Thesis Title: Physical Layer Security in Energy Harvesting Cooperative Networks

Student's Name: Kirti Kant Sharma

Entry Number: 2015BSZ8442

Abstract:

Telecommunication networks of the future will connect a vast number of heterogeneous devices wirelessly in the Internet of Things and machine-to-machine communications. Most of these applications require devices with a small size, low cost, and low energy consumption. Energy harvesting mechanisms will be a recommended feature in some of these devices due to the difficulty of charging and battery replacement due to device location and economic feasibility. Secure communications and energy efficiency for this large number of resource-limited devices are crucial due to the broadcast nature of the wireless medium and the severe repercussions of information leakage. Usually, cryptographic techniques are used for information security while assuming that the decryption will be difficult and take longer for an intruder without knowing secret keys. These schemes have challenges regarding key management, and the reliance on the eavesdropper's limited computing capabilities. Physical layer security techniques have been proposed as a low-complexity alternative for secure communications by utilizing the inherent random characteristics of wireless channels. These physical layer security techniques employ multiple antennas, carriers, artificial noise, and node cooperation to secure information transfer.

In this thesis, we first study the cost of secure transmission in terms of secure energy efficiency with relaying and jamming. We consider two cooperative scenarios in wireless networks to analyze secure energy efficiency. We propose a simple relay and jammer selection scheme for a decode-and-forward relaying network with friendly jamming in the first problem. Here, we study power allocation among selected nodes considering global channel state information to maximize secure energy efficiency. It is observed that the friendly jammer can improve energy efficiency with security compared to the relay-only scheme. In the second scenario, we analyze the secure energy efficiency of a direct link in the presence of an unknown eavesdropper with the help of multiple spatially-distributed friendly jammers. We propose a practical uncoordinated cooperative jamming with less system overhead. Jammers are selected according to the source-to-destination channel quality within

a finite region surrounding the source to limit energy consumption. We have considered a more realistic power consumption model with the transmit power of various nodes as well as their circuit consumption power. This analysis shows that some optimal value of selection parameters exists at which secure energy efficiency achieves maximum value.

Next, we analyze the importance of RF energy harvesting in cases of using a jammer and then an incremental relay to improve secrecy performance without the knowledge of the eavesdropper's channel state information. In these cases, we first utilize an RF energy harvesting cooperative jammer and analyze secrecy improvement in the presence of an unknown passive eavesdropper. By considering artificial noise transmission from a friendly multiantenna jammer with finite and infinite energy storage, the analytical expressions for secrecy outage probability are obtained considering the finite and infinite size energy buffer. This analysis shows that always-on jamming performs better than on-off jamming for the same buffer size. Results show the existence of an optimal secrecy rate to maximize secure throughput for a given source SNR. It is observed that the availability of jamming power has a more pronounced effect on secrecy outage than a larger number of antennas at the jammer. Further, we study the improvement in secrecy using a self-sustainable incremental relay and transmit antenna selection at both source and relay to reduce the feedback overhead. We propose a threshold-based incremental relaying scheme while considering both the direct and relaying links to the destination and eavesdropper. We have also considered the effect of outdated channel state information on secrecy performance. We model the energy present in the buffer as a discrete-time discrete-state Markov chain and derive a closed-form expression for secrecy outage probability. This analysis shows that the proposed scheme performs better than direct communication and conventional decode-and-forward relaying. Results show that secrecy performance can be further improved by choosing a proper value of the signal-to-noise ratio and energy threshold for relaying. These analyses show the adequacy of a finite buffer for RF energy harvesting at the cooperative node.