Stockholm, 28. November 2017

Master Thesis Project Proposal

Jamming-Resilient Deployment of Wireless Systems for IoT

Motivation - Smart infrastructures like smart grid, smart transportation, smart buildings, smart cities, etc. are nowadays heavily relying on wireless connectivity. While wireless connectivity enables remote sensing, actuation, and maintenance at low cost, it also increases the attack surface of smart infrastructures. A large body of IoT security research has recently focused on privacy and data integrity aspects. Unfortunately, much less attention has been paid to denial-of-service attacks carried out by jamming wireless transmissions.

Purpose - The goal of this thesis project is to:

- Provide a literature survey on jamming-resilient deployment of wireless systems in an IoT context.
- Develop mathematical models to describe the impact of a jammer on wireless systems; this includes different types of jamming strategies, channel access technologies, channel and propagation models, antenna configurations and deployments like CoMP, and non-linearity of RF frontends. If relevant, the available USRP hardware at ISE can be used to collect real-world measurement data and conduct experiments.
- Evaluate the impact of jamming attacks by system-level simulations.
- Propose new jamming-resilient deployment strategies and demonstrate their advantages in system level simulations.

Requirements - The candidate is expected to have good theoretic knowledge within the fields of communication theory and wireless communication. The candidate is also expected to be familiar with the key features of 4G and 5G wireless infrastructures. Very good – excellent programming skills are necessary. Experience with software defined radio platforms and wireless security is a plus.

Contact **Ragnar Thobaben**
Information Science and Engineering
KTH – School of Electrical Engineering
Email: **ragnart@kth.se**