1

Introduction

Although the wireless medium has limited spectrum and additional constraints when compared to guided media, it provides the only means of mobile communication. In addition, more effective usage of the limited spectrum and advanced physical/data link layer protocols enable broadband communications and integrated services over the limited wireless spectrum. Moreover, random and rapid deployment of a large number of tetherless nodes is possible through wireless ad hoc networking, which is a technology with a wide range of applications such as tactical communications, disaster relief operations and temporary networking in areas that are not densely populated. As a result, the use of wireless ad hoc networking has become pervasive. However, wireless ad hoc networking also introduces additional security challenges on top of those that exist for tethered networking:

- the wireless broadcast medium is easier to tap than guided media;
- the wireless medium has limited capacity and therefore requires more efficient schemes with less overhead;
- the self-forming, self-organization and self-healing algorithms required for ad hoc networking, and the schemes that tackle challenges such as hidden and exposed terminals, may be targeted to design sophisticated security attacks;
- the wireless medium is more susceptible to jamming and other denial-of-service attacks.

Wireless sensor and actuator networks (WSANs) are based on the random deployment of a large number of tiny sensor nodes and actuators into or very close to the phenomenon to be observed. They facilitate many application areas such as tactical surveillance by military unattended sensor networks, elderly and patient monitoring by body area networks (BANs) and building automation by building automation and control networks (BACnets). They are, in essence, ad hoc networks with additional and more stringent constraints. They need to be more energy efficient and scalable than conventional ad hoc networks, which exacerbates the security challenges. The security schemes for WSANs should require less computational power and memory because sensor nodes are tiny and have more limited capacity than the typical ad hoc network nodes such as a personal digital assistant (PDA) or a laptop computer.

Security in Wireless Ad Hoc and Sensor Networks Erdal Çayırcı and Chunming Rong

The wireless mesh network (WMN) is another member of the ad hoc network domain. WMNs enable application areas such as infrastructureless networks for developing regions, low-cost multihop wireless backhaul connections and community wireless networks. Actually, ad hoc networks can be considered a subset of WMNs because WMNs also provide a wireless backbone for working other mesh, ad hoc or infrastructure-based networks such as the Internet, IEEE 802.11, IEEE 802.15, IEEE 802.16, cellular, wireless sensor, wireless fidelity (Wi-Fi), worldwide interoperability for microwave access (WiMAX) and WiMedia networks. Lack of central authority and the availability of various access technologies to access the network make WMNs a more challenging domain in terms of security.

1.1 Information Security

In order to make the above and many more ad hoc application scenarios practical, they need to be secured against attacks. A security attack is an attempt to compromise the security of information owned by others (RFC 2828). We classify and examine all the security attacks designed to target ad hoc networks in the second part of this book. Security services are needed to defend against these attacks and to ensure the security of the information; these services can be categorized into two broad classes, namely *communications security* and *computer security* (Figure 1.1). Communications security defends against passive or active attacks through communication links or unintentional emanations. It ensures that communication services continue with the required level of quality and that classified data or information cannot be derived or captured from communications by an unauthorized node. Computer security ensures the security of computer hardware and software. It detects when a node or host is compromised, and recovers that specific node or host from the attack.

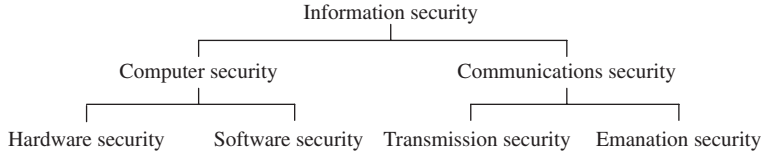

Figure 1.1 Information security

1.1.1 Computer Security

Host computers or network nodes can be attacked physically, and certain hardware components may be replaced, damaged or put out of service. Moreover, hardware can be infected by microbes which eat electronic components. Hardware security is designed to prevent, detect and repair these kinds of physical attack.

Another form of attack against computer hardware, especially in a battlefield, may be carried out by electromagnetic pulse (EMP) weapons. Portable systems that can emit EMPs are

now available and critical hardware can be built to resist such attacks. Note that EMPs not only damage the software but also burn the hardware.

Viruses, worms and Trojan horses are examples of techniques used to attack software. They are programs that can infect an adversary's computer. A virus can duplicate itself many times and is generally designed to cause damage to the attacked software. A Trojan horse is a means of gaining unauthorized access to an attacked system. Finally, a worm copies itself from one node to another in the network and consumes resources such as computational power and memory. There are various software packages to eliminate these kinds of threat. However, most of them can detect only known viruses, worms and Trojan horses. Therefore, they rely heavily on the availability of the signature related to the attacking program.

1.1.2 Communications Security

An important part of communications security is transmission security, which is designed to prevent classified data in transmission being disclosed to unauthorized recipients, to defend against attacks that compromise a computer via communications links and to ensure that communication services are not hindered by malicious attacks. Note that once a computer is compromised or infected by a virus via a network connection, counteracting this falls under the remit of computer security. However, a compromised node can be used to attack a network from inside, and securing a network from an internal attack should also be considered within the scope of transmission security.

Emanation security is another important part of communications security. Computers may unintentionally transmit through Van Eck radiation or conduction. Every piece of electronic equipment, for example a computer, photocopier, printer, telephone, etc, radiates electromagnetic waves called *Van Eck radiation*. It is possible to receive this radiation and fuse the screen shots, key strokes and copied documents from a distance. Conduction of classified data through power lines, metal ducts, water pipes, wires and cables that are close to the media that carry or store these data is also possible. Emanation security aims to prevent this, and this field has been studied extensively by the military. The system is called TEMPEST, which is not an abbreviation but a word made up for military purposes.

1.2 Scope of the Book

In this book, we focus on transmission security for wireless ad hoc, sensor and mesh networks (WASMs). Transmission security has also been called *network security* or *Internet security* by other authors. All these terms are synonymous for us and incorporate all information security issues except for computer security and emanation security, explained in the previous subsection. Although our focus is on transmission security, we refer to both computer security and emanation security as they become relevant, because Van Eck radiation and EMP in particular are important issues for the military, and one of the most important application areas for WASMs is tactical field. Note that the utmost care has been taken not to disclose any classified information in this book. Everything explained in the book is generic, i.e. it does not reflect any specific tactical system but general requirements and design principles, all of which are already in the public domain.

The book elaborates all the known security weaknesses of WASMs and explains the potential threats and attacks that can capitalize on these weaknesses. We examine how to provide the following security services in the presence of these potential threats and attacks:

- authentication to ensure that a message is from the claimed source;
- access control to prevent the unauthorized use of network resources;
- data confidentiality to ensure that classified data cannot be disclosed by an unauthorized recipient;
- data integrity to ensure that a message is not modified during transmission;
- nonrepudiation to ensure that both the source and the destination are as specified in the message.

Other security-related issues such as the following are also within the scope of this book:

- defense against denial-of-service (DOS) attacks;
- reliable end-to-end services in a hostile environment;
- secure routing;
- measures to prevent the misuse of limited resources;
- measures to reduce the cost, i.e. computational, memory and power consumption, of security schemes.

1.3 Structure of the Book

This book is designed as a self-contained textbook for both academicians and practitioners. Therefore, it has two parts. It first introduces fundamentals and key issues related to WASMs. Although the primary goal of the first part is to provide the reader with the requisite background knowledge, we also highlight and explain the facts that have an impact on information security in this part. In the second part, we present advanced information on security for WASMs.

The first part of the book consists of seven chapters including the Introduction. The second chapter explains WASMs and the application areas. We also provide a subsection about tactical communications in this chapter because it is one of the most important application areas and has some special features that impact on security. Then we examine the factors influencing the design of the networks in our domain and how they impact on security schemes.

The fundamentals about the wireless medium are explained in Chapter 3, where the requisite knowledge for the physical layer is provided. The propagation environment, modulation, wireless channel impairments, jamming and the security considerations related to these issues are elaborated in this chapter.

Chapters 4, 5 and 6 explain the challenges and solutions in the data link, network and transport layers respectively. This layered approach is designed to provide interoperability and reusability of the protocols and schemes. However, it does not always lead to the optimal solutions. Therefore, transparency from the lower layer details, interoperability and reusability of protocols may be achieved at the expense of a more costly protocol stack compared to the cross-layer design. Since WASMs introduce some very stringent constraints; cross-layer protocols are common in our domain.

In Chapter 7, challenges specific to WASMs, such as node localization, time synchronization, addressing, coverage, mobility and resource management, are introduced together with the solutions available in the literature. Again, the security implications of the schemes that tackle these challenges are presented.

The second part of the book consists of eight chapters and starts with a detailed discussion of security attacks in WASMs. Then the cryptographic primitives are explained in Chapter 9. Challenges and solutions related to the basic issues such as bootstrapping, key distribution and integrity are covered in Chapter 10. Chapter 11 is about the challenges and solutions related to protection such as privacy, anonymity, intrusion detection, traffic analysis, access control, tamper resilience, availability and plausibility.

The self-forming, self-organization and self-healing features of ad hoc networks create new challenges for information security. These challenges and solutions related to secure routing are provided in Chapter 12, which is followed by another chapter about challenges and solutions specific to WASMs.

We also provide a short introductory chapter about information operations and electronic warfare and how this relates to security in WASMs in Chapter 14. Note that electronic warfare is a huge topic alone, and our intention is to provide only introductory coverage. Our final chapter is about the standards related to the security in wireless networks.

1.4 Electronic Resources for the Book

The book has a website at http://www.securityinadhoc.net/. At this site you can access the following:

- **Slides:** Powerpoint slides to complement the content of the book are available at this link. The slides are designed for a 14-week course where the book provides the text. They are kept updated.
- **Updates table:** any updates and corrections to the book are listed in this table. If you have any comments or suggestions on how to improve our book, please email them to us by using the 'contact us' link on the website.
- **The interest group:** this link provides you with a user name and password to access the interest group for the content of the book.
- **Useful links:** links to useful websites are provided here.

1.5 Review Questions

1.1 What is information security? How can you categorize it?
1.2 What is Van Eck radiation?
1.3 What is emanation through conduction? How can it be prevented?
1.4 What are the differences between a virus, a worm and a Trojan horse?
1.5 What is an electromagnetic pulse attack?
1.6 What is a security attack?
1.7 What is a denial-of-service attack?
1.8 What are the security services?