

Preface

Securing communications is a challenging task. A first attempt at security involves learning basic cryptography, and applying encryption algorithms to make messages unintelligible to adversaries. However, rarely is the task of securing a message exchange so simple. When one steps back and contemplates how to secure the exchange of communications, one realizes that the challenge is fundamentally one of building a *complete* solution. For example, one must ensure that all entities involved have proper and authenticated cryptographic material, or one must ensure that one verifiably knows to whom one is communicating, or one must understand how the communication process takes place so as to make certain there are no vulnerabilities introduced by the communication process itself.

This last issue, namely that security methods are often built without consideration to how communication takes place, represents a fundamental gap where much of modern security research has fallen short. The security literature is filled with a mass of articles on cryptographic primitives and, although there are still many theoretical hurdles to be overcome by the cryptographic community, most of these shortcomings are academic and there are now numerous textbooks on cryptography that can provide the basic introduction needed to employ cryptographic primitives. On the other side of the coin, the security literature is also filled with a mass of articles devoted to building secure protocols and, similarly, there are now numerous textbooks on computer security that provide the instruction needed to design secure protocols. Unfortunately, the issue of how communication takes place or, more specifically, whether there are any specific issues that might arise or be circumvented because message exchanges are taking place on one medium versus another (e.g., wireless communication versus wired communication), is generally neglected.

In fact, although the layered approach to communication system design, as corresponds to the general Open Systems Interconnection (OSI) reference model, is often referred to in the design of network security protocols, the resulting protocols tend to be layer-specific and ignore the most fundamental of communication layers—the physical layer, whereby devices communicate through the encoding and modulation of information into waveforms. This is truly a sad situation, as it means that the approaches taken to secure modern communication systems are incomplete and, as

is often chanted as a mantra in the security circles, we should be concerned because “a system is only as strong as the weakest link.”

In response to this apparent shortcoming, this anthology presents a collection of chapters devoted to recent research results examining security issues at the physical layer. In particular, all of the authors amassed in this collection take the viewpoint that the physical layer of wireless communications should be considered as unique and different from the physical layer of other communication systems, and thus the challenges of securing the physical layer should take into account the special properties of the wireless medium. Throughout this book, a common theme that frequently emerges is that, in the rich multipath environment typical of wireless scenarios, the channel response of the medium along any transmit-receive path is frequency-selective (or in the time domain, dispersive) in a way that is location-specific (implying that channel responses decorrelate rapidly from one transmit-receive path to another if the paths are separated by the order of an RF wavelength). These unique space, time, and frequency characteristics of the wireless physical layer serve as a powerful basis for building new security services at the physical layer.

The chapters that we have assembled are contributions from a broad variety of research groups examining security issues at the physical layer of wireless systems. In selecting the contributions, we have sought to cover a spectrum of security issues (ranging from confidentiality to authentication to trustworthiness), as well as both theoretical and practical aspects of securing the physical layer. As such, the chapters in this book have been loosely organized thematically. We start by examining the issue of confidentiality at the physical layer. Confidentiality typically involves algorithms, like ciphers, and is concerned with the guarantee that information exchange is only able decipherable by legitimate entities. In the context of physical layer security, we are more concerned with mechanisms that use the wireless medium to support the confidential exchange of messages. Typically, though, the resulting mechanisms operate at communication rates that are much lower than their conventional *non-secret* counterparts, and thus physical layer confidentiality mechanisms should be used in support of conventional confidentiality mechanisms. For example, one might use physical layer confidentiality mechanisms to secretly exchange or establish conventional cryptographic keys.

Confidentiality mechanisms at the physical layer may be further decomposed into methods that secretly *disseminate* information using the properties of the wireless medium and methods that *extract* secret information from the wireless medium. We have arranged the confidentiality chapters by first examining the issue of disseminating information secretly. Most of these chapters explore the fundamental theoretical aspects related to secrecy dissemination, and several fundamental observations emerge. First, the fading process experienced in typical wireless communication scenarios is very special and can serve to enhance the ability to secretly communicate when compared to less harsh communication scenarios. Second, the broadcast nature of the wireless medium allows for one to introduce interference into the medium that can harm an adversary’s ability to eavesdrop while strengthening the ability for two legitimate entities to communicate. In all cases, knowledge of the channel state is important to the ability to communicate, and thus understanding the

properties of secret communication when there is incomplete or inaccurate channel information is important. Moving away from the foundational information-theoretic aspects of secrecy dissemination, are two chapters that are devoted to examining the design of specific coding schemes and which serve as the first step towards realistic implementations of secrecy dissemination methods.

The second set of confidentiality chapters seek to use the unique space, time and frequency properties of the wireless channel as the source of shared, secret information between a transmitter and receiver. If this shared, secret information can be mined from the wireless channel, then it can serve as the basis for establishing secret keys. Secrecy extraction techniques are a particularly promising direction for using the physical layer to enhance security as the basic step needed to support secrecy extraction, namely the probing of the wireless medium in order to obtain a channel estimate, is also a fundamental step to general communication, i.e., channel estimation is already performed in the physical layer of most wireless systems. Although the chapters devoted to secrecy extraction involve significant theoretical aspects, they also represent some of the most solid evidence in support of real-world deployment of physical layer security techniques. Many of the chapters include experimental evidence and, in one case, a real-time implementation, of the validity of physical layer security mechanisms.

Next we turn to the problem of authentication. Authentication typically involves providing assurance that entities are who they claim to be, or that messages come from where they claim to originate. At the physical layer, the notion of identity is different. In this context, we are not as worried with *who* someone is, but rather with being able to distinguish between different transmitters. In the general wireless authentication problem, we are concerned with an active adversary injecting communications into the medium and claiming that these transmissions come from a legitimate wireless device. Interestingly, there are many situations where cryptographic techniques for authentication are not easy to employ, and thus it is desirable for an entity to differentiate between signals coming from a legitimate entity and those coming from an illegitimate entity. Physical layer authentication methods are a natural complement to secrecy extraction techniques as, in both cases, the characterization of the wireless channel serves as the fundamental building block. Whereas for secrecy extraction the channel estimate serves as the secret information that is used to establish a key, for physical layer authentication the channel estimate serves as the authenticator to distinguish between transmitters and receivers. An interesting challenge that arises in physical layer authentication is the need to maintain the authenticator when the environment is dynamic and entities are moving around. Our two chapters on physical layer authentication include discussion on the theoretical limits of authentication, as well as provide a thorough survey of physical layer authentication, with special attention devoted to addressing the time-varying nature of the wireless channel.

Lastly, we look at two other aspects related to security and physical layer communication. Cooperative communications is an emerging technique to improve the channel capacity of wireless communication systems, and involves multiple entities assisting each other in the transmission and decoding of messages by relaying

replicas of transmitted messages. Unfortunately, traditional cooperative communication schemes assume that all entities are trustworthy and follow protocols precisely, and thus these promising communication schemes are particularly sensitive to scenarios where entities falsely or maliciously cooperate. We have included a chapter that examines the security issues that arise in cooperative communications, and proposes an improved design for strengthening the security of cooperative transmission schemes by carefully integrating the notion of trust into cooperative communication protocols. Our final chapter discusses the issue of modulation forensics, which involves identifying the type of modulation that is being employed when there is no prior information about the transmitter. This is particularly important for emerging wireless systems, such as cognitive radio systems, where there may not be any prior relationship between a transmitter and a receiver, and it is necessary to identify the communication methods being employed before commencing with communication. Further, such analysis is also important in conducting attacks against the physical layer as knowing what modulation methods are being employed allows one to best adapt their attacks, whether attempting to spoof an entity or interfere with that entity.

We note that the physical layer for wireless systems provides an exciting collection of tools to enhance security that is not available to one who strictly employs a cryptographic toolkit. Traditional higher-layer security methods must play an important role in securing communications and certainly physical layer security techniques should not be considered a replacement for well-tested cryptography algorithms and security protocols. However, the properties of the wireless medium are a powerful source of domain-specific information that can be used to complement and enhance traditional security mechanisms that has remained, to date, an untapped resource and thus should be considered as expanding the tools available to engineers seeking to secure wireless systems. The methods described in this book will serve as the basis for removing a potential weak link in the design of future wireless systems and, as wireless systems become increasingly pervasive, we expect that physical layer security methods will be very useful in thwarting attacks that cannot be dealt with using conventional network security mechanisms.

Securing Wireless Communications at the Physical
Layer

Liu, R.; Trappe, W. (Eds.)

2010, XVI, 396 p., Hardcover

ISBN: 978-1-4419-1384-5