Hindawi Publishing Corporation
EURASIP Journal on Wireless Communications and Networking
Volume 2009, Article ID 404061, 2 pages
doi:10.1155/2009/404061

Editorial

Wireless Physical Layer Security

Mérouane Debbah,[1] Hesham El-Gamal,[2] H. Vincent Poor,[3] and Shlomo Shamai (Shitz)[4]

[1] *Alcatel-Lucent Chair on Flexible Radio, Supélec, 3 rue Joliot-Curie, 91192 Gif-sur-Yvette Cedex, France*
[2] *Department of Electrical & Computer Engineering, Ohio State University, 205 Dreese Labs, 2015 Neil Avenue, Columbus, OH 43210, USA*
[3] *Department of Electrical Engineering, Princeton University, Engineering Quadrangle, Olden Street, Princeton, NJ 08544, USA*
[4] *Department of Electrical Engineering, Technion, Technion City, Haifa 32000, Israel*

Correspondence should be addressed to Mérouane Debbah, merouane.debbah@supelec.fr

Received 31 December 2009; Accepted 31 December 2009

The issues of privacy and security in wireless communication networks have taken on an increasingly important role as these networks continue to flourish worldwide. Traditionally, security is viewed as an independent feature addressed above the physical layer, and all widely used cryptographic protocols are designed and implemented assuming the physical layer has already been established and provides an error-free link. However, with the emergence of ad-hoc and decentralized networks, higher-layer techniques, such as encryption, are complex and difficult to implement. Therefore, there has been a considerable recent attention on studying the fundamental ability of the physical layer to provide secure wireless communications. This paradigm is called Wireless Physical Layer Security. Physical layer security is an emerging research area that explores the possibility of achieving perfect-secrecy data transmission among intended network nodes, while possibly malicious nodes that eavesdrop upon the transmission obtain zero information. The breakthrough concept behind wireless physical layer security is to exploit the characteristics of the wireless channel, such as fading or noise, to provide secrecy for wireless transmissions. While these characteristics have traditionally been seen as impairments, physical layer security takes advantage of these characteristics for improving the security and reliability of wireless communication systems and networks.

Information theoretic security provides the theoretical basis behind wireless physical layer security. Historically, information theoretic security, which builds on Shannon's notion of perfect secrecy, was laid in the 1970s by Wyner and later by Csiszár and Körner, who proved seminal results showing that there exist channel codes guaranteeing both robustness to transmission errors and a prescribed degree of data confidentiality. In the 1970s and 1980s, the impact of these works was limited, partly because practical wiretap codes were not available, but mostly due to the fact that a strictly positive secrecy capacity in the classical wiretap channel setup requires the legitimate sender and receiver to have some advantage (in general, a better SNR) over the attacker. In recent times, information theoretic security has witnessed a renaissance due in part to the work of Maurer in the 1990s, who proved that even when a legitimate user has a worse channel than an eavesdropper, it is possible for him to generate a secret key through public communication over an insecure yet authenticated channel. In the past few years, significant effort has been applied to the study of information theoretic security for wireless channel models, enhancing the classical wiretap channel and including more realistic assumptions which allow for opportunistic exploitation of the space/time/user dimensions of wireless channels for secret communications.

The goal of this special issue is to present recent results in wireless physical layer security that capture the research trends in the field. The papers to be found in this issue provide the reader with a good overview of these trends.

This special issue collects 10 papers clustered into two groups: papers dealing with information theoretic aspects and papers focusing on practical scenarios.

The first group of papers provides information theoretic results for wireless physical layer security. The first of these, by Bustin et al., derives a closed-form expression for the secrecy capacity of the multiple-input multiple output (MIMO) Gaussian wiretap channel, under a power-covariance constraint. The proof uses a clever relationship between information theory and estimation theory in the Gaussian channel that can be extended to other types of MIMO channels. The paper by Ekrem et al. characterizes the secrecy capacity region between a single transmitter and multiple receivers in a broadcast channel in the presence of an eavesdropper. It provides a clear understanding of secure broadcasting, studying several special classes of channels, with increasing generality. The third paper, by Aggarwal et al., looks at the secrecy capacity of relay channels with orthogonal components in the presence of an additional passive eavesdropper node. Inner and outer bounds on the secrecy capacity are developed for both the discrete memoryless and the Gaussian channel models. The paper by Wang et al. studies secret sharing over the fast-fading MIMO wiretap channel. The key capacity is evaluated where the effects of spatial dimensionality created by the use of multiple antennas at the source, destination, and eavesdropper are investigated. The fifth paper, by Liang et al., focuses on the compound wire-tap channel, which generalizes Wyner's wire-tap model to allow both the channel from the transmitter to the legitimate receiver and that from the transmitter to the eavesdropper to take a number of possible states. The secrecy capacity is studied and established for various cases of interest (degraded, MIMO, etc.). Finally, the paper by He et al. considers a source-destination pair that can communicate only through an untrusted intermediate relay node. In this two-hop communication scenario, in which the use of the untrusted relay node is essential, a positive secrecy rate is shown to be achievable and an upper bound on it is provided.

The second group of papers focuses on more practical aspects of wireless physical layer security. The first of these papers, by Tsouri et al., makes use of channel randomness, reciprocity and fast decorrelation in space to secure orthogonal frequency division multiplexing (OFDM) with low overhead on encryption, decryption, and key distribution. These properties make this approach a good alternative to traditional software-based information security algorithms in systems where the costs associated with such algorithms are an obstacle to implementation. The second paper, by Zhan et al., proposes a space-time coding scheme for impulse radio ultra-wideband (UWB) systems. A novel real orthogonal group code is designed for multiantenna UWB signals to exploit the full spatial diversity gain and achieve perfect communication secrecy. The third paper, by Han et al., introduces a game theoretic approach to investigate the interaction between the source that transmits the useful data and friendly jammers who assist the source by masking the eavesdropper. To analyze the outcome of the game, a Stackelberg-type game is investigated and a distributed algorithm is provided. Finally, the paper by Kobayashi et al. studies the frequency-selective broadcast channel with confidential messages, in which the transmitter sends a confidential message to the first receiver and a common message to both receivers. A practical Vandermonde precoding approach is provided for which the achievable rate region is studied.

Acknowledgments

We would like to thank the authors of all submitted papers (both those that were accepted and those that, regrettably, could not be included) for considering our special issue for disseminating their work. We extend our gratitude to the many, very conscientious reviewers for sacrificing so much of their time in order to make this special issue a success. Last but not least, we thank the members of NEWCOM++ for their joint collaboration in submitting high quality papers to this special issue. We also would like to thank the devoted staff of Hindawi for their high level of professionalism, and Luc Vandendorpe, the Editor-in-Chief of the journal, for trusting us with this important assignment and helping us to fulfill it successfully.

Mérouane Debbah
Hesham El-Gamal
H. Vincent Poor
Shlomo Shamai (Shitz)