IJRSET May 2015 Volume 2, Issue 3 Pages: 57 - 62
ISSN 2394-739X
International Journal for Research in Science Engineering and Technology

A SURVEY SECURITY ISSUES IN MOBILE AD HOC NETWORKS

[1] Dr. G. Dalin,
[1] Assistant Professor,
[1] PG & Research Dept of Computer Science,
[1] Hindusthan College of Arts & Science,
[1] Coimbatore, Tamil Nadu India.

ABSTRACT: In this paper, we examine security issues and their present arrangements in the versatile specially appointed system. Owe to the defenseless way of the versatile specially appointed system, there are various security dangers that exasperate the advancement of it. We first break down the principle vulnerabilities in the portable impromptu systems, which have made it much less demanding to experience the ill effects of assaults than the customary wired system. At that point we examine the security criteria of the versatile specially appointed system and present the principle assault sorts that exist in it. At last we study the present security answers for the portable specially appointed system.

Keyword: [Mobile Ad Hoc Network, Security, Intrusion Detection, Secure Routing.]

1. INTRODUCTION

As of late, the hazardous development of portable processing gadgets, which for the most part incorporate tablets, individual advanced aides (PDAs) and handheld computerized gadgets, has induced a progressive change in the figuring scene: registering won't just depend on the ability gave by the PCs, and the idea of pervasive processing rises and gets to be one of the exploration hotspots in the software engineering society [1]. In the universal figuring environment, singular clients use, in the meantime, a few electronic stages through which they can get to all the required data at whatever point and wherever they might be [2]. The way of the pervasive processing has made it important to receive remote system as the interconnection technique: it is unrealistic for the universal gadgets to get wired system interface at whatever point and wherever they have to associate with different omnipresent gadgets. The Mobile Ad Hoc Network is one of the remote systems that have pulled in many focuses from numerous scientists.

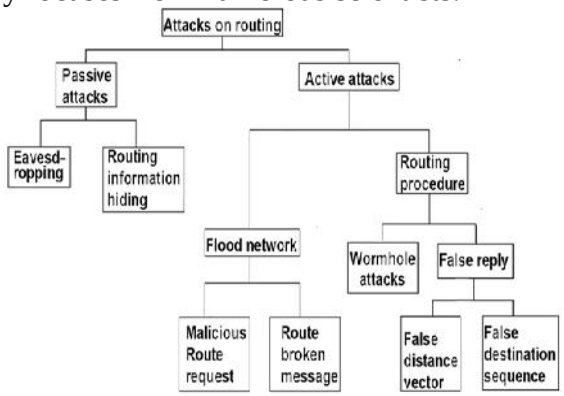

Figure 1-Security Attacks

2. VULNERABILITIES OF THE MOBILE AD HOC NETWORKS

Because mobile ad hoc networks have far more vulnerabilities than the traditional wired networks, security is much more difficult to maintain in the mobile ad hoc network than in the wired network. In this section, we discuss the various vulnerabilities that exist in the mobile ad hoc networks.

2.1. Lack of Secure Boundaries

The meaning of this vulnerability is self-evident: there is not such a clear secure boundary in the mobile ad hoc network, which can be compared with the clear line of defense in the traditional wired network. This vulnerability originates from the nature of the mobile ad hoc network: freedom to join, leave and move inside the network. Lack of secure boundaries makes the mobile ad hoc network susceptible to the attacks. The mobile ad hoc network suffers from all-weather attacks, which can come from any node that is in the radio range of any node in the network, at any time, and target to any other node(s) in the network. To make matters worse, there are various link attacks that can jeopardize the mobile ad hoc network, which make it even harder for the nodes in the network to resist the attacks. The attacks mainly include passive eavesdropping, active interfering, leakage of secret information, data tampering, message replay, message contamination, and denial of service [4].

2.2. Threats from Compromised nodes Inside the Network

In the previous subsection, we mainly discuss the vulnerability that there is no clear secure boundaries in the mobile ad hoc network, which may cause the occurrences of various link attacks. These link attacks place their emphasis on the links between the nodes, and try to perform some malicious behaviors to make destruction to the links. However, there are some other attacks that aim to gain the control over the nodes themselves by some unrighteous means and then use the compromised nodes to execute further malicious actions. This vulnerability can be viewed as the threats that come from the compromised nodes inside the network. Since mobile nodes are autonomous units that can join or leave the network with freedom, it is hard for the nodes themselves to work out some effective policies to prevent the possible malicious behaviors from all the nodes it communicate with because of the behavioral diversity of different nodes. Furthermore, because of the mobility of the ad hoc network, a compromised node can frequently change its attack target and perform malicious behavior to different node in the network, thus it is very difficult to track the malicious behavior performed by a compromised node especially in a large scale ad hoc network. Therefore, threats from compromised nodes inside the network are far more dangerous than the attacks from outside the network, and these attacks are much harder to detect because they come from the compromised nodes, which behave well before they are compromised.

2.3. 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 [7]. It is rather common in the ad hoc network that benign failures, such as path breakages, transmission impairments and packet dropping, happen frequently. Therefore, malicious failures will be more difficult to detect, especially when adversaries change their attack pattern and their attack target in different periods of time. For each of the victims, because it can only observe the failure that occurs in itself, this short-time observation cannot produce a

convincing conclusion that the failure is caused by an adversary.

However, we can easily find from a system point of view that the adversary has performed such a large amount of misbehaviors that we can safely conclude that all of the failures caused by this adversary should be malicious failure instead of benign failure, though these failures occur in different nodes at different time. From this example we find that lack of centralized management machinery will cause severe problems when we try to detect the attacks in the ad hoc network.

2.4. Restricted Power Supply

The first problem that may be caused by the restricted power supply is denial-of-service attacks [4]. Since the adversary knows that the target node is battery-restricted, either it can continuously send additional packets to the target and ask it routing those additional packets, or it can induce the target to be trapped in some kind of time-consuming computations. In this way, the battery power of the target node will be exhausted by these meaningless tasks, and thus the target node will be out of service to all the benign service requests since it has run out of power. Furthermore, a node in the mobile ad hoc network may behave in a selfish manner when it finds that there is only limited power supply, and the selfishness can cause some problems when there is a need for this node to cooperate with other nodes to support some functions in the network. Just take the cluster-based intrusion detection technique as an example [8]. In this technique, there is no need that every node in the ad hoc network is the monitoring node all the time; instead, a cluster of neighboring MANET nodes can randomly and fairly elect a monitoring node that will observe the abnormal behaviors in the network traffic for the entire cluster. However, an important precondition for the success of this technique is that every node in the cluster is willing to take their responsibility as a monitoring node and serve for all other nodes in a period of time.

2.5. Scalability

Finally, we need to address the scalability problem when we discuss the vulnerabilities in the mobile ad hoc network [4]. Unlike the traditional wired network in that its scale is generally predefined when it is designed and will not change much during the use, the scale of the ad hoc network keeps changing all the time: because of the mobility of the nodes in the mobile ad hoc network, you can hardly predict how many nodes there will be in the network in the future. As a result, the protocols and services that are applied to the ad hoc network such as routing protocol and key management service should be compatible to the continuously changing scale of the ad hoc network, which may range from decades of nodes to hundreds of nodes, or even thousands of nodes. In other words, these protocols and services need to scale

2.6. Vulnerabilities of the Mobile Ad Hoc Networks: Summary

From the discussion in this section, we can safely conclude that the mobile ad hoc network is insecure by its nature: there is no such a clear line of defense because of the freedom for the nodes to join, leave and move inside the network; some of the nodes may be compromised by the adversary and thus perform some malicious behaviors that are hard to detect; lack of centralized machinery may cause some problems when there is a need to have such a centralized coordinator; restricted power supply can cause some selfish problems; and continuously changing scale of the network has set higher requirement to the scalability of the protocols and services in the mobile ad hoc network. As a result, compared with the wired network, the mobile ad hoc network will need more robust security scheme to ensure the security of it. In the next section, we will survey several security solutions that can provide some helps to improve the security environment in the ad hoc network.

3. ATTACKS AGAINST ROUTING

Routing is one of the most important services in the network; therefore it is also one of the main targets to which attackers conduct their malicious behaviors. In the mobile ad hoc networks, attacks against routing are generally classified into two categories: attacks on routing protocols and attacks on packet forwarding/delivery [6]. Attacks on routing protocols aim to block the propagation of the routing information to the victim even if there are some routes from the victim to other destinations. Attacks on packet forwarding try to disturb the packet delivery along a predefined path. The main influences brought by the attacks against routing protocols include network partition, routing loop, resource deprivation and route hijack [6]. There are some attacks against routing that have been studied and well known [10] [11] [12] [13]: Impersonating another node to spoof route message. Advertising a false route metric to misrepresent the topology. Sending a route message with wrong sequence number to suppress other legitimate route Messages. Flooding Route Discover excessively as a DoS attack. Modifying a Route Reply message to inject a false route. Generating bogus Route Error to disrupt a working route. Suppressing Route Error to mislead others.

4. PRACTICAL ISSUES

4.1 On Node Failures

In real world organizations, a sensor hub can fail because of many factors, for example, physical damage or vitality consumption. Arobust flooding outline ought to be heartless to hub failures and minor topological changes. In Opportunistic Flooding, flooding packets are forwarded through a dynamically changing structure with redundant connections where the relating senders make the same choices to send. The failure of an astute flooding sender just results in a larger delay because of lower chances for the beneficiaries to get "early packets". Regardless of the possibility that its parent in the vitality optimal tree fails, a hub still has a high chance to get an opportunistically early packet from different senders, subsequently avoiding cascading failures as in tree-based plans.

4.2 On Link Quality Change

Join quality plays an important part in Opportunistic Flood-ing as it is a required contribution to almost every progression of the outline. It is in this manner preferable that the qualities of all the connections don't change once they are measured. In practice, in any case, join quality is affected by many environmental factors and changes after some time notwithstanding amid the interval between two measurements. Hence it is important to talk about if Opportunistic Flooding is still suitable for systems without-of-date connection quality information. Because of the occasional measurements, the connection quality may deviate marginally from the latest measured value. This deviation will potentially lead to two results: the loss of optimality of the vitality optimal tree (which further affects the accuracy of), and an EPD deviating from its accurate value. Be that as it may, the impact of both on Opportunistic Flooding is constrained, because and EPD just affect the basic leadership process. just a set number of hubs will make wrong choices, and hence either decreasing the chance of accepting "early packets" or increasing the chance of sending redundant packets.

CONCLUSION

In this survey paper, we try to inspect the security issues in the mobile ad hoc networks, which may be a main disturbance to the operation of it. Due to the mobility and open media nature, the mobile ad hoc networks are much more prone to all kind of security risks, such as information disclosure, intrusion, or even denial of service. As a result, the security needs in the mobile ad hoc networks are much higher than those in the traditional wired networks. First we briefly introduce the basic characteristics of the mobile ad hoc network. Because of the

emergence of the concept pervasive computing, there is an increasing need for the network users to get connection with the world anytime at anywhere, which inspires the emergence of the mobile ad hoc network. However, with the convenience that the mobile ad hoc networks have brought to us, there are also increasing security threats for the mobile ad hoc network, which need to gain enough attention.

REFERENCE

[1] Wenjia Li and Anupam Joshi , Security Issues in Mobile Ad Hoc Networks - A Survey .

[3] M.S. Corson, J.P. Maker, and J.H. Cernicione, Internet-based Mobile Ad Hoc Networking, IEEE Internet Computing, pages 63–70, July-August 1999.

[4] Amitabh Mishra and Ketan M. Nadkarni, Security in Wireless Ad Hoc Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 30), CRC Press LLC, 2003.

[5] Lidong Zhou and Zygmunt J. Hass, Securing Ad Hoc Networks, IEEE Networks Special Issue on Network Security, November/December 1999.

[6] Yongguang Zhang and Wenke Lee, Security in Mobile Ad-Hoc Networks, in Book Ad Hoc Networks Technologies and Protocols (Chapter 9), Springer, 2005.

[7] Panagiotis Papadimitraos and Zygmunt J. Hass, Securing Mobile Ad Hoc Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 31), CRC Press LLC, 2003.

[8] Yi-an Huang and Wenke Lee, A Cooperative Intrusion Detection System for Ad Hoc Networks, in Proceedings of the 1 st ACM Workshop on Security of Ad hoc and Sensor Networks, Fairfax, Virginia, 2003, pp. 135 – 147.

[9] Data Integrity, from Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Data_integrity.

[10] P. Papadimitratos and Z. J. Hass, Secure Routing for Mobile Ad Hoc Networks, in Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), San Antonio, TX, January 2002.

[11] Y. Hu, A. Perrig and D. Johnson, Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks, in Proceedings of ACM MOBICOM'02, 2002.

[12] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, A Secure Routing Protocol for Ad Hoc Networks, in Proceedings of ICNP'02, 2002.

[13] Y. Hu, D. Johnson, and A. Perrig, SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks, Ad Hoc Networks, 1 (1): 175–192, July 2003.

[14] Y. Hu, A. Perrig and D. Johnson, Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks, in Proceedings of IEEE INFOCOM'03, 2003.

[15] Y. Hu, A. Perrig and D. Johnson, Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols, in Proceedings of ACM MobiCom Workshop - WiSe'03, 2003.

[16] X. Jiao, W. Lou, X. Wang, J. Ma, J. Cao, and X. Zhou, "Interference- Aware Gossiping Scheduling in Uncoordinated Duty-Cycled MultiHop Wireless Networks," Proc. Wireless Algorithms, Systems, and Applications (WASA'10), 2010, pp. 192-202.

[17] A. Kamra, V. Misra, and D. Rubenstein, "CountTorrent: Ubiquitous Access to Query Aggregates in Dynamic and Mobile Sensor Networks," Proc. SenSys'07, 2007, pp. 1-15.

[18] A. Kanzaki, T. Uemukai, T. Hara, and S. Nishio, "Dynamic TDMA Slot Assignment in Ad Hoc Networks," Proc. 17th Int'l Conf. Advanced Information Networking and Applications (AINA'03), 2003, pp. 330-335.

[19] D. Kim and M. Liu, "Optimal Stochastic Routing in Low DutyCycled Wireless Sensor Networks," Proc. 4th Ann. Int'lConf. Wireless Internet (WICON), 2008, pp. 1-12.

[20] J.H. Kim and J.K. Lee, "Capture Effects of Wireless CSMA/CA Protocols in Rayleigh and Shadow Fading Channels," IEEE Trans.

Vehicular Technology, vol. 48, no. 4, pp. 1277-1286, July 1999.
[21] P. Kyasanur, R.R. Choudhury, and I. Gupta, "Smart Gossip: An Adaptive Gossip-based Broadcasting Service for Sensor Networks," Proc. IEEE Conf. Mobile Ad Hoc and Sensor Systems (MASS'06), 2006, pp. 91-100.
[22] S. Lai and B. Ravindran, "On Multihop Broadcast over Adaptively Duty-Cycled Wireless Sensor Networks," Proc. Int'l Conf. Distributed Computing in Sensor Systems (DCOSS'10), 2010, pp. 158-171.
[23] P. Levis, N. Patel, D. Culler, and S. Shenker, "Trickle: A Self-Regulating Algorithm for Code Propagation and Maintenance in Wireless Sensor Networks," Proc. 1st USENIX/ACM Symp. Networked Systems Design and Implementation (NSDI'04), 2004, pp. 15-28.
[24] K. Lin, J. Yu, J. Hsu, S. Zahedi, D. Lee, J. Friedman, A. Kansal, V. Raghunathan, and M. Srivastava, "Heliomote: Enabling LongLived Sensor Networks through Solar Energy Harvesting," Proc. SenSys'05, 2005, p. 1.
[25] G. Lu, N. Sadagopan, B. Krishnamachari, and A. Goel, "Delay Efficient Sleep Scheduling in Wireless Sensor Networks," Proc. INFOCOM'05, 2005, pp. 2470-2481.