International Journal of Research Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 01
January 2018

A Review on Issues and Counter Measures Pertaining Security in Mobile Adhoc Wireless Networks

Pooja Balhara

M. Phil. Scholar, Dr. C. V. Raman University, Chhattisgarh (India)
balhara.pooja2@gmail.com

Abstract

Mobile ad hoc networks (MANETs) are one of the fastest growing areas of research. They are an attractive technology for many applications, such as rescue and tactical operations, due to the flexibility provided by their dynamic infrastructure. However, this flexibility comes at a price and introduces new security threats. Furthermore, many conventional security solutions used for wired networks are ineffective and inefficient for the highly dynamic and resource-constrained environments where MANET use might be expected. To develop suitable security solutions for such new environments, we must first understand how MANETs can be attacked. This chapter provides a comprehensive survey of attacks against a specific type of target, namely the routing protocols used by MANETs. We introduce the security issues specific to MANETs and present a detailed classification of the attacks/attackers against these complex distributed systems. 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.

Keywords: *Security, Threats, Attacks, Issues, MANET.*

1. Introduction

In recent years, the explosive growth of mobile computing devices, which mainly include laptops, personal digital assistants (PDAs) and handheld digital devices, has impelled a revolutionary change in the computing world: computing will not merely rely on the capability provided by the personal computers, and the concept of ubiquitous computing emerges 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) to communicate with each other. In these two situations, all the nodes that have participated in the communication. 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 for the wireless nodes and the mobility of the nodes, the wireless links between mobile nodes 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

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 01
January 2018

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

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 01
January 2018

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, 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.

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. We find that the threats from compromised nodes inside the ad hoc network should be paid more attention, and mobile nodes and infrastructure should not easily trust any node in the network even if it behaves well before because it might have been 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.

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 non-trusted, 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 there 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

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 01
January 2018

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 even 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. 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]:

3.1 External Attacks

In which the attacker aims to cause congestion, propagate fake routing information or disturb nodes from providing services.

3.2 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 the access 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.

3.2.2. Impersonation

Impersonation attack is a severe threat to the security of mobile ad hoc network [4]. As we can see, if there is not such a proper authentication mechanism among the nodes, the adversary can capture some nodes in the network and make them look like benign nodes. In this way, the compromised nodes can join the network as the normal nodes and begin to conduct the malicious behaviors such as propagate fake routing information and gain inappropriate priority to access some confidential information.

3.2.3. Eavesdropping

Eavesdropping is another kind of attack that usually happens in the mobile ad hoc networks. The goal of eavesdropping is to obtain some confidential information that should be kept secret during the communication. The confidential information may include the location, public key, private key or even passwords of the nodes. Because such data are very important to the security state of the nodes, they should be kept away from the unauthorized access.

3.2.4. 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.

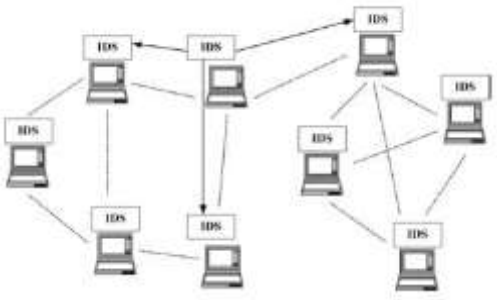
The main influences brought by the attacks against routing protocols include network partition, routing

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.



e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 01
January 2018

Figure 1: An IDS architecture for MANET

3.3. Security Schemes in the Mobile Ad Hoc Networks

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 01
January 2018

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.

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 01
January 2018

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.

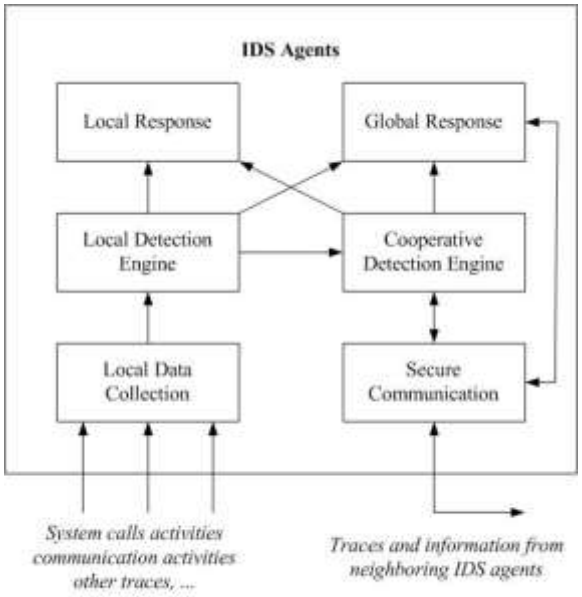


Figure 2. A Conceptual Model for an IDS Agent

In the conceptual model, there are four main functional modules:

Local data collection module, which mainly deals with the data gathering issue, in which the real-time audit data may come from various resources.

Local detection engine, which examines the local data collected by the local data collection module and inspects if there is any anomaly shown in the data. Because there are always new attack types emerging as the known attacks being recognized by the IDS, the detection engine should not expect to merely perform pattern recognition between known attack behaviors and the anomalies that are likely to be some intrusions: instead of the misuse detection technique that cannot deal with the novel attack types effectively, the detection engine should mainly rely on the statistical anomaly detection techniques, which distinguish anomalies from normal behaviors based

on the deviation between the current observation data and the normal profiles of the system.

Cooperative detection engine, which works with other IDS agents when there are some needs to find more evidences for some suspicious anomalies detected in some certain nodes. When there is a need to initiate such cooperated detection process, the participants will propagate the intrusion detection state information of themselves to all of their neighboring nodes, and all of the participants can calculate the new intrusion detection state of them based on all such information they have got from their neighbors by some selected algorithms such as a distributed consensus algorithm with weight.

Since we can make such a reasonable assumption that majority of the nodes in the ad hoc network should be benign, we can trust the conclusion drawn by any of the participants that the network is under attack.

Intrusion response module, which deals with the response to the intrusion when it has been confirmed. The response can be reinitializing the communication channel such as reassigning the key, or reorganizing the network and removing all the compromised nodes. The response to the intrusion behavior varies with the different kinds of intrusion.

In the paper, the authors also briefly discuss multi-layer integrated intrusion detection and response technique, in which the intrusion detection module should be set in each layer on each node of the mobile ad hoc network in order to get better performance on some attacks that may seem rather legitimate to the lower layers such as MAC protocol, but are much more easier to detect in the higher layers such as the application layer. The multi-layer integrated intrusion detection and response technique can greatly enhance the performance of the IDS especially when there are large amount of attacks that can be easily caught in the higher layer but are hard to find in the lower layer. The paper only presents the basic thought of the multi-layer integrated intrusion detection and response technique without providing more specific implementation detail.
In one word, this paper is known as the first paper that explores the intrusion detection techniques in the mobile ad hoc networks. It presents an architecture in which each of the nodes in the mobile ad hoc network should be equipped with an IDS agent, and all of the IDS agents can work independently and

locally as well as cooperative with each other to detect some intrusion behaviors in a larger range. In the paper, the authors also describe the conceptual model of the IDS agents and functionalities of different modules in the model.

Moreover, the paper also presents an intrusion detection and response scheme in which the IDS agents should be placed in each layer of each node such that some attacks can be detected earlier and more efficiently.

In my point of view, there are two points that this paper does not consider: one is the limited battery power problem that will cause some nodes to behave in a selfish manner during the cooperative intrusion detection process; the other is the possible overhead that is brought by the multi-layer integrated intrusion detection and response mechanism compared with the original single-layer intrusion detection mechanism, or, in other words, what the ratio of the performance enhancement over the overhead increase will be if we apply the multi-layer intrusion detection technique to the MANET.

The first point is considered by the authors themselves, which is shown in one of their later papers, and we will discuss that paper in next part. The second point seems not to get enough attention from the researchers, except that there is a preliminary discussion in the paper written by Parker et al. [19], which will also be discussed in this subsection.

3.3.1.2. Cluster-based Intrusion Detection Technique for Ad Hoc Networks

We have discussed a cooperative intrusion detection architecture for the ad hoc networks in the previous part, which was first presented by Zhang et al. However, all of the nodes in this framework are supposed to participate in the cooperative intrusion detection activities when there is such a necessity, which cause huge power consumption for all the participating nodes.

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 01
January 2018

Due to the limited power supply in the ad hoc network, this framework may cause some nodes behave in a selfish way and not cooperative with other nodes so as to save their battery power, which will actually violate the original intention of this cooperative intrusion detection architecture. To solve

this problem, Huang et al. present a cluster-based intrusion detection technique for ad hoc networks [8].

It is presented in this paper that A MANET can be organized into a number of clusters in such a way that every node is a member of at least one cluster, and there will be only one node per cluster that will take care of the monitoring issue in a certain period of time, which is generally called clusterhead. As is defined in the paper, a cluster is a group of nodes that reside within the same radio range with each other, which means that when a node is selected as the clusterhead, all of the other nodes in this cluster should be within 1-hop vicinity.

It is necessary to ensure the fairness and efficiency of the cluster selection process. Here fairness contains two levels of meanings: the probability of every node in the cluster to be selected as the clusterhead should be equal, and each node should act as the cluster node for the same amount of time. Efficiency of the process means that there should be some methods that can select a node from the cluster periodically with high efficiency. The finite state machine of the cluster formation protocol is shown in Figure 3 below.

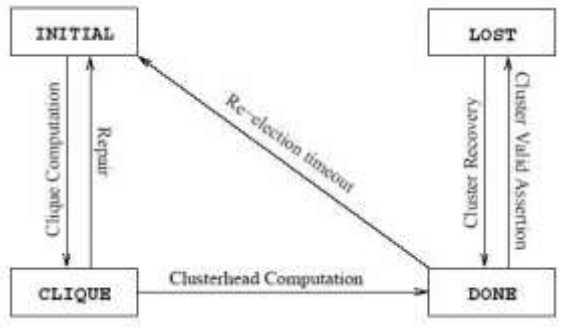


Figure 3. Finite State Machine of the Cluster Formation Protocol

Basically there are four states in the cluster formation protocol: initial, clique, done and lost.
All the nodes in the network will be in the initial state at first, which means that they will monitor their own traffic and detect intrusion behaviors independently. There are two steps that we need to finish before we get the clusterhead of the network: clique computation and clusterhead computation. A clique is defined as a group of nodes where every pair of members can communicate via a direct wireless link.

The definition of clique is a little more restricted than that of cluster. The authors use the cluster formation algorithm from [20] to compute cliques, the members of which are named citizens here in the paper. Once the protocol is finished, every node is aware of its fellow clique members. Then a node will be randomly selected from the clique to act as the clusterhead. There are two other protocols that assist the cluster doing some validation and recovery issues, which are respectively called Cluster Valid Assertion Protocol and Cluster Recovery Protocol. The cluster valid assertion protocol has generally been used in the following two situations:

The node in the cluster will periodically use the Cluster Valid Assertion Protocol to check if the connection between the clusterhead and itself is maintained or not. If not, this node will check to see if it belongs to another cluster, and if it also get negative answer, then the node will enter the LOST state and initiate a routing recovery request.

Furthermore, there need to be a mandatory re-election timeout for the clusterhead to keep the fairness and security of the whole cluster. If the timeout expires, all the nodes switch from DONE state to INITIAL state and begin a new round of clusterhead election.

The Cluster Recovery Protocol is mainly used in the case that a citizen loses its connection with previous clusterhead or a clusterhead loses all its citizens, when it enters LOST state and initiates Cluster Recovery Protocol to re-discover a new clusterhead.

In the paper the authors have justified their cluster-based intrusion detection technique by some experiments that make performance evaluation. From the results we can find that the
CPU speedup is increased for the cluster-based IDS method than the per-node based IDS method, at the same time the network overhead for the cluster-based IDS methods is lower than that for the per-node based IDS method. However, the detection rate of the cluster-based IDS method is slightly lower than that of the per-node IDS method, which may be reasonable because from a whole cluster point of view, there will only be one node that monitor the traffic for the whole cluster, which can make some inaccurate judgments because of the limited processing power of just one node.

3.3.1.3. 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.

3.3.1.4. Intrusion Detection Techniques in MANET: Summary

In this part, we survey several typical intrusion detection techniques in the mobile ad hoc networks. Due to the constantly changing topology and limited battery power, the intrusion
detection mechanism in the mobile ad hoc networks should be cooperative and energy-efficient, which are shown in the two papers written by Zhang et al. and Huang et al., respectively [18] [8]. Due to the mobility of the nodes and the continuously changing topology in the ad hoc network, it is sometimes relatively hard to collect the enough evidences for a node if it only relies on the single-layer detection method, where it may be vulnerable for the setting of the threshold. As a result, the concept of multi-layer or cross-layer detection mechanism is raised and discussed in [18] and [19].

The intrusion detection mechanisms discussed above contain some good thoughts, which have been proved by the experiments and simulations. However, there are still some problems that need to be further explored in the future.

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 get the replayed packets cannot distinguish it from the genuine routing packets. Moreover, for tunneled distances longer than the normal wireless transmission range of a single hop, it is simple for the attacker to make the tunneled packet arrive with better metric than a normal multi-hop route, which makes the victim node be more likely to accept the tunneled packets instead of the genuine routing packets. As a result, the routing functionality in the mobile ad hoc network will be severely interfered by the wormhole attack. For example, most existing ad hoc network routing protocols, without some mechanism to defend against the wormhole attack, would be unable to find routes longer than one or two hops, severely disrupting communication.

There are two main leashes, which are *geographical leashes* and *temporal leashes*. A geographical leash ensures that the recipient of the packet is within a certain distance from the sender. A temporal leash ensures that the packet has an upper bound on its lifetime, which restricts the maximum travel distance, since the packet can travel at most at the speed-of-light.

Either type of leash can prevent the wormhole attack, because it allows the receiver of a packet to detect if the packet traveled further than the leash allows. A geographical leash in conjunction with a signature scheme (i.e., a signature providing nonrepudiation), can be used

to catch the attackers that pretend to reside at multiple locations: when a legitimate node overhears the attacker claiming to be in different locations that would only be possible if the attacker could travel at a velocity above the maximum node velocity v, the legitimate node can use the signed locations to convince other legitimate nodes that the attacker is malicious.

In practice, the paper presents the design of TIK protocol that implements the temporal leashes. The TIK protocol implements temporal leashes and provides efficient instant authentication for broadcast communication in wireless networks. TIK stands for *TESLA with instant key disclosure*, and is an extension of the TESL protocol [24]. When used in conjunction with precise timestamps and tight clock synchronization, TIK can prevent wormhole attacks that cause the signal to travel a distance longer than the nominal range of the radio, or any other range

that might be specified. The TIK protocol has been proved to be efficient since it requires just public keys in a network with nodes, and has relatively modest storage, per packet size, and computation overheads.

In sum, this paper first introduces the wormhole attack, a rather dangerous attack that can have serious consequences on many proposed ad hoc network routing protocols. To detect and defend against the wormhole attack, the paper then introduces the concept of *packet leashes*, which may be either *geographic* or *temporal* leashes, to restrict the maximum transmission distance of a packet. Finally, to implement temporal leashes, the paper presents the design and performance analysis of a novel, efficient protocol, called TIK, which also provides instant authentication of received packets.

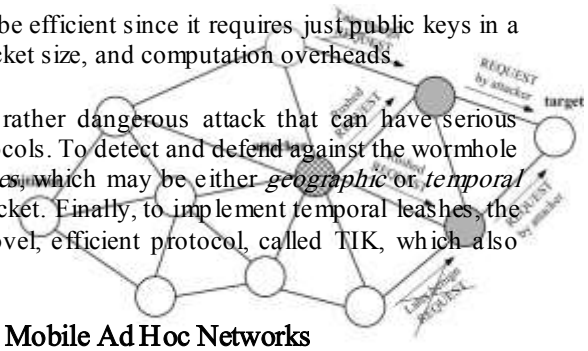


Figure 4. Rush Attack in the Example Ad Hoc Network

3.3.2.2. Defense Mechanism against Rushing Attacks in Mobile Ad Hoc Networks

Rushing attack is a new attack that results in denial-of-service when used against all previous on-demand ad hoc network routing protocols [15]. This attack is also particularly damaging because it can be performed by a relatively weak attacker. The implementation details of rushing attacks are shown in the Figure 4.

In the network shown in Figure 4, the initiator node initiates a Route Discovery for the target node. If the ROUTE REQUESTs for this Discovery forwarded by the attacker are the first to reach each neighbor of the target (shown in gray in the figure), then any route discovered by this Route Discovery will include a hop through the attacker. That is, when a neighbor of the target receives the rushed REQUEST from the attacker, it forwards that REQUEST, and will not forward any further REQUESTs from this Route Discovery. When non-attacking REQUESTs arrive later at these nodes, they will discard those legitimate REQUESTs. As a result, the initiator will be unable to discover any usable routes (i.e., routes that do not include the attacker) containing at least two hops (three nodes).

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 01
January 2018

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 01
January 2018

The rushing attack applies to all proposed on-demand protocols because such protocols must limit the number of packets that any node will transmit in response to a single Route Discovery. Currently proposed protocols choose to forward at most one REQUEST for each Discovery; any protocol that allows an attacker to predict which ROUTE REQUEST(s) will be chosen for forwarding at each hop will be vulnerable to some variant of the rushing attack.

In the paper, the authors describe a set of generic mechanisms that together defend against the rushing attack: *secure Neighbor Detection*, *secure route delegation*, and *randomized* ROUTE REQUEST *forwarding*. The relations among these security mechanisms are shown in Figure 5 below.

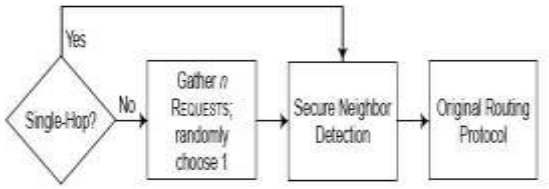


Figure 5. Combined Mechanisms to Secure MANET against Rushing Attacks

Secure Neighbor Detection allows each neighbor to verify that the other is within a given maximum transmission range. Once a node *A* forwarding a ROUTE REQUEST determines that node *B* is a neighbor (that is, is within the allowable range), it signs a *Route Delegation* message, allowing node *B* to forward the ROUTE REQUEST. When node *B* determines that node *A* is within the allowable range, it signs an *Accept Delegation* message. In this way,

the neighborhood relationships between nodes can be verified and guaranteed to be genuine.

Randomized selection of the ROUTE REQUEST message to forward, which replaces traditional duplicate suppression in on-demand route discovery, ensures that paths that forward REQUESTs with low latency are only slightly more likely to be selected than other paths, but not guaranteed to be selected.

The paper also presents a protocol to protect the ad hoc networks from rush attacks, which is called Rushing Attack Prevention (RAP). When integrated with a secure routing protocol, RAP incurs *no cost* unless the underlying secure protocol cannot find valid routes. When RAP is enabled, it incurs higher overhead than do standard Route Discovery techniques, but it can find usable routes when other protocols cannot, thus allowing successful routing and packet delivery when other protocols may fail entirely. In summary, equipped with these mechanisms, the ad hoc routing protocols will be more immune to the rush attacks. Because the approach is generic, any protocol that relies on duplicate suppression in Route Discovery can use our results to fend off rushing attacks. It is also shown in the simulation results that this approach is efficient without introducing too many extra overheads.

3.3.2.3. Watchdog and Pathrater

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 01
January 2018

Watchdog and Pathrater are two main components of a system that tries to improve performance of ad hoc networks in the presence of disruptive nodes, the specific working principles of which are discussed below [21] [25].

Watchdog determines misbehavior by copying packets to be forwarded into a buffer and monitoring the behavior of the adjacent node to these packets. Watchdog promiscuously snoops to decide if the adjacent node forwards the packets without modifications or not. If the packets that are snooped match with the observing node's buffer, then they are discarded;

whereas packets that stay in the buffer beyond a timeout period without any successful match are flagged as having been dropped or modified. The node responsible for forwarding the packet is then noted as being suspicious. If the number of violations becomes greater than a certain predetermined threshold, the violating node is marked as being

malicious. Information about malicious nodes is passed to the Pathrater component for inclusion in path rating evaluation.

Pathrater on an individual node works to rate all of the known nodes in a particular network with respect to their reliabilities. Ratings are made, and updated, from a particular node's perspective. Nodes start with a neutral rating that is modified over time based on observed reliable or unreliable behavior during packet routing. Nodes that are observed by watchdog to
have misbehaved are given an immediate rating of -
100. It should be distinguished that misbehavior is detected as packet mishandling/modification, whereas unreliable behavior is detected as link breaks.

It is shown from the experiments that these two components can well reflect the reliability of the nodes based on their packet forwarding performances.

3.3.2.4. A Secure Ad Hoc Routing Approach using Localized Selfhealing Communities

The paper first describes two routing attacks that use non-cooperative network members and disguised packet losses to deplete ad hoc network resources and to reduce ad hoc routing performance, which are called *RREQ resource depletion* and *RREP packet and data packet loss*, respectively [22]. These two attacks have not been fully addressed in previous research, so it is necessary to introduce these two attacks first.

In the *RREQ resource depletion* attack, an attacker sends RREQ packets, which the underlying on-demand routing protocol floods throughout the network. If the attacker is not a network member, cryptographic authentication can be added to RREQ packets to filter out those forged route discovery requests. However, if the attacker is a compromised or selfish network member, the cryptographic countermeasures are ineffective. In the *RREP packet and data packet loss* attack, when a route discovery procedure is initiated by a good network member, an attacker can use "wormhole attack" [14] or "rushing attack" [15] to surpass other nodes with respect to the underlying routing metric. Then it is highly likely the attacker is selected en route. When the RREP comes back it may not forward or may forward a corrupted

one. The result is equivalent to RREQ resource depletion attack, except now the RREQ initiator is not the one to blame. Also an attacker can severely degrade data delivery performance by selectively dropping data packets [26].

Next we briefly discuss the concept of "self-healing community" and its application in the secure ad hoc routing. The concept of "self-healing community" is based on the observation that wireless packet forwarding typically relies on more than one immediate neighbor to relay packets. Community-based security explores node redundancy at each forwarding step so that the conventional per-node based forwarding scheme is seamlessly converted to a new per community based forwarding scheme. Since a self-healing community is functional as long as there is at least one cooperative "good" node in the community, there is no requirement that how many nodes in the community should be available to provide reliable packet forwarding services. There are one configuration and one reconfiguration protocol that can respectively be used to initially set up the self-healing community and fix the community if there is a shape loss due to the mobility or change of topology.

The paper also presents an analytical analytic model to verify the effectiveness of community based secure routing. Moreover, the paper provides some simulation results to evaluate the performance of the community-based security routing scheme.

In one word, this paper presents a novel security scheme based on the concept of "Self-healing community", in which the community-based security should always be more important than the security of a single node. The paper also works out some practical solutions to set up and maintain such a self-healing community. Finally, an analytical model and some simulation results are provided to prove the performance of the scheme.

3.3.2.5. Secure Routing Techniques in Mobile Ad Hoc Networks: Summary

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 01
January 2018

In this part, we mainly discuss various secure routing techniques that can help ensure the ad hoc routing security. Some of them deal with specific attacks that aim to disturb the ad hoc routing services, and provide some solutions to help defend against these attacks; whereas other techniques try to provide some

effective tools or schemes to protect the ad hoc routing services from all kinds of attacks. Because routing service is one of the most important network services in the mobile ad hoc networks, there may be newly emerging attack types against the ad hoc routing all the time. Thus we need to constantly find new solutions to defend the ad hoc routing service against them.

3.3.3. Security Schemes in the Mobile Ad Hoc Networks: Summary

We mainly discuss two kinds of popular security techniques in the mobile ad hoc network, which are intrusion detection techniques and secure routing techniques. In each of the security schemes, several specific methods are pointed out and compared with each other. There are some points that some of the methods lack of, which are based on our observations. Therefore, we point out some aspects that may be further explored for some of the methods we have mentioned in this subsection.

3.4. Security Solutions in the Mobile Ad Hoc Networks: Summary

In this section, we survey the security solutions in the mobile ad hoc networks. First we analyze the main security criteria for the mobile ad hoc networks, which should be regarded as a guideline for us to find the solutions to the security issues in the mobile ad hoc networks. We then point out various attack types that mainly threaten the mobile ad hoc networks.

According to these attack types, we survey several security schemes that can partly solve the security problems in the mobile ad hoc networks.

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.

hoc Networking & Computing, pp. 146-155, 2001
[4] Buchegger S., Tissieres C., Le Boudec J.-Y.,"A Test-Bed for Misbehaviour Detection in Mobile Ad-Hoc Networks –How Much Can Watchdogs Really Do?", Mobile Computing Systems and Applications (WMCSA '04), pp. 102-111, 2004
[5] Ning P., Sun K., "How to Misuse AODV: A Case Study of Insider Attacks against Mobile Ad-hoc Routing Protocols", In Proc. of the IEEE Workshop on Information Assurance, pp. 60-67, 2003
[6] Stajano F., Anderson R., "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks", In Proc. of Int. Workshop on Security Protocols, Springer, 1999
[7] Yi P., Dai Z., Zhang S., Zhong Y., "A New Routing Attack in Mobile Ad Hoc Networks", Int. Journal of Information Technology, vol. 11, No. 2, pp. 83-94, 2005
[8] Wu B., Chen J., Wu J., Cardei M., "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", Wireless/Mobile Network Security, Chapter 12, Springer, 2006
[9] Hu Y.-C., Perrig A., Johnson D.B., "Rushing Attacks and Defence in Wireless Ad Hoc Network Routing Protocols", In Proc. of the ACM Workshop on Wireless Security, 2003
[10] Karlof C., Wagner D., "Secure Routing in Wireless Sensor Networks: Attacks and

Countermeasures", Ad Hoc Networks, pp. 293-315, 2003
[11] Hu Y.-C., Perrig A., Johnson D.B., "Packet Leashes: A Defence against Wormhole Attacks in Wireless Ad Hoc Networks", In Proc. of INFOCOM, 2003
[12] Li Y., Wei J., "Guidelines on Selecting Intrusion Detection Methods in MANET", In Proc. of Information Systems Educators Conference, 2004