The Department of Electrical and Computer Engineering

Announces the

Final Defense of Dissertation

Reza Sohrabi

Doctor of Philosophy, Graduate Program in Electrical Engineering
University of California, Riverside

Date: 12/11/2018
Time: 2:00-4:00 pm
Location: Winston Chung Hall 205

Jamming Strategies for Secure Wireless Communication

As the technology and computing power advance day by day, physical layer secrecy in wireless communications gains more importance. It allows the securing of wireless communications based on information theoretical guarantees without the need for cryptography. One important practical challenge for physical layer secrecy arises from the fact that no information about the passive eavesdroppers is available to the legitimate nodes. Without such information, optimizing the transmission parameters has always been a difficult task. In this study we aim to address most of the challenging aspects about this issue and propose a new perspective into the analysis of secrecy with a focus on jamming. We start from the case of known Eve's channel state information (CSI) in a three-node single-antenna multi-subcarrier network and present an improved optimization algorithm. Then we expand our horizon to the case of multiple-antenna nodes with unknown Eve CSI. In doing so, we investigate a secure wireless communication scheme which combines two of the most effective strategies to combat eavesdropping, namely mixing information with artificial noise at the transmitter and jamming from a full-duplex receiver. While such setup has been investigated in related works, new and important insights are revealed in this study. We investigate the design of optimal jamming parameters to achieve higher secrecy, and in particular we focus on two important cases corresponding to Bob using either a simple jamming or a smart jamming. We then derive a closed-form expression for asymptotic normalized instantaneous secrecy rate. Based on the results of the asymptotic analysis, we propose an alternative less complex tractable optimization problem for the design of optimal transmission parameters. We show that even with the optimal parameters, secrecy is compromised if Eve is able to increase her number of antennas. To address this issue, we provide a comprehensive analysis of a new scheme called anti-eavesdropping channel estimation (ANECE) which prevents Eve from acquiring accurate channel estimations. By asymptotic analysis, we show that the usage of such scheme, makes it extremely hard for Eve to drive secrecy to zero. Numerical analyses and simulations are presented to support the arguments made in this study.