King Saud University
College of Engineering
Electrical Engineering Department **Semester: 421**

Graduation Design Project Proposal Form

Project # C13

Project Title: Analysis and exploitation of modem wireless links for neutralization of unauthorised drones

Professor(s) Name(s): 1. Omar Aldayel
2. Sami Alhumaidi

Number of Students: Two to three

Students Qualifications

EE301, EE422, communication networks and MATLAB (or others for network simulation).

Statement of Problem/Brief Description of the Project

In this project, the student will apply their analytical and numerical knowledge to Analysis and exploitation of modem wireless links and networks. The first phase of this project (should take place in the first semester), will involve literature study of modem wireless links and networks. In the second phase, the students should implement their system of a Digital Signal Processor (DSP) or any type circuit board/controller and evaluate the pros and cons of hardware options in term of cost, reliability, size and accuracy.

Objectives

(1) Study and understand the concept of wireless links and networks.
(2) Study and understand the exploitation of modem wireless links.
(3) Implement these method(s)/Algorithm(s) using MATALB and evaluate their performance in terms of accuracy, computational complexity, etc
(4) Implement the candidate method/algorithm on real low-cost system.

Technical Approach and Expected Deliverables

1) Review of the recent literature on wireless networks.

2) Correct and accurate software implementation of exploitation method(s)/algorithm(s).

3) Knowledge of the hardware requirement to build the detector.

4) Deliverables: real low-cost system exploitation of modem wireless links

Project # C14

Project Title: Drone detection and classification implementation using FPGA.

Professor(s) Name(s): 1. Omar Saad Aldayel
2. Sami Alhumaidi

Number of Students: Two to three

Students Qualifications

EE301, EE420, EE422 and MATLAB.

Statement of Problem/Brief Description of the Project

In this project, the student will apply their analytical and numerical knowledge to design a low cost and accurate drone detection system using FPGA. The system should be able to detect and identify drones and their locations with high accuracy. The first phase of this project (should take place in the first semester), will involve the modeling of micro-Doppler signature and Matlab simulations. In the second phase, the students should implement their system of a Digital Signal Processor (DSP) or any type circuit board/controller and evaluate the pros and cons of hardware options in term of cost, reliability, size and accuracy.

Objectives

(1) Study and understand the concept of array sensors and how the can be used to detect targets.
(2) Study and understand few detection methods/Algorithms in the literature, compare them and, if possible, improve or enhance their performance.
(3) Implement these method(s)/Algorithm(s) using MATALB and evaluate their performance in terms of accuracy, computational complexity, etc.

Implement the candidate method/algorithm on real low-cost system.

Technical Approach and Expected Deliverables

1) Review of the recent literature on radar and micro-Doppler.

2) Correct and accurate software implementation detection method(s)/algorithm(s).

3) Knowledge of the hardware requirement to build the detector.

4) Evaluation of the pros and cons of this prototype and how it compares to other prototypes in terms of cost, performance and complexity.

Project # C15

Project Title: Design and Implementation of Attestation-Based Security Mechanism for IoT and Cyber-Physical Systems

Professor(s) Name(s): Naif Almakhdhub

Number of Students: Two

Students Qualifications

Course work: EE353. Must be comfortable coding in C.
The students can be from the communication or electronics groups. Preferably have a good background in communication networks. Cybersecurity background is a plus.

Statement of Problem

Internet of Things (IoT) and Cyber-Physical Systems (CPS) are ubiquitous and are almost found in every domain. From smart-home (e.g., door lock) and healthcare (e.g., pacemaker) devices, to critical infrastructure (e.g., industrial controller, smart-meters, traffic lights). The number of deployed IoT/CPS devices has already exceeded billions and is expected to grow further in the future.

Many of these IoT and CPS devices are built using low-cost and constrained microcontroller-based systems. Unfortunately, such devices are becoming an attractive target for remote attacks as a result of their wide deployment and poor security posture. For example, attacks on IoT and CPS devices already caused power grid blackouts and large-scale Distributed Denial-of-Service (DDoS) attacks.

Compared to traditional systems, securing microcontroller systems is a challenging task since they lack essential resources that are needed enforce well-known security mechanisms. In addition, such systems can be deployed in geographically dispersed areas. Thus, detecting attacks and recovering a large scale of devices becomes a daunting task (e.g., manually recovering each device).

Brief Description of the Project

The goal of this project is to design and implement an attestation mechanism to improve the security posture of microcontroller systems. Attestation allows a remote entity (e.g., an administrator) to verify the integrity of the remote device (i.e., check if it is malware-infected or not). An additional (optional) goal is to design a mechanism to recover the device in case of an attack is detected.

Objectives

This project mainly focuses on a hand-on experience and implementation using a microcontroller board (e.g. STM32F769IDISCOVERY board). At the of this project you will:

(1) Be able to program an application, debug, and configure a microcontroller board.
(2) Gain an overall understanding of cybersecurity attacks and defenses for IoT/CPS systems.
(3) Design and implement the attestation mechanism on the selected application and board.

Technical Approach and Expected Deliverables

Phase 1

(1) Literature review and understanding of microcontroller systems and security challenges associated with them.
(2) Develop and implement a suitable microcontroller application to demonstrate the attestation mechanism.
(3) Develop a threat model and formulate the design of the attestation mechanism to tackle.
(4) Write the report of the first phase.

Phase 2

(1) Implement the attestation mechanism on the microcontroller board and developed application from phase 1.
(2) Collect the runtime and memory overhead of the proposed mechanism.
(3) Evaluate the security of the attestation mechanism.
(4) Update the final report with the results from phase2.

Expected Delivereable

A prototype of the attestation mechanism using the microcontroller board and a remote PC.

Project # C16

Project Title: 5G Fronthauling over Passive Optical Networks

Professor(s) Name(s): 1. Amr Ragheb 2. Ahmed Almaiman

Number of Students: Two

Students Qualifications

1- Knowledge of Digital Communication.
2- Knowledge of simulation tools such as Matlab.
3- Having skills in report writing and presentation.

Statement of Problem

Passive optical networks (PONs) are widely deployed around the world with fixed access service. PON architecture is a point to multipoint implemented as time or/and wavelength division multiplexing (i.e. TDM-, WDM-, and TDM over WDM-PON). On the other side, 5G new radio networks promise to provide 1000-fold system capacity and milliseconds end-to-end latency. This project aims to use and investigate the various PON features to transport 5G signals. This includes PON type, power budget analysis, data multiplexing, etc.

Brief Description of the Project

One direction of the advanced/new photonic technologies is the transmission of millimeter wave (MMW) signals over fiber channel. 5G fronthauling is a key design technology to transport MMW signals. In this project we will work to investigate the different type of widely deployed PON to transport 5G signals. This includes TDM, WDM, and TDM over WDM PON. Besides, two design issues will be considered in this project: (1) the power budget analysis and (2) the multiplexing of legacy PON data and MMW signals. Simulation design and experimental demonstration will be conducted to complete the work in this project.

Methodology

1. Conducting literature review about next generation-PON (NG-PON) standards and specifications,
2. Assessing the performance of 5G fronthauling over PON using simulation tools (i.e. Matlab, VPI, ..etc),
3. Investigating 5G fronthauling over PON using Experimental demonstration,
4. Evaluating the developed optical system using communication metrics (i.e. BER, EVM, Constellation…etc.).

Technical Approach and Expected Deliverables

Literature review and model programming will be conducted using KSU electronic library and Matlab/VPI software, respectively. Hardware implementation will be conducted using devices, equipment, and software available at RFTONICS CNL-lab.

Expected Deliverables

5G fronthaluing over PON test-bed.