Chapter 4
Physical Layer Security in Wireless Communication Networks

Özge Cepheli
Istanbul Technical University, Turkey

Güneş Karabulut Kurt
Istanbul Technical University, Turkey

ABSTRACT

Physical layer (PHY) security has become an emerging area of research recently. Wireless networks use unguided medium as communication channels, so gathering wireless data transmission is easier when compared to traditional cable systems. With the rise of new security challenges, many different solutions have been offered and are being developed. However, maintaining security in wireless networks still remains a challenge. Secure transmission techniques in these networks are discussed throughout this chapter. PHY security measures, the secrecy rate, the secrecy capacity, and the outage secrecy rate are introduced. Security needs of wireless networks are discussed and the related common attack types are described. Main countermeasures that are proposed to prevent these attacks are also presented with both practical and theoretical perspectives.

INTRODUCTION

In order to highlight the effect of mobility in current security systems, the network model of the Open Systems Interconnect (OSI) reference model can be considered (ISO/IEC 7498-1, 1994).This model, proposing a composition of seven layers; physical, data link, network, transport, presentation, session and application layers, distributes network's functionalities to distinct layers that are assumed to act independently from other layers. Using the OSI reference model can provide a formal definition and practical terms that affects information security on a layer-by-layer basis.

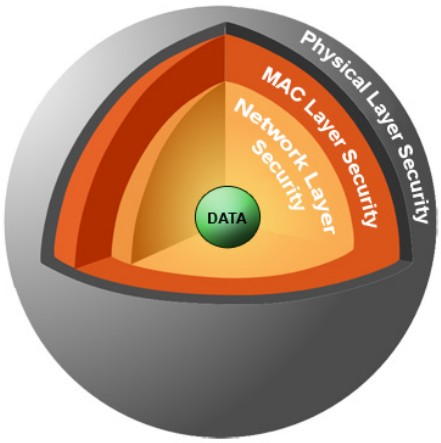
DOI: 10.4018/978-1-4666-4691-9.ch004

Security can be seen as an aggregation of protection mechanisms of different layers.

A conceptual visualization of layered security solutions is shown in Figure 1. One should pass through the security layers in order to acquire private data. In such cases, physical layer (PHY) security becomes inevitably important, as it forms the first step of the security system.

PHY security has become popular with the arising of wireless technologies. Wireless medium is potentially unsafe as the communications signals are broadcasted into air and anyone in the antenna range can access the transmitted signals. In traditional wired technologies, the possibility of the transmit signals are gathered by an untrusted third party may not be a main trouble, as physical security is deployed by hiding cables in walls and cable endpoints locked up in server rooms or cabinets. If one use a special device to "line in" to the link, a physical attempt needs to be done. Hence, even though it is not impossible, there is a certain difficulty for gathering the signals from a cable unless you have the endpoint. As a result, traditional systems usually accept that cable is secure, meaning that it is assumed that no one can access the data unless they access the endpoints. However, this assumption cannot be made for wireless networks, as wireless channels, unlike cables, are available to every node in a range equipped with a proper receiving antenna.

Figure 1. Layers of data



In this chapter, information theoretical approaches, which are also included in the initial PHY security studies, will be introduced. This will be followed by a discussion of physical vulnerabilities of wireless systems. Common PHY attacks, namely eavesdropping, traffic analysis, jamming, massage modification, information disclosure, masquerade, ID theft, man-in-the-middle and denial of service will be introduced to the reader afterwards. The book chapter will introduce PHY security methods under two titles; code based methods and signalling based methods, along with the corresponding attack types that they aim to prevent.

In this chapter, signalling based methods will be the main focus of the countermeasures. Beamforming and artificial noise techniques are proven to be effective countermeasures for privacy attacks and are therefore very important. *Beamforming* is a multi-antenna technique that enables the transmitter to focus signals spatially. *Artificial noise* (AN) is a recent concept that is utilized in PHY security methods, consisting of transmitting noise signals generated by the transmitter to non-legitimate users to degrade their signal reception quality. The AN studies in the literature usually follow isotropic AN and smart AN approaches (Liao, 2011). Isotropic AN approach is based on broadcasting the generated noise without spatial selectivity (except for the legitimate user's direction), whereas the smart AN approach is based on sending AN only to only the locations and/or frequency bands where eavesdropper exists. Here, we will give also a comparison of AN techniques. This chapter will be concluded with the open issues about implementations of PHY security countermeasures.