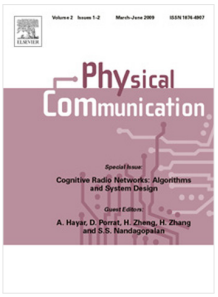
Accepted Manuscript



On physical-layer concepts and metrics in secure signal transmission

Ertuğrul Güvenkaya, Jehad M. Hamamreh, Hüseyin Arslan

PII: S1874-4907(17)30090-3
DOI: http://dx.doi.org/10.1016/j.phycom.2017.08.011
Reference: PHYCOM 421

To appear in: *Physical Communication*

Received date : 23 March 2017
Revised date : 12 August 2017
Accepted date : 12 August 2017

Please cite this article as: E. Güvenkaya, J.M. Hamamreh, H. Arslan, On physical-layer concepts and metrics in secure signal transmission, *Physical Communication* (2017), http://dx.doi.org/10.1016/j.phycom.2017.08.011

On Physical-Layer Concepts and Metrics in Secure Signal Transmission

Ertuğrul Güvenkaya[1], Jehad M. Hamamreh[2] and Hüseyin Arslan[1,2]

[1]Department of Electrical Engineering, University of South Florida, Tampa, FL 33620 USA

[2] School of Engineering and Natural Sciences, Istanbul Medipol University, Istanbul 34810 Turkey

Emails: ertugrul@mail.usf.edu; jmhamamreh@st.medipol.edu.tr; arslan@usf.edu

Abstract

Communication secrecy in the wireless systems has unique challenges due to broadcasting nature of the radio waves, as compared to its wire-line counterpart. At the same time, different and independent perceptions of the transmitted signal by the legitimate receiver and the eavesdropper provide new opportunities for secure communication. The distinctness in the physical propagation environment, e.g., in received power, wireless channel, and location of the legitimate and illegitimate nodes, when coupled with random and unique signatures, can be exploited for secure communication without using secret keys. In this paper, fundamental stages as well as requirements of the physical layer (PHY) security in information transmission are reviewed from a novel perspective. Then, main performance metrics in secure communication are surveyed including from information theoretic measures to practical considerations along with associated generalizations. The presented comprehensive viewpoint of PHY security stages and metrics is helpful to better understand the techniques exploiting the physics to secure the information in the lowest layer of the communication system.

Index Terms

Eavesdropping, PHY-security, secrecy rate, security gap, wireless communications, wireless fading channel.

I. Introduction

The communication between distant entities requires exposing the message to outside world in some form of signal transmission. When the physical propagation medium between the transmitter and receiver is not perfectly secured, information transmission comes with confidentiality issues. That is, the transmitted signal is subject to be captured by an unintended third entity with not so good intention, i.e., eavesdropper. Security risk in the propagation can be due to protocol-based such as shared medium, or physical phenomenons such as wireless propagation of radio waves. In particular to wireless systems, although broadcasting nature of the radio waves provides benefits such as connectivity, support of mobility, and flexibility in communication distance, wireless transmission leads to security vulnerabilities due to the lack of physical boundaries preventing the eavesdroppers from capturing the transmitted message.

The key for achieving secure communication is to put the eavesdropper at a relative disadvantage compared to the legitimate receiver [1]. This can be performed by some cooperation between the transmitter and the receiver such as encryption/decryption, which has been a widespread method for securing the data in both storage and transmission phases. The other approach is to exploit the discrepancies in the physical characteristics of the propagation environment. Namely, nonidentical observations of the transmitted signal by the legitimate and illegitimate receivers, stemming from wireless channel, location, and antenna configurations can be the enabling factor for secure communication.