Volume 4, Issue 2, February 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

An Analytical Approach for Security Measures Issues in MANET

Sakil Ahmad Ansari
Research Scholar
AFSET,Faridabad , Haryana,India

Prof. Saoud Sarwar
(HOD,CSE Deptt.)
AFSET,Faridabad , Haryana,India

Abstract: In this paper, we discuss security issues and their current solutions in the mobile ad hoc network. Owe to the vulnerable nature of the mobile ad hoc network, there are numerous security threats that disturb the development of it. We first analyze the main vulnerabilities in the mobile ad hoc networks, which have made it much easier to suffer from attacks than the traditional wired network. Then we discuss the security criteria of the mobile ad hoc network and present the main attack types that exist in it. Finally we survey the current security solutions for the mobile ad hoc network.

Key Words: Mobile Ad Hoc Network, Security, IDS, Secure Routing

1. Introduction

In recent years, the explosive growth of mobile computing devices, which mainly include laptops, personal digital assistants and handheld digital devices, has impelled are evolutionary change in the computing world: computing will not merely rely on the capability provided by the personal computers, and the concept of ubiquitous computing merges and becomes one of the research hotspots in the computer science society [1]. In the ubiquitous computing environment, individual users utilize, at the same time, several electronic platforms through which they can access all the required information whenever and wherever they may be [2]. The nature of the ubiquitous computing has made it necessary to adopt wireless network as the interconnection method: it is not possible for the ubiquitous devices to get wired network link whenever and wherever they need to connect with other ubiquitous devices. The Mobile Ad Hoc Network is one of the wireless networks that have attracted most concentrations from many researchers. A Mobile Ad hoc NETwork (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. People and vehicles can thus be internetworked in areas without a preexisting communication infrastructure or when the use of such infrastructure requires wireless extension [3]. In the mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes that not in the direct communication range use intermediate node(s) communicate with each other. In these two situations, all the nodes that have participated in hemmunication automatically form a wireless network, therefore this kind of wireless network can be viewed as mobile ad hoc network. The mobile ad hoc network has the following typical features [4]: Unreliability of wireless links between nodes. Because of the limited energy supply forthe wireless nodes and the mobility of the nodes, the wireless links between mobilenodes in the ad hoc network are not consistent for the communication participants. Constantly changing topology. Due to the continuous motion of nodes, the topology of the mobile ad hoc network changes constantly: the nodes can continuously move into and out of the radio range of the other nodes in the ad hoc network, and the routing information will be changing all the time because of the movement of the nodes. Lack of incorporation of security features in statically configured wireless routing protocol not meant for ad hoc environments. Because the topology of the ad hoc networks is changing constantly, it is necessary for each pair of adjacent nodes to incorporate in the routing issue so as to prevent some kind of potential attacks that try to make use of vulnerabilities in the statically configured routing protocol. Because of the features listed above, the mobile ad hoc networks are more prone to suffer from the malicious behaviors than the traditional wired networks. Therefore, we need to pay more attention to the security issues in the mobile ad hoc networks. The rest of the paper is organized as follows: In Section 2, we discuss the main vulnerabilities that make the mobile ad hoc networks not secure. In Section 3, we survey the current security solutions for the mobile ad hoc networks and analyze the feasibility of them. In Section 4, we draw the conclusion for the paper and point out some potential works in the future.

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. In the wired network, adversaries must get physical access to the network medium, or even pass through several lines of defense such as

firewall and gateway before they can perform malicious behavior to the targets [6]. However, in the mobile ad hoc network, there is no need for an adversary to gain the physical access to visit the network: once the adversary is in the radio range of any other nodes in the mobile ad hoc network, it can communicate with those nodes in its radio range and thus join the network automatically. As a result, the mobile ad hoc network does not provide the so-called secure boundary to protect the network from some potentially dangerous network accesses. 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, itis 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. A good example of this kind of threats comes from the potential *Byzantine failures* encountered in the routing protocol for the mobile ad hoc network [4]. We call it a Byzantine failure when a set of nodes are compromised in such a way that the incorrect and malicious behavior cannot be directly detected because of the cooperation among these compromised nodes when they perform malicious behaviors. The compromised nodes may seemingly behave well; however, they may actually make use of the flaws and inconsistencies in the routing protocol to undetectably destroy the routing fabric of the network, generate and advertise new routing information that contains nonexistent link, provide fake link state information, or even flood other nodes with routing traffic. Because the compromised nodes cannot be easily recognized, their malicious behaviors are prone to be ignored by other nodes. Therefore Byzantine failure is very harmful to the mobile ad hoc network.

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. Second, lack of centralized management machinery will impede the trust management for the nodes in the ad hoc network [4]. In mobile ad hoc network, all the nodes are required to cooperate in the network operation, while no security association (SA2) can be assumed for all the network nodes. Thus, it is not practical to perform an *a priori* classification, and as a result, the usual practice of establishing a line of defense, which distinguishes nodes as trusted and nontrusted, cannot be achieved here in the mobile ad hoc network. Third, some algorithms in the mobile ad hoc network rely on the cooperative participation of all nodes and the infrastructure. Because there is no centralized authority ,and decision making in mobile ad hoc network is sometimes decentralized, the adversary can make use of this vulnerability and perform some attacks that can break the cooperative algorithm [6]. In one word, the absence of centralized management machinery will cause vulnerability that can influence several aspects of operations in the mobile ad hoc network. Thus we should work out some solutions to deal with this problem, which might be discussed in the later section.

2.4. Restricted Power Supply

As we all know, due to the mobility of nodes in the ad hoc network, it is common that the nodes in the ad hoc network will reply on battery as their power supply method. While nodes in the wired network do not need to consider the power

supply problem because they can get electric power supply from the outlets, which generally mean that their power supply should be approximately infinite; the nodes in the mobile ad hoc network need to consider the restricted battery power, which will cause several problems. 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. There may be some nodes that behave selfishly and do not want to cooperate in the monitoring node election process, which will make the election fail if here are too many selfish nodes. Moreover, we should not view all of the selfish nodes as malicious nodes: some nodes may encounter restricted power supply problem and thus behave in a selfish manner, which can be tolerated; however, there can be some other node who intentionally announces that it runs out of battery power and therefore do not want to cooperate with other nodes in some cooperative operation, but actually this node still has enough battery power to support the cooperative operation. In a word, selfish behaviors should not be regarded as malicious behaviors, but we need to know if the selfishness is really caused by the limited battery power, or by the intentional non-cooperation.

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 eve thousands of nodes. In other words, these protocols and services need to scale

up and down efficiently.

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. Security Solutions to the Mobile Ad Hoc Networks

We have discussed several vulnerabilities that potentially make the mobile ad hoc networks insecure in the previous section. However, it is far from our ultimate goal to secure the mobile ad hoc network if we merely know the existing vulnerabilities in it. As a result, we need to find some security solutions to the mobile ad hoc network. In this section, we survey some security schemes that can be useful to protect the mobile ad hoc network from malicious behaviors.

3.1. Security Criteria

Before we survey the solutions that can help secure the mobile ad hoc network, we think it necessary to find out how we can judge if a mobile ad hoc network is secure or not, or in other words, what should be covered in the security criteria for the mobile ad hoc network when we want to inspect the security state of the mobile ad hoc network. In the following, we briefly introduce the widely-used criteria to evaluate if the mobile ad hoc network is secure.

3.1.1. Availability

The term *Availability* means that a node should maintain its ability to provide all the designed services regardless of the security state of it [4]. This security criterion is challenged mainly during the denial-of-service attacks, in which all the nodes in the network can be the attacktarget and thus some selfish nodes make some of the network services unavailable, such as the routing protocol or the key management service [5].

3.1.2. Integrity

Integrity guarantees the identity of the messages when they are transmitted. Integrity can be compromised mainly in two ways [9] Malicious altering :Accidental altering A message can be removed, replayed or revised by an adversary with malicious goal, which is regarded as malicious altering; on the contrary, if the message is lost or its content is changed due to some benign failures, which may be transmission errors in communication or hardware errors such as hard disk failure, then it is categorized as accidental altering.

3.1.3. Confidentiality

Confidentiality means that certain information is only accessible to those who have been authorized to access it. In other words, in order to maintain the confidentiality of some confidential information, we need to keep them secret from all entities that do not have the privilege to access them.

3.1.4. Authenticity

Authenticity is essentially assurance that participants in communication are genuine and not impersonators [4]. It is necessary for the communication participants to prove their identities as what they have claimed using some techniques so as to ensure the authenticity. If there isnot such an authentication mechanism, the adversary could impersonate a benign node and thus get access to confidential resources, or even propagate some fake messages to disturb the normal network operations.

3.1.5. Non repudiation

Non repudiation ensures that the sender and the receiver of a message cannot disavow that they have ever sent or received such a message. This is useful especially when we need to discriminate if a node with some abnormal behavior is compromised or not: if a node recognizes that the message it has received is roneous, it can then use the incorrect message as an evidence to notify other nodes that the node sending out the improper message should have been compromised.

3.1.6. Authorization

Authorization is a process in which an entity is issued a credential, which specifies the privileges and permissions it has and cannot be falsified, by the certificate authority. Authorization is generally used to assign different access rights to different level of users. For instance, we need to ensure that network management function is only accessible by the network administrator. Therefore there should be an authorization process before the network administrator accesses the network management functions.

3.1.7. Anonymity

Anonymity means that all the information that can be used to identify the owner or the current user of the node should default be kept private and not be distributed by the node itself or the system software. This criterion is closely related to privacy preserving, in which we should try to protect the privacy of the nodes from arbitrary disclosure to any other entities.

3.1.8. Security Criteria: Summary

We have discussed several main requirements that need to be achieved to ensure the security of the mobile ad hoc network. Moreover, there are some other security criteria that are more specialized and application-oriented, which include location privacy, self-stabilization and Byzantine Robustness, all of which are related to the routing protocol in the mobile ad hoc network. Having dealt with the main security criteria, we then move to the discussion on the main threats that violate the security criteria, which are generally called as attacks.

3.2. Attack Types in Mobile Ad Hoc Networks

There are numerous kinds of attacks in the mobile ad hoc network, almost all of which can be classified as the following two types [6]: (i). External attacks, in which the attacker aims to cause congestion, propagate fake routinginformation or disturb nodes from providing services. (ii). Internal attacks, in which the adversary wants to gain the normal access to the network and participate the network activities, either by some malicious impersonation to get theaccess to the network as a new node, or by directly compromising a current node and using it as a basis to conduct its malicious behaviors. In the two categories shown above, external attacks are similar to the normal attacks in the traditional wired networks in that the adversary is in the proximity but not a trusted node in the network, therefore, this type of attack can be prevented and detected by the security methods such as membership authentication or firewall, which are relatively conventional security solutions. However, due to the pervasive communication nature and open network media in the mobile ad hoc network, internal attacks are far more dangerous than the internal attacks: because the compromised nodes are originally the benign users of the ad hoc network, they can easily pass the authentication and get protection from the security mechanisms. As a result, the adversaries can make use of them to gain normal access to the services that should only be available to the authorized users in the network, and they can use the legal identity provided by the compromised nodes to conceal their malicious behaviors. Therefore, we should pay more attention to the internal attacks initiated by the malicious insiders when we consider the security issues in the mobile ad hoc networks. In the following, we discuss the main attack types that emerge in the mobile ad hoc networks.

3.2.1. Denial of Service (DoS)

The first type of attack is denial of service, which aims to crab the availability of certain node or even the services of the entire ad hoc networks. In the traditional wired network, the DoS attacks are carried out by flooding some kind of network traffic to the target so as to exhaust the processing power of the target and make the services provided by the target become unavailable. Nevertheless, it becomes not practical to perform the traditional DoS attacks in the mobile ad hoc networks because of the distributed nature of the services. Moreover, the mobile ad hoc networks are more vulnerable than the wired networks because of the

interference-prone radio channel and the limited battery power. In the practice, the attackers exactly use the radio jamming and battery exhaustion methods to conduct DoS attacks to the mobile ad hoc networks, which well correspond to the two vulnerabilities

Attack Types in Mobile Ad Hoc Networks: Summary

In this part, we mainly discuss the attack types in the mobile ad hoc networks. The attacks in MANET can be briefly classified into two categories: external attacks and internal attacks, latter of which are far more dangerous to the mobile

ad hoc network. Then we briefly introduce the main attack types in the mobile ad hoc network, which are denial-of-service (DoS) attacks, impersonation attacks, eavesdropping attacks and attacks against routing. In the next subsection, we will survey several popular security solutions to the attacks discussed ..

3.3. Security Schemes in the Mobile Ad Hoc Networks

In the previous subsection, we have introduced several well known attack types in the mobile ad hoc network. Therefore, it should be an appropriate time now to find some security schemes to deal with these attacks. In this part, we discuss several popular security schemes that aim to handle different kinds of attack listed in the previous subsection.

3.3.1. Intrusion Detection Techniques

Intrusion detection is not a new concept in the network research. According to the definition in the *Wikipedia*, an Intrusion Detection System (or IDS) generally detects unwanted manipulations to systems [17]. Although there are some differences between the traditional wired network and the mobile ad hoc network, intrusion detection technique, which is developed first in the wired network and has become a very important security solution for the wired network, has also gained some attentions from the researchers when they explore the security solution for the mobile ad hoc network. In the following, we discuss some typical intrusion detection techniques in the mobile ad hoc networks in details.

3.3.1.1. Intrusion Detection Techniques in MANET: the First Discussion

The first discussion about the intrusion detection techniques in the mobile ad hoc networks was presented in the paper written by Zhang et al. [18]. In this paper, a general intrusion detection framework in MANET was proposed, which was distributed and copperative to meet with the needs of MANET. The proposed architecture of the intrusion detection system is shown below in Figure 1.

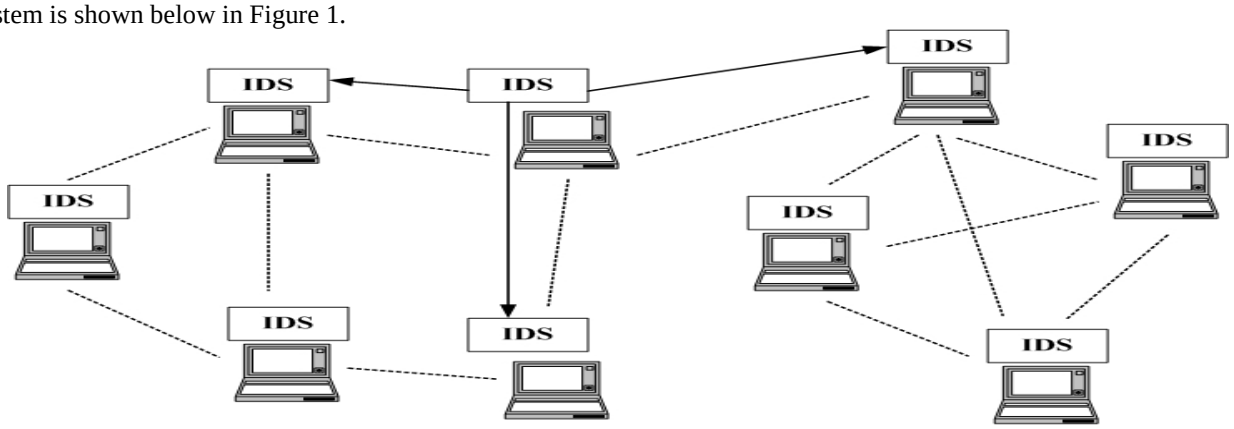

Figure 1. An IDS Architecture for MANET

In this architecture, every node in the mobile ad hoc networks participates in the intrusion detection and response activities by detecting signs of intrusion behavior locally and independently, which are performed by the built-in IDS agent. However, the neighboring nodes can share their investigation results with each other and cooperate in a broader range. The cooperation between nodes generally happens when a certain node detects an anomaly but does not have enough evidence to figure out what kind of intrusion it belongs to. In this situation, the node that has detected the anomaly requires other nodes in the communication

range to perform searches to their security logs in order to track the possible traces of the intruder. The internal structure of an IDS agent is shown in Figure 2 below.

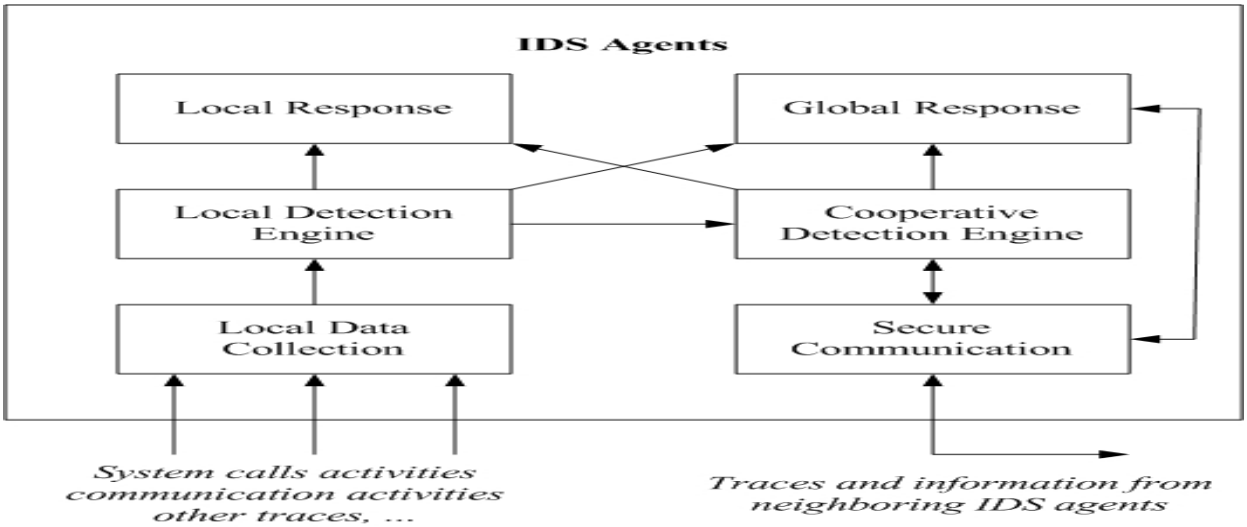

Figure 2. A Conceptual Model for an IDS Agent

Misbehavior Detection through Cross-layer Analysis

Multi-layer intrusion detection technique is another potential research area that Zhang et al. point out in their paper [18]. However, they seem not to explore deeper in this area. In this part, we will discuss the cross-layer analysis method presented by Parker et al. [19]. In this paper, the authors observe the attack behaviors in the MANET, and find that some *smart* attackers may simultaneously exploit several vulnerabilities at multiple layers but keep the attack to each of the vulnerabilities stay below the detection threshold so as to escape from capture by the single-layer misbehavior detector. This type of cross-layer attack will be far more threatening than the single-layer attack in that it can be easily skipped by the single-layer misbehavior detector. Nevertheless, this attack scenario can be detected by a cross-layer misbehavior detector, in which the inputs from all layers of the network stack are combined and analyzed by the cross-layer detector in a comprehensive way. The authors also present their attempt by working with RTS/CTS input from the 802.11 MAC layer combined with network layer detection of dropped packets. As far as I know, there are several aspects that can be further explored in this area. First of all, it will be an important problem that how to make the cross-layer detection more efficient, or in other words, how to cooperate between single-layer detectors to make them work well. Because different single-layer detectors deal with different types of attacks, there can be some different viewpoints to the same attack scenario when it is observed in different layers. Therefore it is necessary to figure out the possible solution if there are different detection results generated by different layers. Second, we need to find out how much the system resource and network overhead will be increased due to the use of cross-layer detector compared with the original single-layer detector. Due to the limited battery power of the nodes in the ad hoc networks, the system and network overhead brought by the cross-layer detection should be taken into account and compared with the performance gain caused by the use of cross-layer detection method.

3.3.2. Secure Routing Techniques in Mobile Ad Hoc Network

As we have discussed in Section 3.2.4, there are numerous kinds of attacks against the routing layer in the mobile ad hoc networks, some of which are more sophisticated and harder to detect than others, such as Wormhole attacks and Rush attacks. In this part, we first discuss these two kinds of sophisticated attacks and then we introduce *Watchdog* and *Pathrater*, which are two main components in a system that aims to mitigate the routing misbehaviors in mobile ad hoc networks [21]. Finally we move to a secure ad hoc routing approach using localized self-healing communities [22].

3.3.2.1. Defense Method Against Wormhole Attacks in Mobile Ad Hoc Networks

Wormhole attack is a threatening attack again routing protocols for the mobile ad hoc networks [14] [23]. In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them (possibly selectively) to another location, and replays them there into the network. The replay of the information will make great confusion to the routing issue in mobile ad hoc network because the nodes that

4. 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] M. Weiser, The Computer for the Twenty-First Century, *Scientific American*, September 1991.

[2] 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.

[3] 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.

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

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

[6] 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.

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

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

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

