In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic. Traffic analysis can be performed in the context of military intelligence or counter-intelligence, and is a concern in computer security. In this type of attack, an attacker tries to sense the communication path between the sender and receiver. This way attacker found the amount of data which is travel between the route of sender and receiver. There is no alteration in data by the traffic analysis. Monitoring is another passive attack in which attacker can see the confidential data, but he cannot change the data or cannot modify the data.

b) Active Attacks: Active attack: Some important passive attacks are: Blackmail, Denial of service attack, Fabrication, Gray hole Attacks, Disclosure Attacks, Routing Attacks and Recourse Consumption Attacks.

A black mail attack is relevant against routing protocols that uses mechanisms for identification of malicious nodes and propagate messages that try to blacklist the offender. Denial of service attacks are aimed at complete disruption of routing information and therefore the whole operation of ad-hoc network. The notation “fabrication” is used when referring to attacks performed by generating false routing messages. Such kind of attacks can be difficult to identify as they come as valid routing constructs, especially in the case of fabricated routing error messages, which claim that a neighbor can no longer be contacted [15]. Gray hole, a gray hole attack is a variation of the black hole attack, where the malicious node is not initially malicious, it turns malicious sometime later. In this attack, an attacker drops all data packets but it lets control messages to route through it [16]. Disclosure attacks are aimed at acquiring system-specific information about a website such as software distribution, version numbers, and patch levels. The acquired information might also contain the location of backup files or temporary files [17]. In Routing Attacks, attackers try to alter the routing information and data in the routing control packet. There are several types of routing attacks mounted on the routing protocol which are intended for disturbing the operation of the network In Resource Consumption Attack, a malicious node intentionally tries to consume or misuse of the resources (battery power, bandwidth, and computational power) of other nodes’ exist in the network by requesting excessive route discovery (unnecessary route request control messages), very frequent generation of beacon packets, or by forwarding unnecessary packets (stale information) to that node [18].

c) Collaborative attacks: Collaborative attacks (CA) occur when more than one attacker or running process synchronize their actions to disturb a target network. Multiple attacks occur when a system is disturbed by more than one attacker, but not necessarily in collaboration. We have study different types of attacks and then provided the definition of collaborative attacks; we are now going to categorize these attacks into two different categories. First: Direct Collaborative Attacks and Second: Indirect Collaborative Attacks.

Here, the attacker nodes are already in existence in the original network or a malicious node joins the network or an internal node is compromised in the network. This kind of collaborative attacks can be referred to as direct collaborative attacks. A Blackhole and Wormhole attack belongs to this category. In the black hole attack, attacker uses the routing protocol to advertise itself as having the best path to the node whose packets it want to intercept. An attacker use the flooding based protocol for listing the request for a route from the initiator, then attacker create a reply message he has the shortest path to the receiver . As this message from the attacker reached to the initiator before the reply from the actual node, then initiator assume that it is the shortest path to the receiver. So that a fake route is create. Once the attacker has been able to insert himself between the communications node, then attacker may able to do anything with the packet which is send by the initiator for the receiver [19]

V. CONCLUSION

Mobile Ad-Hoc Networks has the ability to deploy a network where a traditional network infrastructure environment cannot possibly be deployed. With the importance of MANET comparative to its vast potential it has still many challenges left in order to overcome. Security of MANET is one of the important features for its deployment.

The main goal of our thesis was to help improve the security in MANETs against collaborative black hole attacks. Firstly, we have analyzed the behavior and challenges of security threats in mobile ad hoc networks as well as how black hole attacks affect the performance and security for such networks. After some extensive research on many recent ideas of black hole attack prevention in MANETs, we were able to suggest ideas to address the problem of collaborative black hole attacks in MANETs.

Although many solutions have been proposed to mitigate the black hole attacks in MANETs, most of the solutions proposed were reactive in nature i.e. they can identify the malicious node only after the attack has been carried out by the malicious node. Many of these solutions are also only capable of mitigating single black hole attack and are not capable of avoiding collaborative black hole attack. For mitigation of black hole attack in MANETs, firstly, we proposed the SCAODV scheme, a feasible AODV based solution to mitigate black hole attacks in MANETs. We simulate our proposed solution using NS3 simulator and compare the performance with SAODV in terms Packet Delivery Ratio, Throughput and End-to-End Delay. Simulation result shown that the SCAODV performance is good as compare to SAODV.

REFERENCES

[1] Umesh Kumar Singh, Kailash Phuleria, Shailja Sharma & D.N. Goswami, An analysis of Security Attacks found in Mobile Ad-hoc Network, International Journal of Advanced Research in Computer Science, Volume 5, No. 5, pp. 34-39, May-June 2014.

[2] Umesh Kumar Singh, Kailash Phuleria, Shailja Sharma & D.N. Goswami, A Comparative study of Collaborative Attacks on Mobile Ad-Hoc Networks.

[3] H. Deng, W. Li, and D. P. Agrawal, "Routing security in wireless ad hoc networks," IEEE Communications Magazine, vol. 40, pp. 70-75, 2002

[4] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in Mobile Ad Hoc Networks: Challenges and Solutions," IEEE Wireless Communications, vol. 11, pp. 38-47, 2004.

[5] L. Peters, F. De Turck, I. Moerman, B. Dhoedt, P. Demeester, and A. A. Lazar, "Network layer solutions for wireless shadow networks," Proceedings of the International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, IC#/ICO#S/MCL'06, vol. 2006, p. 1628384, 2006.

[6] S. A. Razak, S. M. Furnell, and P. J. Brooke, "Attacks against Mobile Ad Hoc Networks Routing Protocols," 2004.

[7] C.-C. Chiang, "Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel," Proc. /E€€ SlCON '97, Apr. 1997, pp. 197-211.

[8] 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, October 2007, page, 85-91.

[9] Z. Karakehayov, "Using REWARD to Detect Team Black- Hole Attacks in Wireless Sensor Networks," Wksp. Real-World Wireless Sensor Networks, June 20–21, 2005.

[10] S. Lee, B. Han, and M. Shin, "Robust Routing in Wireless Ad Hoc Networks," 2002 Int'l. Conf. Parallel Processing Wksps., Vancouver, Canada, Aug. 18–21, 2002.

[11] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in Mobile Ad Hoc Networks: Challenges and Solutions," IEEE Wireless Communications, vol. 11, pp. 38-47, 2004.

[12] Shuyao Yu, Youkun Zhang, Chuck Song and Kai Chen, security architecture for Mobile Ad Hoc Networks". http://www.portal.prozhe118.com, pp.1-4.

[13] L. Peters, F. De Turck, I. Moerman, B. Dhoedt, P. Demeester, and A. A. Lazar, "Network layer solutions for wireless shadow networks," Proceedings of the International Conference on networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, , vol. 2, 2006.

[14] S. A. Razak, S. M. Furnell, and P. J. Brooke, "Attacks against Mobile Ad Hoc Networks Routing Protocols," www.scm.tees.ac.uk, pp.-1-6, 2004.

[15] A. Mishra, Security and Quality of Service in Ad Hoc Wireless Networks, 2008.

[16] L. Tamilselvan and V. Sankaranarayanan, "Prevention of co-operative black hole attack in MANET," Journal of networks, vol. 3, pp. 13-20, 2008.

[17] H. Deng, W. Li, and D. P. Agrawal, "Routing security in wireless ad hoc networks," IEEE Communications Magazine, vol. 40, pp. 70-75, 2002.

[18] S. Saraeian, F. Adibniya, M. GhasemZadeh, and S. Abtahi, "Performance Evaluation of AODV Protocol under DDoS Attacks in MANET," Proceedings of World Academy of Science, Engineering and Technology, vol. Vol. 33, pp. 501 - 503, September 2008.

[19] Abolhasan, M., Wysocki, T., and Dutkiewicz, E. A review of routing protocols for mobile ad hoc networks. Ad Hoc Networks, 2(1), 2004, pp. 1–22.