Séminaire ICI : Miroslav Mitev

10 Juillet 2018, 14:00

Titre du séminaire et orateur

Wireless Secret Key Generation Exploiting Shared Randomness for Low Latency Applications.

Miroslav Mitev (University of Essex)

Date et lieu

Mardi 10 juillet 2018, 14h.

ENSEA, salle 384

Abstract

The security and integrity of communication systems, and especially of wireless networks, is a matter of increasing importance, affecting government, industry, commerce and the privacy and financial security of us all. Conventional cryptographic techniques are nearly all based on computational security in some form, and rely on the availability of secret keys. In this work we investigate novel cross-layer security protocols in which session keys are generated at the physical layer using standard techniques of secret key generation (SKG) from shared randomness. In this framework, we study the optimal power allocation in block-fading additive white Gaussian noise (BF-AWGN) channels with short-term power constraints when a subset of the subcarriers is used for SKG and the rest for data transmission. It is shown that optimally the strongest subcarriers–in terms of SNR–should be used for data and the weakest for SKG. Subsequently, a further step is taken in our analysis to account for active attacks by introducing a reactive jammer whose purpose is to compromise the SKG process. In this scenario, it is shown that the optimal power allocation in the presence of the adversary is solely determined by whether a minimum average power level is available for SKG.

Bio

Miroslav Mitev obtained his BSc from the Technical University of Varna, Bulgaria.Subsequently he finished with honours an internationally esteemed double degree MSc programme at the Technical University of Sofia (Bulgaria) and Aalborg University (Denmark). His interest in wireless communications led him to undertake an MSc dissertation on “Indoor Positioning for Smart Ambient Assisted Living Services” under the supervision of Prof. Albena Mihovska. After his graduation he had the privilege of working as a Research Assistant at the Center for TeleInFrastuktur (CTIF) in Aalborg University (Denmark). There, he worked on indoor localization in the “eWALL – For Active Long Living” project and studied the possibility of using such a service in a smart health monitoring environment with enhanced

privacy assurances. In 2017 he was offered the opportunity to become a PhD student at the University of Essex (UK) under the supervision of Dr. Arsenia Chorti and subsequently Dr. Martin Reed. The topic of his PhD is “Physical Layer Security for IoT applications”. Since April 2018 he is on a funded research visit at ENSEA (France), where he is working with Dr. Arsenia Chorti and Dr. Veronica Belmega on game theoretic analyses of active attacks on physical layer security systems.