PhD Defense Presentation

Tuesday, December 6, 2016
9:00 AM – 11:00 AM
Engineering Building Room 2219

SECURE AND EFFICIENT SPECTRUM SHARING AND QOS ANALYSIS
IN OFDM-BASED HETEROGENEOUS WIRELESS NETWORKS

By
Ahmed Alahmadi
Advisor: Dr. Tongtong Li

Department of Electrical & Computer Engineering
Michigan State University
The Internet of Things (IoT), which networks versatile devices for information exchange, remote sensing, monitoring and control, is finding promising applications in nearly every field. However, due to its high density and enormous spectrum requirement, the practical development of IoT technology seems to be not available until the release of the large millimeter wave (mmWave) band (30GHz-300GHz). Compared to existing lower band systems (such as 3G, 4G), mmWave band signals generally require line of sight (LOS) path and suffer from severe fading effects, leading to much smaller coverage area. For network design and management, this implies that: (i) MmWave band alone could not support the IoT networks, but has to be integrated with the existing lower band systems through secure and effective spectrum sharing, especially in the lower frequency bands; and (ii) The IoT networks will have very high density node distribution, which is a significant challenge in network design, especially with the scarce energy budget and the low cost requirements of IoT applications.

Motivated by these observations, in this dissertation, we consider three problems: (1) How to achieve secure and effective spectrum sharing? (2) How to accommodate the energy limited IoT devices? (3) How to evaluate the Quality of Service (QoS) in the high density IoT networks? We aim to develop innovative techniques for the design, evaluation and management of future IoT networks under both benign and hostile environments. The main contributions of this dissertation are outlined as follows.

First, we develop a secure and efficient spectrum sharing scheme in the HDTV bands. Cognitive radio (CR) is a key enabling technology for spectrum sharing, where the unoccupied spectrum is identified for secondary users (SUs), without interfering with the primary user (PU). A serious security threat to the CR networks is referred to as primary user emulation attack (PUEA), in which a malicious user (MU) emulates the signal characteristics of the PU, thereby causing the SUs to erroneously identify the attacker as the PU. Here, we start with single-carrier transmission, where the signal is processed in the entire spectrum. We consider full-band PUEA detection and propose
a reliable AES-assisted DTV scheme, where an AES-encrypted reference signal is generated at the DTV transmitter and used as the sync bits of the DTV data frames. For primary user detection, we investigate the cross-correlation between the received sequence and reference sequence. The malicious user detection can be performed by investigating the auto-correlation of the received sequence.

We further develop a secure and efficient spectrum sharing scheme in multi-carrier wireless networks. Motivated by the prevalence of the OFDM-based systems, we consider sub-band malicious user detection and propose a secure AES-based DTV scheme, where the existing reference sequence used to generate the pilot symbols in the DVB-T2 frames is encrypted using the AES algorithm, and the resulted sequence is exploited for accurate detection of the authorized PU and the MU.

Second, we develop an energy efficient transmission scheme in CR networks using energy harvesting. We propose a transmitting scheme for the SUs such that each SU can perform information reception and energy harvesting simultaneously. We perform sum-rate optimization for the SUs under PUEA. It is observed that the sum-rate of the SU network can be improved significantly with the energy harvesting technique. Potentially, the proposed scheme can be applied directly to the high density IoT network, which basically relies on transceivers with limited power capabilities.

Finally, we investigate QoS performance analysis methodologies, which can provide insightful feedbacks to IoT network design and planning. Taking the spatial randomness of the IoT network into consideration, we investigate coverage probability (CP) and blocking probability (BP) in relay-assisted OFDMA networks using stochastic geometry. More specifically, we model the inter-cell interference from the neighboring cells at each typical node, and derive the CP in the downlink transmissions. Based on their data rate requirements, we classify the incoming users into different classes, and calculate the BP using the multi-dimensional loss model. We show that the BP can be reduced by exploiting relay-assisted transmissions. Further study on IoT network design and routing protocol development under both benign and hostile environments will be conducted in our future research.
Publications

Journal Publications:


Conference Proceedings:

C1 Ahmed Alahmadi, Yuan Liang, Run Tian and Tongtong Li, “Blocking Probability Analysis for Relay-Assisted OFDMA Networks using Stochastic Geometry”, to be submitted to *IEEE Global Communications Conference (GLOBECOM17)*.


