Attacks and Intrusion Detection in Mobile Ad Hoc Networks

Assignment in Computer Science

Philippe Hunberbühler
04-706-016

March 18, 2007

Supervisors:
Prof. Dr. Burkhard Stiller
Dr. Hasan
Gregor Schaffrath

University of Zurich
Department of Informatics

Abstract

Mobile ad hoc networks (MANET) have gained in importance. Although MANETs are spontaneously built, fast deployed and have a rapidly changing environment, there is a need for security.
This paper covers the topic of attacks and intrusion detection in mobile ad hoc networks. First, it gives a short insight into the basic of intrusion detection systems and mobile ad hoc networks. Further, the vulnerabilities, caused by the particular characteristics of MANETs, are analyzed and the attacks that can be derived from them are explained in more details. Last, approaches and solutions of intrusion detection are shown. Here, as well, the particular characteristics of MANET make it partially impossible to use approaches, used in traditional, wired networks. Even though intrusion prevention is also required, this topic is not covered in this paper.

Zusammenfassung

Diese Arbeit befasst sich mit dem Thema Attacken und Intrusion Detection in mobilen ad hoc Netzwerken. Als erstes werden die Grundlagen von Intrusion Detection und mobilen ad hoc Netzwerken (MANET) aufgezeigt. Insbesondere die speziellen Eigenschaften von MANETs werden hervorgehoben, die als eine Ausgangslage für die Analyse der Verwundbarkeiten der MANETs herangezogen werden können. Weiter werden diese Verwundbarkeiten genauer analysiert und mögliche Attacken, die von diesen Verwundbarkeiten abgeleitet werden können, genauer beschrieben. Als letztes werden Versuche und Ansätze zur Intrusion Detection aufgezeigt. Dabei wird nicht auf die Problematik der Intrusion Prevention, die für ein sicheres System auch unentbehrlich ist, eingegangen.

Contents

Chapter 1

Introduction

The current development of mobile communications allows users to be connected to any kind of network, including GSM, WLAN, Bluetooth etc, almost everywhere. The demand on mobility pushes the research and development to new, faster and long-distance communication techniques.

Besides the traditional networks with infrastructure the demand on fast and spontaneously deployable networks arises. Ad hoc networks are not only used where the deployment has to be done rapidly, but also where it is not possible or not economic to use or to build up an infrastructure. Nowadays, it is no problem to build an ad hoc network using only two mobile devices, *e.g.*, two notebooks. The only requirement is that they have a communication interface.

This development requires advances in security. However, a lot of known security measures cannot be used in an ad hoc environment or have to be adapted to the circumstances. Security is mainly achieved by prevention, i.e. to make attacks as difficult as possible. However, once an attack has been successful, it has to be recognized and the appropriate actions have to be triggered. This is the part of the detection. Its goal is to minimize the damage of the attack.

Intrusion detection has to deal with different difficulties. The detection of an intrusion has to be done in a fast and effective manner. However, it must not produce many false alarms. IDSs are originally designed for wired networks and work only under certain conditions, i.e. having an infrastructure with central authority, no cooperative algorithms, only slowly changing topology etc. These conditions are not or only partially fulfilled by MANETs.

This paper gives first an overview of intrusion detection systems (IDS) in chapter 2 and mobile ad hoc networks (MANET) in chapter 3. In the chapter 4 the vulnerabilities of MANETs are shown and the attacks that can be derived from these vulnerabilities are discussed. Solutions and approaches regarding these vulnerabilities and attacks are showed and evaluated in chapter 5.

Chapter 2

Intrusion Detection Systems

Nowadays, a huge number of open networks exists, which a lot of mobile communication device can easily connect to. Therefore it is absolutely necessary to make the networks secure, so that no unauthorized person may connect to the network, get information which are not send to the person or disturb the traffic of the network. The security is achieved by two main steps: prevention and detection. *Prevention* are the actions that are implemented before an attack has happened to avoid them. These measures try to make successful attacks impossible or to hamper the attack, so that they are only successful with a huge effort. Established examples are firewalls, authentification or encryption. However, if an attack has already successfully been proceeded, there is a need to *detect* the attack and trigger countermeasures. To minimize the damage of such an attack, it is necessary to detect the attack as early as possible.

Bace and Mell [BM01] describe intrusion detection system (IDS) as software or hardware that monitors the activity and events in a network and analyzes them for security problems. Intrusion detection is the process of observing the activities in a network and analyzing them for indication of an intrusion. Intrusion is an attempt to compromise the integrity, availability or the confidentiality of the network or computer.

The chapter has following structure. The targets of attackers are described in a first section. The basic functionality of an intrusion detection system is described thereafter and examines the main functionalities more deeply. Finally, the chapter shows the different control strategies an intrusion detection system may have.

2.1 Targets

The intention or purpose of an attack is in the following named as the *target*. Most attackers have an object while attacking a network, *e.g.*, getting access to confidential information, spoofing the own identity etc. The target of an attack to networks may vary widely. Stajano and Anderson [SA99] name four targets: availability, authenticity, confidentiality and integrity. In the following these targets are described more deeply .

2.1.1 Confidentiality

Attacks against confidentiality aims at getting access to private or confidential data, for instance user names and passwords, credit card numbers, secret reports etc. To keep the confidentiality, it is required to ensure to communicate with right partner. Stajano and Ross [SA99] claims that confidentiality is *simply a matter of encrypting the session with whatever key material is made available by the authentication process.*

2.1.2 Availability

Availability is ensuring that a service is for users available when they expected. Availability is one of the most important properties a system might have [SA99]. A not working service is worthless to a user that has a need at that moment for this service. For instance, a user wants to order tickets for a movie theatre, but at the time he wants to order them the online-service is not available, so that he has to order the tickets on a different way and the service has not fulfilled its purpose.

2.1.3 Authenticity

Authenticity means the verifying and proving the identity of the participants in a network. This is in most safety aspect a prerequisite, *e.g.*, sending a password to an untrusted server is risky. Many authentication protocols are design to prove the identity of a specific participant, but these protocols use often a service of a third party, *e.g.*, certificate server of VeriSign.

2.1.4 Integrity

Integrity means that the system is not maliciously altered. There are two kinds of integrity: the integrity of the whole system and the one concerning data. Former means that the nodes and their behavior are not modified by an attacker. Latter defines that the nodes can relay that the data is not being changed during transmission.

2.2 Functionality

There are a lot of different intrusion detection systems. Depending on the environment, requirements of the IDSs differ from one another quite largely. However, there are three main components in which an intrusion detection system can be classified. Most of the IDSs implement all of the following components [BM01]:

- *Information Sources*: This component determine, from where the IDS get the information of the activities and events within the network. The information is used by Analysis.
- *Analysis*: The Analysis is the part where the decision, based on the gathered information, is made, whether an attack is being performed or whether has already happened or not.

- *Response*: The response is the action that is initiated by the IDS, once the analysis has identified an intrusion. The action involves not only the system, but also humans that decide what action should be taken based on reports generated by the IDS.

2.3 Information Sources

Basically, there are two different possibilities to collect information in a network. Either the IDSs analyze the network packets, captured form the backbone of the network or it analyze data generated by the host, that is the application or the operation system on the individual nodes. In the following the approaches network-based and host-based are introduced [BM01].

2.3.1 Network-Based IDSs

The majority of the commercial intrusion detection systems are implemented as network-based IDSs. The information is gathered by sensors, which are placed in segments of the network . The sensors are well hidden, in order to complicate the determination of their presence or location.

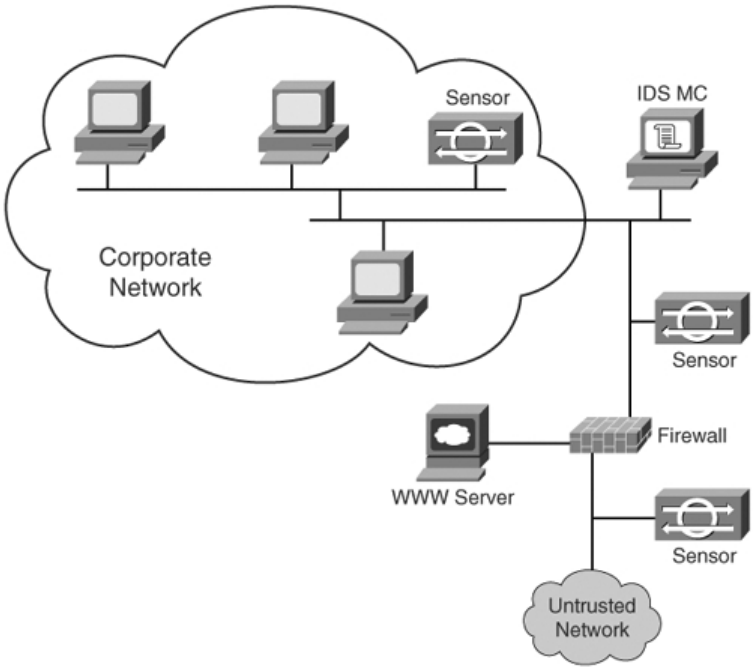

Figure 2.1: Network-based IDS [AW05]

As in figure 2.1 showed, the sensors capture packets and perform a local analysis. In the case of an intrusion the sensors send the result to central management console (IDS MC).

Advantages

- Network-based IDSs are without any attracting attention, almost invisible, which makes them secure against attacks.
- With a network-based IDSs there are no changes or only small ones in the architecture/infrastructure necessary. Moreover, it does not constrict with the operation of the network.
- Placing the sensor on crucial points, few sensors can monitor a large network.

Disadvantages

- In a large and busy network the sensors have to analyze an enormous amount of data, which makes them more likely to fail.
- Network-based IDSs are not applicable in networks where the traffic is encrypted.
- Network-based IDS detect only the attempt of an attack. Only in exceptional cases network-based IDS can resolve if the attack was successful or not. At this point a human has to take over.

2.3.2 Host-Based IDSs

In host-based IDS the collection of the data takes place at the individual participants of the network (see figure 2.2). It uses either the operating system audit trails or the system logs. Audit trails are generated by the kernel of the OS and are much more detailed than the system logs.

Even using the less accurate system logs allows a better analysis of what happens within the network than with a network-based IDS. Unlike to network-based IDSs, host-based IDSs are able to ascertain whether an attack has been successful. The reason is that the collection takes place almost at the point where the attack is accomplished, that is right at the computer system. It exist decentralized host-based IDS solutions, where the hosts report their findings to a single management console.

Bace and Mell describe in [BM01] a third information source: *application-based IDS*, which is subset of the host-based IDS. The information is gathered not on operating system level, but on application level. However, the differences between these two techniques are rather small. Therefore, in many paper this two types are not discussed separately [YZ03, BK03].

Advantages

- With the ability to gather information locally, host-based IDSs detect attacks which network-based would not.
- In contrast to network-based IDSs, host-based can be utilized in encrypted network traffic (only if the information source is before the encryption takes place at the sender, respectively after the decryption at the recipient).

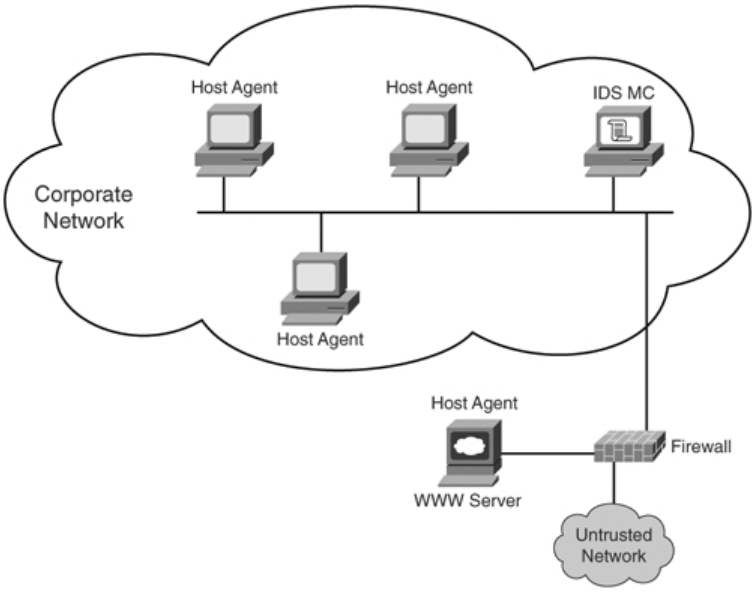

Figure 2.2: Host-based IDS [AW05]

Disadvantages

- The management of the system is more complex, because the management and configuration has to be done on every host individually.
- An attack may not only hit the node, but also disable a part of the IDS, *e.g.*, certain denial-of-service attacks disarm host-based IDSs [BM01]. On this way it losses its reliableness.
- The amount of data that has to be analyzed might be tremendous, especially if the operating system audit trails are used. The analysis is made by the hosts, using their computation power for intrusion detection instead of their main purpose.

2.4 IDS Analysis

After gathered a lot of data from the activities and events in the network, the information has to be processed to detect attacks. This is done by the IDS analysis. [BM01] describes for this purpose *misuse detection* or *signatures-based detection* and *anomaly detection*. Whereas [MNP04] introduce a third method, named *specification-based detection*. These three methods are being discussed in the following.

2.4.1 Misuse Detection

To detect attacks misuse detection uses a large database of known attacks and matches them with the occurring events. In the known attacks the system

looks for a unique pattern, the so called signature. Therefore, this technique is sometimes also named as signature-based detection. The database has to be updated, regularly.

This technique is the most widely spread method in commercial system for IDS Analysis [BM01]. However, most of them are combining it with anomaly detection, because misuse detection detects only attacks that are already in the database. Another drawback is, that most attacks are so tightly defined, that variants of known attacks will not be detected. The advantages of this technique are the very low false positive rate, the effectiveness and the reliability.

2.4.2 Anomaly Detection

Anomaly detection operates with a profile that represents the status of normal activities, i.e. activities that do not belong to an attack or to the preparation of one. Whenever an event is monitored that does not fit into the profile, the system has to decide whether it is an attack. For this purpose it works with a threshold: once the threshold is exceeded, it raises an alarm. For instance, the system has observed the behavior of users over a period and calculated a profile of normal activities concerning accessing files on the hard drive. A user, that access anomaly many files on the hard drive, is viewed as misbehaving user.

Besides that the systems has a much higher false positive rate than misuse detection, it also produce more false negative. This is because it does not detect attacks that behave "normal" and it suspects legitimate actions.

2.4.3 Specification-based Detection

A system that uses specification-based detection defines a set of constraints for a correctly behaving program or protocol. These constraints define exactly, what an application is allowed to do (*e.g.*, whether an application has the right to read from a file system). It monitors the operations of the program or protocol against the constraints. The technique has the advantage to detect unknown attacks with a lower false positive rate than the anomaly detection.

2.5 Intrusion Response

Detecting an attempt of an attack, an attack or only suspicious activities, the IDS triggers countermeasures, so called Intrusion Response. The responses can be categorized into two types: active and passive [BM01].

2.5.1 Active Response

Active response are action that are automatically triggered by the IDS once an intrusion has been detected, there is no need of human interaction. Again, these actions are categorized into three types.

Collect additional Information

In the case of a possible intrusion the IDS gathers additional information. This is done by increasing the level of sensitivity, *e.g.*, it captures not only the traffic on few defined ports, but on every port or the OS audit trail logs a bigger

number of events. The collection of additional information has many reasons. With additional information it is easier to determine whether it is an attack or just a suspicious activity. Moreover, the additional information can be used to track back to the attacker for legal actions.

Change the Environment

If there is enough information gathered to identify the source of the attack, the IDS might change the environment. If known, it can block traffic from the IP-address of the attacker or block traffic on certain ports over which the attacks are conducted.

Take Action Against the Intruder

During this action the IDS triggers actions against the intruder or the intruder's address with the object of stopping the intrusion. However, this might be tempting, this action should be considered at last and only with human support. Particularly due to legal concerns and it might hit uninvolved systems or networks.

2.5.2 Passive Response

In these actions the IDS has only a supporting role, it provides the humans with information. Based on the collected information the IDS generates reports for administrators, with the object that the administrators can make a decision what to do.

Alarms and Notifications

Alarms and notifications are well-known actions. The IDS generates based on its configuration alarms and notifications for the users (*e.g.*, a pop up window on the screen). The content of the notifications vary widely: it can be only short message that an attempt has happened or it can already provide some detailed information, like IP address of the attacker.

Reporting and Archiving Capabilities

In the case of an intrusion the IDS generates an entry in a report. These reports are periodically generated for the users.

Failsafe Considerations for IDS Responses

An IDS is only feasible, if it cannot easily be defeated. An IDS has, therefore, to provide different failsafe features. Failsafe features are meant to protect the IDS from being defeated. An attack on the IDS is much harder, when the position of it is unknown. For instance, the fact, that broadcasting alarms and alerts might reveal the position of the IDS, has to be considered by the IDS.

2.6 Control Strategy

The control strategy of an intrusion detection system defines how the elements and how the input respectively output of an IDS is managed. [BM01]

names three different possibilities of control strategies: centralized, partially distributed and fully distributed.

2.6.1 Centralized Control Strategy

In *centralized control* strategy the main functionalities are performed at one central point of the network. This means all monitoring, detection and reporting is done at the same place. This approach is only applicable in network that has traffic concentration points. Those are points, over which the major part of the traffic is routed, *e.g.*, a gateway. This is required, because of the central monitoring, which is only possible at such points.

2.6.2 Partially Distributed Strategy

In *partially distributed* IDSs the nodes gather individually information, monitor activities and also the detection and analysis is done locally. But, only a central managed node has the responsibility of reporting [BM01]. This approach generates ineluctable overhead traffic for the communication between the individual nodes and the central node.

2.6.3 Fully Distributed Strategy

In *fully distributed* IDSs all functionalities are implemented and performed at each individual node. The intrusion responses are processed at the local nodes, too [BM01]. For instance, every node blocks traffic on a certain port individually.

2.7 Summary

This chapter defines what an intrusion detection system is and gives a generic overview of state-of-the-art intrusion detection systems. It describes how an IDS is built and its main functionalities. The focus lies on how the information are gathered (information sources), how an intrusion is identified (IDS analysis) and how to deal with an intrusion (intrusion response).

Chapter 3

Overview of Mobile Ad Hoc Networks

Mobile ad-hoc networks (MANETs) are spontaneously built networks between mobile devices. The only condition the device has to fulfill is the communication interface, as it needs one to build up a connection to other devices. The networks itself is self-organized and adaptive. A MANET has no infrastructure, which means that the participants (the nodes) are directly connected with one another and not to an access point, to a gateway or something similar. The nodes must, therefore, not just send and receive, but also forward packets. In MANETs the composition of the nodes varies very rapidly: in every a moment a new node may connect or an established node may disconnect.

Based on [CCMN04] this paper assumes that MANETs use wireless connections for communication and that the devices are battery powered. There are two reasons that support this assertion. MANETs are by definition mobile and spontaneously built networks. In order to be mobile the devices have to be independent of electricity. The ad hoc manner of MANETs eliminates the application of wired connection between the nodes.

MANETs are particularly used in situation where a fast installation is needed and no infrastructure is available, for instance in disaster missions or on the battlefield. Not surprisingly, the origin of ad hoc networks is in military [Toh02].

This chapter takes a closer look of how MANETs are built, with focus on the routing protocols in MANETs. Wireless sensor networks as a special subset of MANETs are discussed later in this chapter.

3.1 Architectures of MANETs

MANETs might be organized in different fashion. Either they have a flat organization in which all nodes are considered as equal or in multi-layered organization, in which not all nodes have the same functions and responsibilities. In flat MANETs all nodes participate in the routing process, whereas in multi-layered networks the nodes are organized into cluster and elect a cluster-head to centralize the routing information within the cluster [BK03]. Former organization is more suitable for classroom or meetings, later is manly used in military applications, *e.g.*, on battlefield or disaster missions.

As mentioned, cluster heads have central function: they provide the intra- and inter-cluster routing, deliver the packets destined to a cluster and might exchange data with a node that provides a gateway to a wired network [CCMN04]. The size of the cluster is mainly determined by the transmission power of the cluster head, respectively the transmission range of it.

3.2 Routing in MANETs

As already mentioned, MANETs do not have any infrastructure and therefore there is no router in the network which every node is connected to. It is even more complicated, the nodes are not connected to every other node, so that the nodes have to forward packets and route the packets to the addressee, known as *multi hop communication*.

The fast changing environment, the constantly connecting and disconnecting of nodes makes it impossible to route the traffic using approaches like traditional link state or traditional distance vector routing. These protocols are designed for a static, only slowly changing topology [TL98].

The different routing-algorithms for MANETs can be grouped in table driven (proactive) and on-demand-driven (reactive) protocols. Well-known example of table driven algorithms is the *destination sequenced distance vector*. *Ad hoc on-demand distance vector routing* and *dynamic source routing* are two examples of on-demand approaches.

In wireless networks, especially in fast-changing ad hoc networks, the traditional metrics to measure the quality of a connection, like ping-time, are not suitable. In MANETs the links are unreliable. The nodes are moving and therefore, connections between nodes may weaken or the node may even move out of the transmission range.

3.2.1 Table-Driven Approaches

In table-driven approaches every single node maintains a routing table with the information which node is accessible through which other node. Once the topology has changed, the routing tables have to be updated. To maintain a consistent network view the changes in the routing tables are broadcasted to all nodes [Toh02].

The *Destination Sequenced Distance Vector* (DSDV) routing protocol is a table-driven approach based on the Bellman-Ford routing algorithm. Unlike traditional distance vector algorithm, DSDV guarantees a loop-free path. This is achieved with sequence numbers to distinguish new paths form already visited paths [Toh02, TL98].

As all table-driven protocols do, the DSDV broadcasts periodically table updates. In a MANET, in which the composition is changing rapidly, this results in huge control traffic. Therefore, the DSDV knows two types of update packets: *full dump* and *incremental packets*. The former transmits the whole routing information, whereas the latter transmits only information about what has changed since the last full dump.

3.2.2 On-Demand-Driven Approaches

Routing information in on-demand-driven approaches are only generated when it is needed, this in contrast to the table-driven where at every moment a full routing table is available. Once routing information is needed a routing discovery process is initiated. Only as long as the route is needed and the connection is possible the information is kept.

The *Ad Hoc On-Demand Distance Vector Routing* (AODV) is based on the DSDV (for further information on DSDV see [PB94]) and guarantees loop-freedom as well. Moreover, it minimizes the traffic in the network as it only broadcasts requests, when a route is needed and does not have the count to infinity problem. Since this protocol is used hereafter in examples, it is described in more detail.

The route discovery process depends on the collaborating with other nodes. To discover a route to a destination, a so called path discovery is initiated and the node broadcasts a route request packet (RREQ). Nodes that receive a RREQ update their routing table with the inverse route of the RREQ. All nodes, that do not have an entry in the routing table to the destination, send the RREQ to their neighbors. Once a RREQ arrives at the destination, a route replay (RREP) is sent back to the source. Nodes, which receives a RREP updates their table with an entry of the destination and the route to this node. The detailed functionality is described in [PR99].

Dynamic Source Routing (DSR) is a reactive routing protocol. It is based on the source routing, which means every packet sent trough the network has a list in its header with the nodes it has to pass. Unlike in AODV, there is absolutely no router advertisement, DSR requires the help of the MAC layer to determine the status of the links to the neighbors. DSR has two basic functions: route discovery and route maintenance.

3.2.3 Other

Besides the two already discussed approaches, it exist routing algorithms which are explicitly designed for the characteristic of MANETs. The *power-aware routing* is one of them. In power-aware routing battery life is a primary metric for routing. Its target is to minimize energy consumption for the routing process and keep the network unpartitioned as long as possible. For more information see [SWR98].

3.2.4 Multicast Routing

The challenge of multicast routing in MANETs is the fast changing topology of MANETs and the limited bandwidth of the wireless links. None of the routing protocols, used in wired networks (*e.g.* DVMRP or MOSPF), is applicable for MANETs. However, they build the basis for the multicast routing protocols in MANETs. Toh [Toh02] categorized the routing protocols for MANETs in 5 groups, based on their multicast delivery structures, i.e. the structures which defines how to form the path to all addressed nodes.

- Flooding

In this approach a node sends the packets to all neighbors. The challenge is to keep the route loop-free. The method is robust, but has a huge waste of bandwidth.

- Source-Based Multicast Tree (SBT)

  In SBT, a multicast tree is build and maintained for each multicast source in each multicast group. The paths found with SBT are on the efficient path, but the SBT has enormous overhead costs to construct and keep the trees up to date, which makes this approach not scalable for bigger MANETs.

- Core-Base Multicast (CBT)

  CBT is an analog scheme as SBT with the difference that it builds only one shared, collective tree to connect all multicast group members, i.e. one tree for all groups is built. Along this tree the packets are distributed. This makes the approach more scalable then SBT, but the route to the nodes is not always the shortest ones.

- Multicast Mesh

  Multicast mesh considers especially the fast changing environment of MANETs. Instead of building up a tree, it constructs a mesh with redundant paths. This makes the algorithm less vulnerable to failures of single nodes, but creates unnecessary traffic.

- Group-Based Multicast Forwarding

  This approach simplifies the process of maintaining the path to the nodes in the MANETs. It builds groups of nodes which act as multicast forwarding nodes for each multicast group.

3.3 Wireless Sensor Networks

Wireless sensor networks (WSN) are typically built of numerous tiny devices, connect to one another in an ad-hoc manner. WSNs are particularly deployed to gather data and information in inhospitable places, *e.g.*, enemy's movement on the battlefield [dSMR+05].

The domain of WSNs makes it necessary that the nodes are inconspicuous, small and cheap. That causes that the devices have only scare resources: low bandwidth, minor processing power, low storage and low energy capacity. This circumstance makes the WSNs even more vulnerable than "normal" MANETs, formed with notebooks, PDAs or cell phones, and requires special actions [Pot98].

3.4 Summary

This Chapter presents an overview of the current technology and standard of mobile ad hoc networks. It takes a closer look at the routing protocols of MANETS and classifies them into table-driven, on-demand-driven and in others. Wireless Sensor Networks as a specific kind of MANETs are also described as

well as the field of application. Moreover, it describes also the differences in the routing algorithm in traditional and ad hoc networks.

Chapter 4

Vulnerability of MANETs and Attacks on MANETs

The characteristic of MANETs, i.e. the mobility and the fast changing topology, results in new and novel vulnerabilities. The vulnerabilities allow aimed attacks on MANETs. Vulnerabilities have to be known to make a system secure against attacks. Prevention tries to close or hide these vulnerabilities, whereas detection pays additional attention to the vulnerabilities; aware, that these points are the origin of attacks and intrusions.

The targets an attack is aiming at, are described in section 2.1. Though, the most obvious attack in a network that uses radio as transmission medium is the one against confidentiality. In wireless networks, everybody should be aware, that eavesdropping of the network traffic is possible with a small effort. Nevertheless, attacks against availability are also common. Besides denial of service attacks, which are also known in wired networks, the topology of MANETs allows new form of attacks. Thus, there is no physically control mechanism for accessing the medium, it is easily possible to jam the communication channels. The interference of radio waves makes it impossible to communicate between two nodes, if they are in the range of a jamming transmitter. Another problem is the battery life of the nodes. To be mobile and independent to electricity, they are operating with a battery and have therefore only limited energy resources. Attackers might utilize this circumstance and revoke energy from nodes to make them unavailable.

This chapter takes a closer look at the vulnerabilities of MANETs and the attacks that can be derived from these vulnerabilities.

4.1 Vulnerabilities of MANETs

Vulnerability is defined as a point at which an attack can be performed (based on [YZ03]). The attacker utilizes explicitly the vulnerability to achieve its target.

That MANETs are vulnerable to attacks, has different reasons. In wireless networks the access to the medium is much easier than in wired networks. Additionally, most of the techniques used in wired networks relay on an infrastructure, and therefore the absence of any infrastructure is one of the most striking difference to other networks and a big vulnerability of MANETs. How-

ever, there are other vulnerabilities in MANETs. One of them is the routing protocol used in MANETs. Routing is achieved with cooperative routing algorithms. That implies that single nodes are involved in the routing process and on this way a malicious node may interfere with the routing process or may even willingly manipulate. Another vulnerability is the battery life of the nodes.

Table 4.1 shows which target can be achieved utilizing which vulnerability. The common targets of attacks are described in Section 2.1. To attack the availability all of vulnerabilities can be utilized. In the following, the vulnerabilities are explained in more details.

		Vulnerability		
		Routing Protocols	Battery Life	Medium
Target	Authenticity	X		
	Availability	X	X	X
	Integrity	X		X
	Confidentially	X		X

Table 4.1: Attacks and Vulnerabilities

4.1.1 Open Medium

The term of mobile ad hoc network is composed of *mobile* and *ad hoc*. A mobile network implicates wireless links between the nodes, whereas ad hoc means that there is no preparation necessary, which implicates no infrastructure. The open access to the network is vulnerability, whereas the lack of infrastructure is an unfavorable characteristic (see section 5.2).

Wireless connections between the nodes make it almost impossible to physically shield the transmission medium against attackers. Moreover, it is absolutely no problem to eavesdrop the network traffic. As already mentioned, it is also possible to jam the traffic in an open medium as radio is one.

4.1.2 Cooperative Routing Protocols

Routing protocols in MANETs are cooperative, i.e. the nodes rely on information received from their neighbors. Hence, many routing protocols are vulnerable to misbehaving neighbors. The problems occur during route discovery and packets forwarding. Fake routing information may easily injected by *Byzantine nodes* or modify legitimate ones so that the routing process is heavily disturbed. Byzantine nodes are misbehaving nodes. During packet forwarding exists also possibilities to derogate the network by not forwarding the packets or maliciously altering packets [BH03].

AODV is an example of a cooperative routing protocol. Misbehaving nodes may easily disturb the route discovery process while dropping packets, altering content of control packets or spoofing IP- and MAC-addresses [VGS+04]. *Control packets* are packet that are only needed to maintain the functionality of the network, *e.g.*, for routing purpose. Spoofing is pretending a foreign identity, *e.g.*, the IP-address of another participant.

4.1.3 Battery Life

To stay independent of *any* infrastructure and to allow highest mobility, the nodes of a MANET are battery powered. Devices are operable as long as they have energy left in their batteries. Thus, there is made a big effort in energy saving measures in designing mobile devices, including communication standards that are used in MANETs. This limitation of energy is thus a vulnerability of MANETs. It can be utilized for an attack against the availability while generating a lot of traffic so that the nodes cannot go into sleep modus, so that they run out of energy.

4.2 Attacks in MANETs

Attacks in MANETs are of different kind of nature, but all of them with a target discussed in section 2.1 utilizing one of the vulnerabilities showed in section 4.1. Vigna et al. [VGS+04] classify the attacks according to their targets. Attacks against confidentiality are often passive, *e.g.*, eavesdropping of packets. The attacker takes no further actions than capturing the packets and recording or analyzing them. To detect such an attack is very hard, using good prevention (*e.g.* encryption), however, this attack might be avoided. Yet, prevention in MANETs is neither achieved without any problems, because the attacks might come from an inside node. Considering IDSs the attacks against availability and integrity are much more relevant. The single major attack against authenticity is spoofing of IP-, MAC- or TCP-addresses.

4.2.1 Misrouting Attacks

Misrouting attacks are attacks with the target to sap the integrity. In misrouting attacks the packets do not reach their destination. Due to the characteristic of MANETs misrouting attacks are easier to perform than in traditional networks. Since all nodes are involved in the routing process, it is not necessary to attack a central, probably better protected, router, gateway or switch. Either an attacker might attack an inside node and change its behavior or it authenticate himself as a participating node.

It is possible to attack the route discovery process or to disturb the packet forwarding process. In the route discovery process, there are multiple possibilities to disturb the process: changing misleadingly the sequence number, dropping all RREQ packets or sending false route errors (RERR) packets. Also in the forwarding process are different attacks possible: dropping the packets, changing addressee or deliberately forwarding to the wrong node. *Blackhole* is a special kind of a misrouting attack, where all packets are routed to one single node. Not forwarding these packets by this node, but dropping them, makes this action to a severe attack against the network.

4.2.2 Denial-of-Service

There are plenty of ways to perform denial-of-service attacks, some of them do not utilize an explicit vulnerability of MANETs, but others, *e.g.*, vulnerability of applications or operating system. A malicious behaving node may drop any data packets. If this node is critical, the network gets partitioned. The limitation of

the wireless links is utilized in *resource depletion attacks*. The attackers (the red ones; see figure 4.1) transfer big, unnecessary volumes of data between them to deplete the resource of the network, i.e. the bandwidth of the links. Transferring big volumes of data, clogs the available bandwidth of the network. During this transfer A and B might send and receive only with a limited efficiency. Sleep deprivation is also a DoS attack: once a node has no energy left, it will not be able to handle any further requests.

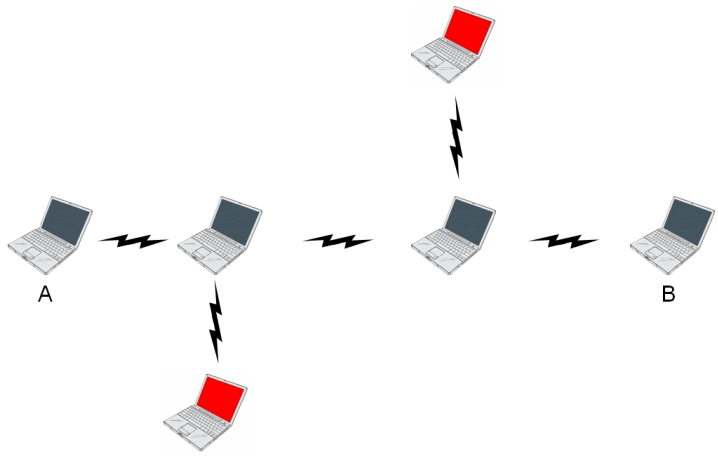

Figure 4.1: A resource depletion attack

4.2.3 Wormhole

In wormhole attacks, the traffic is tunneled between two nodes to unnoticeably send packets. As long as all packets are tunneled, wormholes are not malign. Once the attacker forwards only control packets a severe attack on the network is performed [BH03]. For instance, the routing process in a network using AODV protocols might be highly disrupted.

Figure 4.2 shows a situation of a wormhole attack. Assuming the network uses the AODV routing protocol and the sender node on the left wants to send a packet to the receiver. Since AODV is an on-demand routing protocol, the sender starts a route discovery process, before it transmits the data packets. A RREQ packet is broadcasted to the two nodes within transmission range. The red one is the attacker, the other a normal participant in the network. The attacker sends the RREQ through the tunnel, which is in this case a wired connection, to the other malicious behaving node. That sends the RREQ packet to the receiver, which is answering with a RREP. The benign nodes find a route as well, but this route is longer, i.e. has more hops in between. The sender chooses the shortest route to send the packets, which is the one over tunnel from the attackers. Yet, the attackers do not forward the data packets and the packets never reach their destination. Not receiving a confirmation the sender assumes the connection is not available any more and starts a new route discovery. The resulting route, however, will be the same as before.

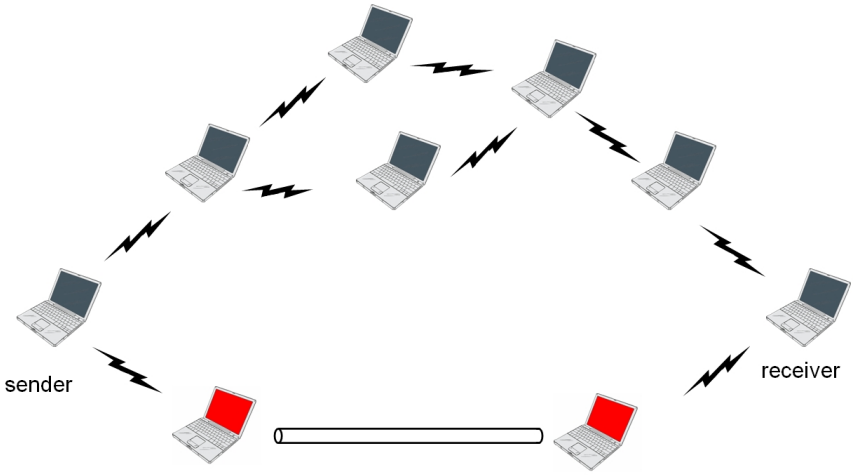

Figure 4.2: Wormhole attack

4.2.4 Jamming

Jamming is another attack to reduce the availability of a service or the whole network. Collisions of network packets are willfully generated while sending insignificant packets at the same time and on the same frequency as other legitimate massages are transmitted. Using frequency-hopping or code division multiple access spread spectrum techniques help only, as long as the attackers does not know the hopping/chipping frequency or does not jam the whole frequency band.

Check sums can be used to detect the incorrectness of the packets, but it results in a higher need for energy due to retransmission. Error correction codes operate only if enough packets reach the destination [BGD05].

4.2.5 Data Alteration

Maliciously changing the content of packets is called data alteration. Data alteration is an attack against the authenticity. Spoofing is also a kind of data alteration, whereas control packets with modified source addresses are injected.

4.3 Summary

Vulnerabilities are the attacking points of an attack against a computer system or network. For security reasons the vulnerability should be known in order to prevent or to easier detect attacks. In this chapter the vulnerability of MANETs are discussed and the attacks that can be derived from them. Several attacks are described, yet this list does not claim to be complete. In the following chapter, techniques to detect these attacks are presented.

Chapter 5

Intrusion Detection in Mobile Ad Hoc Networks

In chapter 4 the vulnerability and the attacks against MANETs are discussed. This chapter tries to give an overview of solutions or approaches to antagonize to those problems.

5.1 Requirements

The requirements for IDS in MANETs are characterized by the properties of mobility and wireless links. Mishra et al. [MNP04] names efficiency and effectiveness as the *key requirements* and lists few others.

- **Efficiency:** Wireless links have very limited bandwidth and therefore the IDS must not generate or require a lot of traffic. The system has also to consider the power consumption of the devices.
- **Effectiveness:** The target of the IDS is to classify malign and benign activities correctly in effective manner. Especially in fast changing environments effectiveness plays a decisive role.
- **No introduction of additional vulnerabilities:** An IDS, that protects a network against a certain attack, should not introduce new or additional vulnerabilities to the network.

5.2 Unfavorable Characteristics

An unfavorable characteristic is defined as a property of the system which makes it more difficult to detect an intrusion, weaken the system against attacks or is the reason of a vulnerability. Unfavorable characteristics cannot be attacked, but vulnerabilities.

5.2.1 Fast Changing Topology

The fast changing topology makes it difficult to identify attacks and intrusions. Especially, anomaly detection as IDS analysis is more challenging. A node that

forwards packets only occasionally might be a malicious node, but it is also possible that the node is just at the border of transmission range and is not capable of forwarding all packets. Another example is a node responding with false routing information. It is not obvious whether it is a malicious node or a node out of synchronization due to movement.

5.2.2 No Infrastructure

The absence of infrastructure implies that there is no central authority and it is therefore not easy to distinguish nodes as trusted or none trusted. A single misbehaving node (*Byzantine node*) can have an enormous impact on the quality, security of the network. Moreover, it is hardly possible to establish a clear line of defense in a network that has no infrastructure. In traditional networks exists often a gateway to not trusted network (i.e. internet). In MANETs, however, it is not that clear where to draw this line of defense [MNP04].

5.2.3 Selfishness

In order to save their own energy reserves, nodes may behave very selfishly, while not forwarding any packets of other nodes. Hereby, the network might be partitioned.

5.3 Problems

Originally, IDSs are designed for wired networks, the characteristic of MANETs though generating problems for intrusion detection. These problems of IDS in MANETs are partially related with the unfavorable characteristics described in section 5.2.

5.3.1 No Traffic Concentration Points

In traditional MANETs, there are no traffic concentration points. This makes it almost impossible to use network-based IDSs, which - as already said - captures the traffic at crucial points of the network, i.e. at router, switches or gateways [YZ03]. While it is almost impossible to use network-based IDSs, the possibility of implementing an IDS is highly constricted.

5.3.2 Low Resources

Due to mobility and energy saving considerations mobile devices have only low resources: low CPU power and very limited memory. The smaller the frequency (and voltage) of a CPU is, the less energy it consumes. The dimensions of the mobile devices are the reason for the small amount of memory. Depending on the IDS analysis, the process of identifying an attack might use a lot of resource. If only limited resources exist, this impedes an effective detection.

5.3.3 Definition of Anomaly

In a fast changing environment, like in a MANET, it is harder to define a profile of normal activities. That complicates the implementation of anomaly detection

in MANETs.

5.4 Architectures for Intrusion Detection Systems in MANETs

Optimal architectures for IDSs might depend on the architectures of the MANET itself (see section 3.1). Brutch and Ko [BK03] name three different architectures: stand-alone, distributed and cooperative and hierarchical. These architectures are in the following explained.

5.4.1 Stand-alone IDS

In stand-alone IDS, every nodes runs locally and independently an IDS. No information or analysis results are shared with other nodes in the network. The effectiveness of this solution is very limited, but it may be deployed where not all nodes are capable of running an IDS or have an IDS installed [BK03].

5.4.2 Distributed and Cooperative IDS

Distributed IDS are most suitable in flat organized MANETs. Intrusion detection is performed locally at every host, but the host may participate in global intrusion detection. Especially, in the case of inconclusive evidence, the nodes may request the help of neighbors and other nodes within the network. A problem of distributed and cooperative IDS is false claiming of Byzantine nodes. Thereby they claim a correct behaving node to be acting malicious. If a correct node is wrongly banned from the network, the network might not work correctly.

5.4.3 Hierarchical IDS

Hierarchical IDSs are deployed in multi-layered MANETs. The cluster head has a leading role, because all nodes report their suspicions to the cluster head. The cluster has then the possibility to ban the misbehaving node. Due to the power of the cluster heads, it is essential to detect Byzantine cluster head nodes [BK03]. On the one hand, cluster head are responsible for the connection between the clusters; they provide the links to other cluster heads and on the other hand they route the packets within a cluster. A Byzantine cluster head may disturb the routing process in a cluster completely and partially in the whole network.

5.5 Common Approaches

This section describes a common approach for IDS in MANETs. Although the focus of the method described below is on routing protocols, its approach might be extended on other layers.

5.5.1 Anomaly Detection for Mobile Wireless Networks

As already mentioned in section 5.2, anomaly detection, including the challenge of the questions "what is anomaly?" and "what are normal activities?", can

not easily implemented. However, Zhang et al. present in [YZ03] a model for anomaly detection. Thereby, nodes locally collect data and monitor independently the activities in the neighborhood. Like in the intrusion detection and response model, which is discussed later, the search might be extended in a collaborative investigation over broader range, i.e. using the help of nodes in the neighborhood.

The authors assume that the entropy of information flows may be used to determine anomaly. That means, that given n previous events, the following event is predictable. If the predicted event does not happen, the system assumes an anomaly. The profile which is defining the normal behavior is constructed from local audit data. Yet, this profile needs regularly updates, because the routing characteristic may change.

5.6 Protection of Availability

As shown in section 4.2 the availability might be attacked in different ways, a good and effective intrusion detection system is therefore indispensable. In the following there is a model showed to assure availability.

5.6.1 Watchdog-Pathrater

Watchdog-Pathrater, a technique introduced by Marti et al. [MGLB00], consists of two main functionalities: watchdog, identifying misbehaving nodes, and pathrater, helping the routing protocols to avoid routes with these nodes. Hereafter, these techniques are explained in more details. Watchdog-Pathrater is a stand-alone IDS.

Watchdog

The idea behind watchdog is really simple: every nodes check whether the sent packets are correctly forwarded (if necessary). This is achieved by maintaining a buffer of all sent packets. Once the neighbor node forwards the packets, the sender notices that, due to wireless transmission, and removes the packet from the buffer. If the packet stays for a certain time in the buffer, the node observes the other node and in case of recurrence it assumes the forwarding node is misbehaving. This techniques has multiple vulnerabilities, the most severe is that nodes may malicious false reporting of misbehaving nodes to partitioning the network. On the other hand, this method allows detecting replay attacks. In replay attacks packets are repeatedly sent or forwarded.

Pathrater

Pathrater combines the information received from watchdog and the link reliability to choose the route that is the most likely to be reliable. Hence, every node maintains a list of all know nodes with a rating. The metric for the path is calculated by averaging the rating of the nodes. In contrast to traditional routing protocols, pathrater chooses not the shortest path, but the most reliable [MGLB00].

5.7 Protection of Integrity

In the following *a distributed IDS* and *intrusion detection and response model* are introduced. Latter is an enhancement of the former. Both are IDS approaches to protect the integrity of the MANET.

5.7.1 A Distributed IDS

The System proposed from Zhang and Lee [ZL00] bases on autonomous nodes, which perform local data collection, local intrusion detection and local intrusion responses. Only in defined cases the search is spread to other nodes. The IDS is divided into six modules (see figure 5.1)

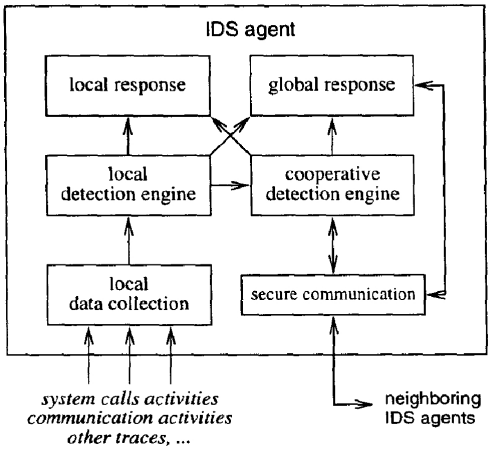

Figure 5.1: A distributed IDS [ZL00]

The module *local data collection* is responsible for gathering and saving the data (*e.g.* system calls activities). The *local detection engine* module analyzes the data on anomaly. If the evidence is not conclusive, the search and the detection are spread out to the *cooperative detection engine.* Based on the decisions made by the detection engines either a *local response* or a global responseis performed. The module *secure communication* provides a high confidence channel between the nodes.

This IDS approach is one of the first for MANETs, however it has a big weakness. The approach is not or too less concerned about attacks coming from an inside node. Two examples support this claim. First, the communication module is worthless when the attack is coming form an inside node. The encryption is not safe, when the attackers have also access to the keys. Second, the proposed intrusion response - re-initializing communication channels (force re-key) - might not have the desired effect when the attacker is a node within the network.

5.7.2 Intrusion Detection and Response Model

The intrusion detection and response model (IDRM) bases and extends the above described distributed IDS [MNP04]. Each node observes its neighborhood and utilizes the information to detect misbehaving neighbors. Again, a threshold is used for the misbehavior of the neighbor nodes. Once the threshold is exceeded, the node informs all other nodes. A node which receives such information and its threshold is exceeded as well for the suspicious node, broadcast a MAL message, advertising the failure of the node. If another node shares the concerns about the same node, this node sends a REMAL-packet to the whole network. If two other nodes confirm the suspect with a packet called PURGE, the suspicious node is being excluded from the network, i.e. routes over the malicious node are avoided and its packets are dropped.

5.8 Protection of Confidentiality

A detection method for passive eavesdropping is hardly to be implemented. Due to the open accessible medium, it has no impact when an intruder is listening to the network traffic. The protection of confidential information and private data has to be achieved by prevention, *e.g.*, using encryption. However, encryption is inefficient when the attack is performed by a node form within the network.

5.9 Summary

Intrusion detection is never trivial, in MANETs come aggravating circumstances along. These circumstances result of the facts, that MANETs do not have any infrastructure, the topology is rapidly changing, the wireless links have only a limited bandwidth and the mobile nodes have only scare resources. Nevertheless, there are promising approaches for intrusion detection systems. Some of them are cooperative, although the contributor might be a malicious node. However, some attacks or vulnerabilities are very hard to cope with intrusion detection, *e.g.*, passive eavesdropping. These problems have to be solved by intrusion prevention.

Chapter 6

Conclusion

This paper gives an insight in attacks in mobile ad hoc networks and the intrusion detection techniques to identify them. First, the basic principles of intrusion detection systems and mobile ad hoc networks are discussed. In the chapter on intrusion detection system the common targets of attack against computer systems are shown. Besides the attacks against confidentiality, i.e. getting access of private, secret or restricted information, availability, authenticity and integrity are targets an intruder might attack. The main functions, which are gathering information, analyzing it and triggering an appropriate measure, are explained in more detail. In the chapter on mobile ad hoc networks the main focus was on the routing algorithms. These differ from traditional networks because all participant nodes have to take part in the routing process. The different architectures and wireless sensor networks are also touched in that chapter. In the chapter about vulnerabilities and attacks in MANETs the specific vulnerabilities of MANETs are shown and the attacks that can be derived form them. The main vulnerabilities are the open medium, the cooperative nature of the routing protocols and the fact, that the devices are battery powered. These vulnerabilities allow denial of service, misrouting and jamming attacks. The chapter intrusion detection in mobile ad hoc networks describes first the problems of intrusion detection in a fast changing, spontaneously built environment and provides an overview of solutions and approaches for intrusion detection.

This paper deals only with intrusion detection and not with general concerns of security in MANETs. Intrusion prevention is, therefore, no topic of this document.

Bibliography

[AW05] Daniel Newman Andrew Whitaker. *Penetration Testing and Cisco Network Defense*. Networking Technolog. Cisco Press, 1st edition, Oct 2005.

[BGD05] M. Brownfield, Yatharth Gupta, and N. Davis. Wireless sensor network denial of sleep attack. In *Systems, Man and Cybernetics (SMC) Information Assurance Workshop, 2005. Proceedings from the Sixth Annual IEEE*, pages 356–364, 15-17 June 2005.

[BH03] Levente Buttyán and Jean-Pierre Hubaux. Report on a working session on security in wireless ad hoc networks. *SIGMOBILE Mob. Comput. Commun. Rev.*, 7(1):74–94, 2003.

[BK03] P. Brutch and C. Ko. Challenges in intrusion detection for wireless ad-hoc networks. In *Applications and the Internet Workshops, 2003. Proceedings. 2003 Symposium on*, pages 368–373, 27-31 Jan. 2003.

[BM01] Rebecca Bace and Peter Mell. *Intrusion detection systems*. U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology, 2001.

[CCMN04] Carla-Fabiana Chiasserini, Imrich Chlamtac, Paolo Monti, and Antonio Nucci. An energy-efficient method for nodes assignment in cluster-based ad hoc networks. *Wirel. Netw.*, 10(3):223–231, 2004.

[dSMR+05] Ana Paula R. da Silva, Marcelo H. T. Martins, Bruno P. S. Rocha, Antonio A. F. Loureiro, Linnyer B. Ruiz, and Hao Chi Wong. Decentralized intrusion detection in wireless sensor networks. In *Q2SWinet '05: Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks*, pages 16–23, New York, NY, USA, 2005. ACM Press.

[MGLB00] Sergio Marti, T. J. Giuli, Kevin Lai, and Mary Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking*, pages 255–265, New York, NY, USA, 2000. ACM Press.

[MNP04] A. Mishra, K. Nadkarni, and A. Patcha. Intrusion detection in wireless ad hoc networks. *Wireless Communications, IEEE [see also IEEE Personal Communications]*, 11(1):48–60, Feb 2004.

[PB94] Charles E. Perkins and Pravin Bhagwat. Highly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computers. In *SIGCOMM '94: Proceedings of the conference on Communications architectures, protocols and applications*, pages 234–244, New York, NY, USA, 1994. ACM Press.

[Pot98] G.J. Pottie. Wireless sensor networks. In *Information Theory Workshop, 1998*, pages 139–140, 22-26 June 1998.

[PR99] C.E. Perkins and E.M. Royer. Ad-hoc on-demand distance vector routing. In *Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA '99. Second IEEE Workshop on*, pages 90–100, 25-26 Feb. 1999.

[SA99] Frank Stajano and Ross Anderson. The resurrecting duckling: Security issues for ad-hoc wireless networks. pages 172–194. AT&T Software Symposium, 1999.

[SWR98] Suresh Singh, Mike Woo, and C. S. Raghavendra. Power-aware routing in mobile ad hoc networks. In *MobiCom '98: Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking*, pages 181–190, New York, NY, USA, 1998. ACM Press.

[TL98] Nicklas Hedman Tony Larsson. Routing protocols in wireless ad-hoc networks - a simulation study. Master's thesis, Luleå University of Technology, Stockholm, http://www.ietf.org/proceedings/99mar/slides/manet-thesis-99mar.pdf, 1998.

[Toh02] C.-K. Toh. *Ad hoc mobile wireless networks : protocols and systems.* Upper Saddle River, New Jersey, 2002.

[VGS+04] G. Vigna, S. Gwalani, K. Srinivasan, E.M. Belding-Royer, and R.A. Kemmerer. An intrusion detection tool for aodv-based ad hoc wireless networks. In *Computer Security Applications Conference, 2004. 20th Annual*, pages 16–27, 6-10 Dec. 2004.

[YZ03] Yi-An Huang Yongguang Zhang, Wenke Lee. Intrusion deetection techniques for mobile wireless networks. In *Wireless Networks*, volume 9, pages 545–556. Kluwer Academic Publishers, 2003.

[ZL00] Yongguang Zhang and Wenke Lee. Intrusion detection in wireless ad-hoc networks. In *MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking*, pages 275–283, New York, NY, USA, 2000. ACM Press.

List of Figures

List of Tables