1 Introduction

1.1 DEFINITION OF WIRELESS AD HOC NETWORKS

In the last few years we have seen the proliferation of wireless communications technologies. Wireless technologies are being widely used today across the globe to support the communications needs of very large numbers of end users. There are over 1 billion wireless subscribers of cellular services today utilizing wireless devices for voice communications (e.g. phone calls) and data services. Data services include activities such as sending e-mail and instant messages, and accessing the Web. In fact, in some areas of the world wireless technologies are more prevalent than traditional wireline communications technologies.

There are several reasons for the current popularity of wireless technologies. The cost of wireless equipment has dropped significantly, allowing service providers to significantly reduce the price of wireless services and making them much more affordable to end users. The cost of installing wireless networks in emerging markets has dropped well below the cost of installing wireline networks. The wireless technologies themselves have improved tremendously, making it possible to offer both voice and data services over such networks. The resulting allure of anytime, anywhere services makes such services very attractive for the end users.

In wireless networks, nodes transmit information through electromagnetic propagation over the air. The signal transmitted by a node can only be received by nodes that are located within a specific distance from the transmitting node. This distance is typically called the transmission range. The transmission range depends not only on the power level used for the transmission, but also on the terrain, obstacles, and the specific scheme used for transmitting the information. Typically, for simplicity, the transmission range of nodes is assumed to be a circle around the transmitting node, as shown in Figure 1.1.

Typically multiple nodes exist within an area and these nodes might need to make use of the wireless medium for communication. If many such transmissions happen at the same time within the transmission range of a node, then this will result in the transmissions colliding with each other. Such collisions make it impossible for receivers to interpret the data being transmitted by individual nodes. The effect here is similar to many people talking simultaneously to a person, in which case the person involved will not be able to understand any of them. Therefore, it is vital to prevent or minimize such collisions. This can be done by controlling access to the wireless medium. This is the approach typically followed by the collision avoidance or minimization schemes.

Many collision avoidance or minimization schemes have been developed for sharing the available wireless spectrum among wireless nodes transmitting concurrently.

Security for Wireless Ad Hoc Networks, by Farooq Anjum and Petros Mouchtaris
Copyright © 2007 John Wiley & Sons, Inc.

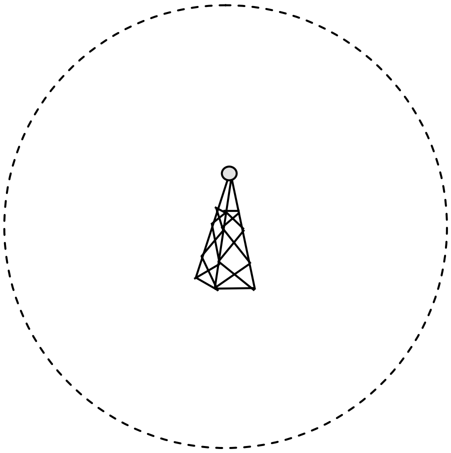

Figure 1.1. Transmission range.

Typical schemes include: (1) time division multiple access (TDMA), which divides time into small time slots and requires nodes to take turns transmitting data during separate time slots; (2) frequency division multiple access (FDMA), which provides for different frequencies such that each node transmits on a different frequency; (3) carrier sense multiple access (CSMA), which requires for every node to listen for transmissions on the wireless channel (on a given frequency) and transmit its own data when the node perceives the channel to be free of any other wireless transmissions; and (4) code division multiple access (CDMA), which allows nodes to transmit at the same time but requires them to use different spreading codes so that the signals from different nodes can be distinguished by the receivers.

Nodes might need to communicate with other nodes that are outside their transmission range. This is typically accomplished by having other nodes that are within the transmission range of the transmitting node receive and then retransmit the signal. As a result of this retransmission, nodes within transmission range of the node repeating the original signal receive the data. Depending on the location of the destination, multiple nodes may need to retransmit/repeat the data, as shown in Figure 1.2.

Various network architectures have been introduced based on the high-level concepts discussed so far. Such architectures allow wireless services and provide for end-to-end communication among users often located far away from each other. Figure 1.3 shows

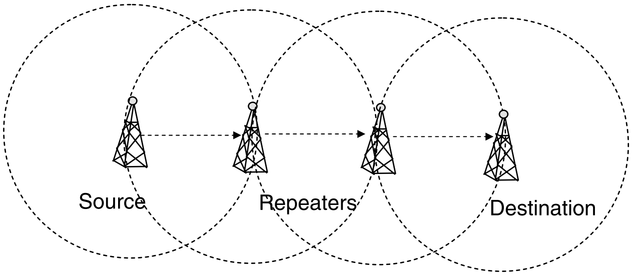

Figure 1.2. End-to-end transmissions.

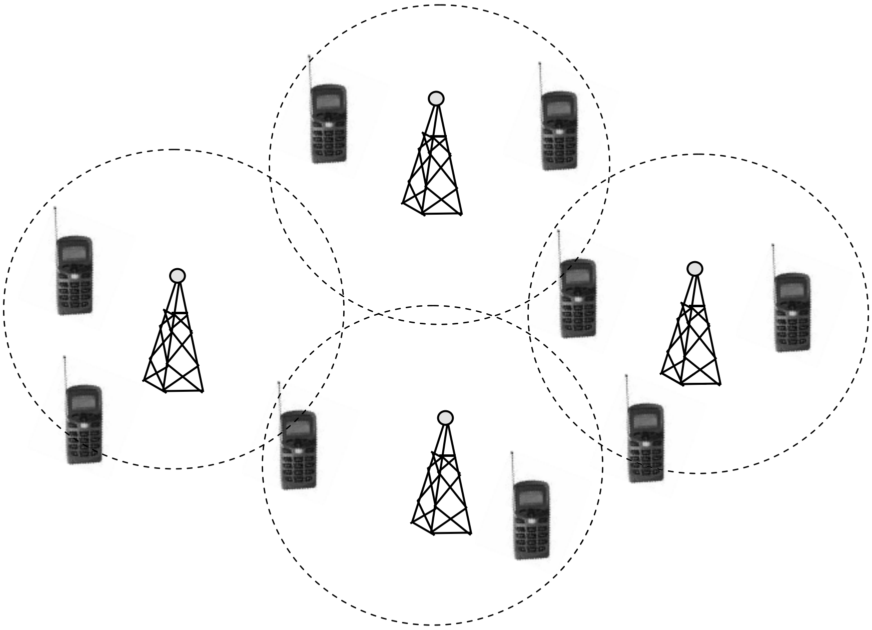

Figure 1.3. Architecture of cellular networks.

a typical architecture that is used for cellular networks. In a typical cellular architecture, radio transmission towers are placed across the area that the service provider desires to offer cellular service in. These towers are often built on top of buildings, on big towers, on high ground, and so on, and are hence stationary. These radio transmission towers are responsible for receiving the data transmitted by other nodes and then retransmitting the data as needed in order to reach the destination. The devices used by end users for accessing the service are typically small and mobile (e.g. mobile phones). End devices typically only communicate directly with the radio transmission tower that is closest to them. The radio transmission tower is then responsible for transmitting that information towards the node that needs to receive that information. The radio transmission tower might also enlist the help of other radio transmission towers in order to do this.

In a cellular network, towers are typically interconnected through a static wireline network (e.g. SONET network) with each other. An end device transmits information to the local tower. If the destination end device is unreachable from the local tower, then the local tower locates the tower closest to the destination. Following this, the local tower transmits the information to the tower closest to the destination end device through the wireline network. The tower closest to the destination is then responsible for transmitting the information to the destination end device.

Cellular technology is not the only wireless technology in existence. Another widely used wireless technology is IEEE 802.11-based wireless local area network (WLAN), also popularly referred to as Wi-Fi. Wi-Fi has mostly been used for providing wireless data connectivity inside buildings for personal computers and laptops. This technology allows such devices to communicate potentially at very high speeds (but over relatively smaller distances) as compared with cellular networks. In fact, these networks are called WLAN networks since they typically provide the equivalent of LAN connectivity

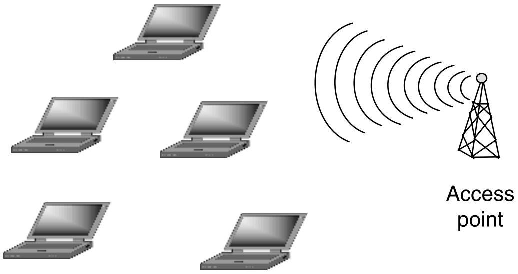

Figure 1.4. Typical enterprise architecture using 802.11 technology.

inside buildings. Figure 1.4 shows the typical network architecture used today for 802.11. This architecture utilizes fixed access points (APs) that play a similar role to that played by radio towers in the cellular environment. APs are responsible for receiving the signal from end devices and then retransmitting them to the destination. The APs also have the responsibility for interconnecting the wireless LAN to external networks such as the internet or other WLANs (through other access points to which they could be connected over wireline links).

The wireless networks that we have discussed so far are dependent on fixed nodes (the radio towers and access points) for connecting the mobile nodes. In addition, these networks require some fixed infrastructure to interconnect the fixed nodes with each other. This type of architecture has been very successful and widely deployed throughout the world for offering a variety of voice and data services, despite being inflexible (by requiring fixed nodes). This is because the architecture has been sufficient for services typically offered by service providers.

Having a communications network that relies on a fixed infrastructure, however, is not always acceptable for some applications (see Section 1.2). For example, when emergency responders move into an area (say to deal with a disaster), it is possible that the fixed infrastructure may have been destroyed or may be unavailable (e.g. in some remote areas). Emergency responders might not have enough time to establish a fixed infrastructure in such cases. A similar situation might also arise in a battlefield environment.

In the past few years, a new wireless architecture has been introduced that does not rely on any fixed infrastructure. In this architecture, all nodes may be mobile and no nodes play any special role. One example of this architecture is the “ad hoc” mode architecture of 802.11, as shown in Figure 1.5. In this architecture, 802.11 nodes do not rely on access points to communicate with each other. In fact, nodes reach other nodes they need to

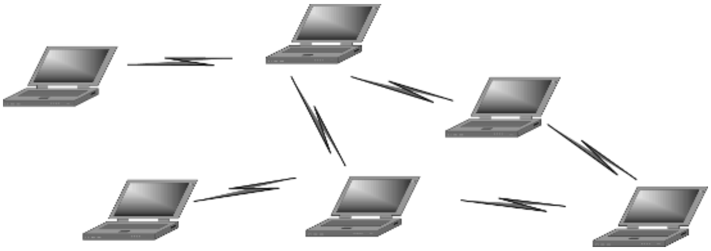

Figure 1.5. Ad hoc mode architecture using 802.11 technology.

communicate with using their neighbors. Nodes that are close to each other discover their neighbors. When a node needs to communicate with another node, it sends the traffic to its neighbors and these neighbors pass it along towards their neighbors and so on. This repeats until the destination of the traffic is reached. Such an architecture requires that every node in the network play the role of a router by being able to determine the paths that packets need to take in order to reach their destinations.

Networks that support the ad hoc architecture are typically called wireless ad hoc networks or mobile ad hoc networks (MANET). We will use these two terms interchangeably throughout the book. Such networks are typically assumed to be self-forming and self-healing. This is because the typical applications of such networks require nodes to form networks quickly without any human intervention. Given the wireless links and mobility of nodes, it is possible that nodes may lose connectivity to some other nodes. This can happen if the nodes move out of each other's transmission range. As a result, it is possible for portions of the network to split from other portions of the network. In some applications it is also possible that some nodes may get completely disconnected from the other nodes, run out of battery, or be destroyed. For these reasons, nodes in a MANET cannot be configured to play any special role either in the way nodes communicate or in the way of providing communication services (e.g. naming services). This leads to a symmetric architecture where each node shares all the responsibilities. The network needs to be able to reconfigure itself quickly to deal with the disappearance (or reappearance) of any node and continue operating efficiently without any human intervention.

Routing in such networks is particularly challenging because typical routing protocols do not operate efficiently in the presence of frequent movements, intermittent connectivity, network splits and joins. In typical routing protocols such events generate a large amount of overhead and require a significant amount of time to reach stability after some of those events. The Internet Engineering Task Force (IETF), which is the main standardization body for the internet, has recognized that existing routing protocols cannot meet the unique requirements of MANET and has played a key role in the creation of novel MANET routing protocols. This is done through the IETF MANET Working Group, which has been a focal point for a lot of the related research. This group was established in 1997 and since then has created some of the most widely cited MANET routing protocols such as the ad hoc on demand distance vector (AODV) and optimized link state routing (OLSR) routing protocols (see www.ietf.org/html.charters/manet-charter.html). Its efforts are continuing with a focus on additional routing protocols and multicast.

1.2 APPLICATIONS OF WIRELESS AD HOC NETWORKS

So far we have discussed the unique concept of MANET. We next discuss the applications that have motivated much of the research on MANETs and are well suited for their use. Perhaps the most widely considered application of a MANET is battlefield communications. The Department of Defense (DoD) future transformation is based on a key initiative called Network Centric Warfare (NCW). It is expected that there will typically be a large number of nodes in the battlefield environment that need to be interconnected, including radios carried by soldiers, and radios mounted on vehicles, missiles, unattended air vehicles (UAV), and sensors. In such an environment the network plays a critical role in the success of the military mission. The vast majority of these nodes move around at varying speeds and nodes may lose connectivity to other nodes as they move around in the battlefield because of the terrain (e.g. obstacles may prevent line of sight), distance among the nodes, and so on. Because of the rapid pace and the large degree of unpredictability it is not possible to assume a fixed infrastructure in the battlefield environment. Network administrators have little time to react and reconfigure the networks. Existing networking technologies cannot support such an environment efficiently. MANETs are viewed as a potential solution for providing a much more flexible network in support of NCW. The DoD has been funding a large number of research efforts exploring the use of MANETs for battlefield communication. As a result, a large number of research papers are motivated by such applications.

The other widely considered application for MANETs is interconnection of sensors in an industrial, commercial, or military setting. Sensors are typically small devices measuring environmental inputs (such as temperature, motion, light, etc.) and often alerting users and/or taking specific reactions (e.g. starting an air-conditioner) when those inputs reach specific ranges. Sensors have been used extensively in industrial applications and even for applications inside the home (such as in security systems, heating systems, etc.). Most recently, advanced sensors are being considered for the detection of harmful agents (such as anthrax) or nuclear material. The availability of very inexpensive network interfaces has made it possible to provide network connectivity to sensors. Certain uses of sensors seem to be well suited for MANETs. For example, the military has considered scenarios where large numbers of sensors are dropped in an area of interest and those sensors then establish connectivity to each other and to the soldiers for providing advanced reconnaissance. In some cases, applications are considered where a very large number of sensors (hundreds or even thousands) is dropped in areas that need to be monitored closely. Sensors in such areas then establish a network. For example, "Smart Dust" which is a project at the University of California, Berkeley, (see http://robotics.eecs.berkeley.edu/~pister/SmartDust/) has focused on the development of small devices that have both sensor and communication capabilities and are smaller than 1 cubic millimeter. Typically in such applications it is not possible to have a fixed infrastructure and therefore these applications seem to be well suited for MANETS.

Another relevant application is that of emergency response. During major emergencies and disasters such as hurricanes or large explosions, the communications infrastructure in the immediate area of the disaster or emergency may be unusable, unavailable, or completely destroyed. When emergency responders first arrive in the disaster-struck area, it is critical for them to be able to communicate with each other. The communications make it possible for the team to coordinate the relief operations with each other. Since the communication infrastructure is often unavailable, first responders need to be able to establish connectivity immediately. MANETs are well suited for such an application because of their ability to create connectivity rapidly with limited human effort.

Several other applications of MANETs are also being considered. For example, municipalities are considering deployment of wireless ad hoc networks (in the form of so called mesh networks) for offering broadband access to end users including employees of the municipality, first responders, and even residents of the municipality. Such networks have already been deployed in a small (but increasing) number of municipalities. More recently researchers have considered the use of MANET in the vehicular environment. Making MANET networking capabilities available in such environments can enable a variety of new applications such as sharing of up-to-date traffic information between vehicles.

1.3 THREATS, ATTACKS, AND VULNERABILITIES

Having discussed the basic concept of wireless ad hoc networks, we next look at the threat, attacks, and vulnerabilities in such networks. Any system that has to be protected might have weaknesses or vulnerabilities, some or all of which may be targeted by an attacker. Hence, one approach to designing security mechanisms for systems is to look at the threats that the system faces and the attacks possible given the vulnerabilities. The designed security mechanisms should then ensure that the system is secure in the light of these threats, attacks, and vulnerabilities. While we look at the security mechanisms designed to achieve various objectives in ad hoc networks in several chapters throughout the book, we look at the threats, attacks, and vulnerabilities in this section. We start by providing definitions of the terms, threat, vulnerability, and attack.

- *Threat* is the means through which the ability or intent of an agent to adversely affect an automated system, facility or operation can be manifested. All methods or things used to exploit a weakness in a system, operation, or facility constitute threat agents. Examples of threats include hackers, disgruntled employees, industrial espionage, national intelligence services, and criminal organizations.
- *Vulnerability* is any hardware, firmware, or software flaw that leaves an information system open for potential exploitation. The exploitation can be of various types, such as gaining unauthorized access to information or disrupting critical processing.
- An *attack* is an attempt to bypass the security controls on a computer. The attack may alter, release, or deny data. The success of an attack depends on the vulnerability of the system and the effectiveness of existing countermeasures. Examples of attacks include actions such as stealing data from storage media and devices, obtaining illegitimate privileges, inserting data falsely, modifying information, analyzing network traffic, obtaining illegitimate access to systems through social engineering, or disrupting network operation using malicious software. Attacks can be divided into two main categories:

  Passive attacks—in these types of attack an attacker passively listens to the packet or frame exchanges in the wireless medium by sniffing the airwaves. Since an attacker only listens to the packets that are passing by without modifying or tampering with the packets, these attacks mainly target the confidentiality attribute of the system. However, this process of gathering information might lead to active attacks later on. Typically this attack is easier to launch than the next type of attacks.

  Active attacks—active attacks are those attacks where the attacker takes malicious action in addition to passively listening to on-going traffic. For example an attacker might choose to modify packets, inject packets, or even disrupt network services.

Security in wireless networks differs markedly from security for their wireline counterparts due to the very nature of the physical medium. While communicating over a wireless medium, the transmitted and received signals travel over the air. Hence, any node that resides in the transmission range of the sender and knows the operating frequency and other physical layer attributes (modulation, coding, etc.) can potentially decode the signal without the sender or the intended receiver knowing about such an interception. In contrast, in wireline networks, such an interception is possible only when one obtains access to the physical transmission medium (cable, fiber, etc.), which would typically involve tapping into such mediums.

Another problem with defending wireless ad hoc networks is that existing security technologies are more geared towards wireline networks, which are fairly static. Existing technologies often rely on the availability of traffic chokepoints (which most traffic goes through). Security devices placed at such chokepoints can inspect traffic for suspicious behavior and implement security policies and respond as needed. This is not true in ad hoc networks where the network entities often move around. This results in frequent changes in the structure of the network. Traditional security solutions also depend on a few centrally located devices for managing the security of the network. Such solutions are not applicable for wireless ad hoc networks on account of the features of these networks. The increased vulnerabilities of ad hoc networks and the limitations of existing security solutions designed for wireline networks will become clearer throughout the book.

Ad hoc networks that make extensive use of wireless links are vulnerable to several types of attack due to the inherent nature of the network. We would like to remark here that mechanisms such as encryption and authentication can greatly mask the vulnerabilities on the air-link, but these are not the only vulnerabilities in ad hoc networks. Since wireless ad hoc networks cannot depend upon infrastructure-based resources, such as stable power source, high bandwidth, continuous connectivity, or fixed routing, it is very easy to launch attacks on them. In the following subsections, we will briefly describe some vulnerabilities and attacks that are very common in the ad hoc network environment. Note that while the lists of vulnerabilities and attacks considered in here are by no means exhaustive, an attempt has been made to make the lists representative. Defenses against these vulnerabilities and attacks will be described in the remaining chapters of this book.

1.3.1 Threats

A pragmatic approach to building a secure system is to consider the threats that the system might face after deployment. We consider three main categories of threats:

- amateur adversary;
- professional adversary;
- well-funded adversary.

Some examples of amateur adversaries are script kiddies or hobbyist hackers. Crime syndicates or terrorist organizations can be considered as professional adversaries. Foreign intelligence services can be considered as an example of a well-funded adversary. The above categorization implicitly governs the types of attacks that can be launched by each type of adversary. Amateur adversaries can launch unsophisticated attacks such as wireless sniffing or denial of service. A professional adversary can launch more sophisticated attacks such as layer 2 hijacking, man-in-the-middle attack, or Sybil attack (explained in Chapter 4). A well-funded adversary does not have any constraints on money. Such an adversary can launch very sophisticated attacks such as rushing attacks, wormhole attacks (explained in Chapter 4), as well as capture devices that are part of the network.

1.3.2 Vulnerabilities in Ad Hoc Networks

Mobile computing has introduced new types of computational and communication activities that seldom appear in fixed or wired environments. For example, mobile users tend to be stingy about communication due to slower links, limited bandwidth, higher cost, and battery power constraints. Mechanisms like disconnected operations and location-dependent operations only appear in the mobile wireless environment. Application and services in a mobile wireless network can be a weak link as well. In these networks, there are often proxies and software agents running in intermediate nodes to achieve performance gains through caching, content transcoding, or traffic shaping. Potential attacks may target these proxies or agents to gain sensitive information or to mount denial of service (DoS) attacks, such as flushing the cache with bogus references, or having the content transcoder do useless and expensive computation. In this environment it is also difficult to obtain enough audit data. Mobile networks do not communicate as frequently as their wired counterparts. This can be a problem for intrusion detection systems attempting to define normality for anomaly detection.

Among the intrinsic vulnerabilities of ad hoc networks, some reside in their routing, others in their use of wireless links and still some others in their auto-configuration mechanisms. These key functionalities of ad hoc networks are based on complete trust between all the participating hosts. In the case of routing, the correct transport of the packets in the network relies on the veracity of the information given by the other nodes. The emission of false routing information by a host could thus create bogus entries in routing tables throughout the network, making communication difficult. Furthermore, the delivery of a packet to a destination is based on hop-by-hop routing, and thus needs total cooperation from the intermediate nodes. A malicious host could, by refusing to cooperate, quite simply block, modify, or drop the traffic traversing through it. By fooling the routing algorithm or even by choosing a strategic geographic positioning, a host can control the traffic to and from entire parts of the network.

Use of wireless links makes these networks very vulnerable to attacks ranging from passive eavesdropping to active interfering. An attacker just needs to be within radio range of a node in order to intercept network traffic. The current design of wireless networks places a lot of emphasis on cooperation. A very good example of this is the design of medium access control protocols used in these networks. Since these protocols follow predefined procedures to access the wireless channel, a misbehaving node can easily change the MAC protocol behavior, which may lead to a DoS attack.

The autoconfiguration mechanism also brings up new vulnerabilities. This functionality, whether it uses ICMP router advertisements, neighbor solicitation messages or simple DHCP autoconfiguration messages, is vulnerable to false replies. These processes use information given by the nodes on the network to either calculate an IP address or verify that a particular address is not already used. For example, in the case of duplicate address detection (DAD), a danger exists that a malicious node may pretend to be using any of the addresses chosen by an incoming host, thus denying the incoming host the right to join the network.

Constraints existing in ad hoc networks also add to the vulnerabilities. For example, such networks have limited computational ability, as evidenced by low processor frequencies and smaller memory sizes. The limitations on power usage are another major constraint. This implies that it might be very easy for an adversary to launch DoS attacks in such networks by trying to exhaust the battery of a legitimate node. The nodes in such networks are also vulnerable to being physically captured, which may result in the cryptographic keys being exposed. Another problem with protecting wireless ad hoc networks is on account of the fact that there is much more uncertainty in such networks. This makes it more difficult to discriminate between malicious behavior and acceptable behavior. For example, significant levels of packet dropping may be the result of the physical characteristics of the wireless links. These packet drops might not necessarily imply an attack. Nodes may appear and disappear from the network not because they are being attacked but because of mobility and power constraints.

In addition, ad hoc networks also suffer from the vulnerabilities present in their wired counterparts such as passive eavesdropping, spoofing, replay, or denial of service. Some of these vulnerabilities are accentuated in a wireless context. The topology of an ad hoc network is defined by the geographical position and by the wireless emission ranges of its hosts. A consequence of this is that these networks do not have a clearly defined physical boundary and thus no clearly identified entry point into the network (since typically adversaries try to launch their attacks from outside the network). Access-control to the network, as it is traditionally achieved by a LAN's firewall, thus becomes more difficult to deal with. Attention should thus be placed on the problems of IP masquerading and passive eavesdropping, and a protection against these attacks should be implemented.

To summarize, a mobile ad hoc wireless network is vulnerable due to its features of open medium, dynamic changing network topology, cooperative algorithms, lack of centralized monitoring and management point, and a lack of a clear line of defense.

1.3.3 Attacks

In this book we focus on the problem of securing wireless ad hoc networks and describe techniques and mechanisms that can make such networks less vulnerable against malicious attacks. Attacks against the network may come from malicious nodes that are not part of the network and are trying to join the network without authorization. Such nodes are typically called outsiders. Networks are typically protected from malicious outsiders through the use of cryptographic techniques. Such techniques allow nodes to securely verify the identity of other nodes and can therefore try to prevent any harm being caused by the malicious outsiders. We also consider attacks from nodes that are authorized to be part of the network and are typically called insiders. Insider nodes may launch attacks because they have been compromised by an unauthorized user (e.g. hacker) through some form of remote penetration, or have been physically captured by a malicious user.

We next discuss some possible attacks against wireless ad hoc networks. The list of attacks provided here is by no means a comprehensive list of possible attacks but provides a broad view of the attacks that need to be addressed which will motivate the subsequent chapters discussing approaches to defending against such attacks. Some example attacks that are possible in an ad hoc setting are:

1 *Routing Attacks*—in this case the adversary mounts attacks on the routing protocols or on the routing tables. For example, the adversary could disseminate false routing information. There are several attacks that fall into this category. We look at some of these in more detail in Section 1.3.3.1. We also provide ways of defending against these attacks in Chapter 4.

2 *Sleep Deprivation*—usually this attack [1] is practical only in wireless networks where battery life is a critical parameter. Battery-powered devices try to conserve

energy by transmitting only when absolutely necessary. In this attack a malicious user interacts with a node with the intention of draining the battery of the node. For example, an attacker can attempt to consume battery power by requesting routes from that node, or by forwarding unnecessary packets to that node, or by disrupting routing to route an excessive amount of traffic to that node.

3 *Location Disclosure*—a location disclosure attack can reveal information about the locations of nodes or the structure of the network. The information gained might reveal which other nodes are adjacent to the target, or the physical location of a node. The attack can be as simple as using the equivalent of the trace route command on Unix systems. As a result, the attacker knows which nodes are situated on the route to the target node. If the locations of some of the intermediary nodes are known, information can be obtained about the location of the target as well.

4 *Eavesdropping*—eavesdropping is a very easy passive attack in the radio environment. When one sends a message over the wireless medium, everyone equipped with a suitable transceiver in the range of the transmission can potentially decode the message and obtain sensitive information. The sender or the intended receiver has no means of detecting if the transmission has been eavesdropped. However, this attack can be prevented by using an encryption scheme at the link level to protect the transmitted data. Of course, this requires efficient key distribution strategies so that keys for encrypting the transmitted traffic can be transmitted to all nodes. We will look at such key distribution strategies in more detail in Chapter 3.

5 *Traffic Analysis*—the objective of an adversary launching this attack is to extract information about the characteristics of transmission. This could include information about the amount of data transmitted, identity of communicating nodes, or their locations. Prevention of this attack is not easy. One approach is to make use of routing protocols that make it difficult to get this information. Some examples of such routing protocols are given in Chapter 4.

6 *Denial of Service*—denial of service attacks are also easily applied to wireless networks, where legitimate traffic cannot reach clients or the access point because illegitimate traffic overwhelms the frequencies. DoS attacks are possible at various layers, namely, physical layer, MAC layer, and network layer, and also on the applications executing in such networks. For example, jamming of radio frequencies could be done at the physical layer similarly, violation of medium access control rules could lead to denial of service at the link layer.

7 *Sybil Attack*—in this attack [2] a single node attempts to adopt multiple identities. This attack will be discussed in detail in Chapter 4.

1.3.3.1 General Description of Routing Attacks Routing is a very important function in MANETS, as described earlier. It can also be easily misused, leading to several types of attack. We next describe some of the attacks on routing in MANETS.

Routing protocols in general are prone to attacks from malicious nodes. These protocols are usually not designed with security in mind and often are very vulnerable to node misbehavior. This is particularly true for MANET routing protocols because they are designed for minimizing the level of overhead and for allowing every node to participate in the routing process. Making routing protocols efficient often increases the security risk of the protocol and allows a single node to significantly impact the operation of the protocol because of the lack of protocol redundancy.

Below are some examples of attacks that can be launched against MANET routing protocols. The reader is referred to the literature [3–6] for a discussion of the various types of attacks against routing protocols and ways of categorizing those attacks. We would also like to remark here that we discuss several routing protocols that address one or more of these attacks in Chapter 4.

- *Black Hole Attack*—in this attack, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. The attacker will then receive the traffic destined for other nodes and can then choose to drop the packets to perform a denial-of-service attack, or alternatively use its place on the route as the first step in a man-in-the-middle attack by redirecting the packets to nodes pretending to be the destination.
- *Spoofing*—a node may attempt to take over the identity of another node. It then attempts to receive all the packets destined for the legitimate node, may advertise fake routes, and so on. This attack can be prevented simply by requiring each node to sign each routing message (assuming there is a key management infrastructure). Signing each message may increase the bandwidth overhead and the CPU utilization on each node.
- *Modifying Routing Packets in Transit*—a node may modify a routing message sent by another node. Such modifications can be done with the intention of misleading other nodes. For example, sequence numbers in routing protocols such as AODV are used for indicating the freshness of routes. Nodes can launch attacks by modifying the sequence numbers so that recent route advertisements are ignored. Typically it is particularly difficult to detect the node which modified the routing message in transit. Requiring each node to sign each routing message can prevent these types of attacks. In such a case, if a node modifies routing packets, then it might escape undetected, but it will not be able to mislead other nodes because the routing messages will not have the appropriate signature. Other nodes can detect illegal modifications in the packet via the cryptographic protection mechanisms.
- *Packet Dropping*—a node may advertise routes through itself to many other nodes and may start dropping the received packets rather than forwarding them to the next hop based on the routes advertised. Another variation of this attack is when a node drops packets containing routing messages. These types of attacks are a specific case of the more general packet dropping attacks.
- *Selfish Nodes*—routing in MANET depends on the willingness of every node to participate in the routing process. In certain situations nodes may decide not to participate in the routing process. For example, nodes may do that in order to conserve battery power. If several nodes decide to do that then the MANET will break down and the network will become inoperable. Certain protocols have been proposed for encouraging nodes to participate in the routing process.
- *Wormhole Attack*—in this attack adversaries can collude to transport routing and other packets out of band (using different channels). This will interfere with the operation of the routing protocols. We will discuss this attack in more detail in Chapter 4.
- *Rushing Attack*—in this case, an adversary can rush some routing packets towards the destination, leading to problems with routing. We explain this attack and protection mechanisms against this attack in Chapter 4.

1.4 OVERVIEW OF THE BOOK

As discussed earlier, wireless ad hoc networks have attracted much interest in the research community due to their potential applications. The key characteristic of such networks is their openness, which makes it possible for nodes to come together and form a network with no human intervention and with no existing pre-established infrastructure. Unfortunately this characteristic that makes such networks so important also makes them vulnerable to a wide variety of attacks. In this book, we focus on the problem of securing wireless ad hoc networks and discuss potential solutions for protecting such networks. We focus on solutions that are unique to the wireless ad hoc networking environment. We attempt to explain a large number of solutions and techniques that have been discussed for securing wireless ad hoc networks. We discuss the advantages of these approaches and often their limitations. Securing such networks is a very challenging task, as discussed earlier. Often no perfect solution exists. In such cases we attempt to identify the limitations of the most promising approaches and discuss additional areas that require further research.

Typically, protection of networks is achieved using multiple overlapping approaches (multiple layers of defense) that make it difficult for an attacker to penetrate the network. The approaches used to secure wireless ad hoc networks can be considered to belong to three broad categories: (1) prevention approaches that try to prevent an attacker from penetrating the network and causing harm; (2) detection approaches that detect an attacker after the attacker has already penetrated the preventive barriers; and (3) response and recovery approaches that attempt to respond to an attacker once he/she has been detected to have penetrated the preventive barriers. We will discuss solutions and mechanisms that address all of these approaches. The book is structured as follows:

- Chapter 1 provides a general description of wireless ad hoc networks. Several applications that motivate the importance of this technology are also considered. The chapter also discusses the unique challenges associated with securing such networks.
- The next three chapters focus on protection mechanisms. A key protection mechanism is cryptography, which makes it difficult for malicious nodes to eavesdrop on traffic from other nodes, modify such traffic, or pretend to be somebody else. Chapter 2 discusses some of the fundamental concepts of cryptography that we leverage in later chapters. Several mechanisms for securing wireless ad hoc networks rely on cryptography and this chapter provides the foundation needed to understand such mechanisms.
- Communication is a basic function needed by the entities in the network. Further, communication between entities has to be done securely in order to protect against various attacks that can be launched by the adversaries. However, this is dependent on the sharing of cryptographic keys among the network entities. Chapter 3 discusses several schemes for sharing keys among nodes in wireless ad hoc networks.
- Routing is one of the fundamental requirements in a MANET. Most of the routing protocols have been built with the goal of establishing quick and efficient communication among nodes. Often those goals are orthogonal to the goal of providing secure connectivity. In Chapter 4 we consider some of the widely used MANET routing protocols and describe ways of securing such protocols.
- In spite of all the preventive mechanisms, adversaries might still be able to penetrate the network and launch attacks. Several mechanisms have been proposed in order to

detect such occurrences. Chapter 5 discusses intrusion detection techniques that can be used for detecting malicious behavior in MANETs.

- Once an attack is detected, it is important for appropriate response and recovery steps to be taken. Such actions need to be quick and preferably with limited or no human intervention. This will make it possible to have the network operational quickly so as to continue supporting the application of interest. Chapter 6 discusses the concept of policy management, which has been proposed as a way to automate management of networks. Such automation includes responding to specific events, including faults and attacks. Policy management allows network administrators to define the response of the network to the various events.
- The following chapter focuses on an interesting application, namely secure localization. Nodes in wireless networks are typically mobile. Identifying the location of a node is important for a variety of applications. Various approaches have been proposed for estimating the current location of a node. Several of those approaches are open to attacks from malicious users. Chapter 7 discusses some of the localization schemes and approaches for securing such schemes.
- Chapter 8 introduces another topic of special interest, namely the application of wireless ad hoc networks in vehicular networks. This is an area that we believe will attract a lot of interest in the future. This chapter also presents the conclusion of this book.