Wireless And Mobile (WAM) Systems Lab http://wam.ece.ufl.edu
Director: Dr. Janise McNair

Available Position: Undergraduate Research Student
Topic: Securing and Protecting Smart Grids against Cyber Attacks using Software-Defined Networking (SDN)
PhD Student Supervisor: Dennis Agnew

Research overview: A smart grid is an electricity network enabling a two-way flow of electricity and data with digital communications technology enabling to detect, react and pro-act to changes in usage and multiple issues. Smart grids have self-healing capabilities and enable electricity customers to become active participants. In a NSF-supported project, we are developing a flexible distributed SDN topology for the application of sustainable Smart Grid Security. This project involves designing SDN networks that mimic and represents the communication seen on Smart Grid system (i.e. IEEE 118 bus system). SDN has many practical applications and is showing promising signs of widespread integration in current commercial fields (e.g. Google B4).

What are Software-Defined Networks? Software-Defined Networking (SDN) is a networking technique that communicates with underlying hardware infrastructure and directs traffic on a network using software-based controllers or application programming interfaces (APIs). Software-defined networking (SDN) is a newer network management architecture that separates the network control plane and data plane forwarding activities. Not only does the network controller keep track of data flow, but it also sets forwarding rules. Our research focuses on developing these SDN topologies using an open-source emulation tool, Mininet, in a virtual machine (VM) Linux environment. Within our VMs, we are able to launch cyber attacks against these networks such as Denial-of-Service (DoS), Botnet, Man-in-the-Middle (MiTM), False Data Injection (FDIA), etc. using tools such as Iperf, Hping3, dSniff, and Ettercap. Using the data collected from these attacks on our SDN frameworks, we are able to produce datasets for machine learning models that predict and classify attack types. With that information, we can levy the central control logic of SDN to quickly and efficiently mitigate attack instances.

Undergraduate Project. We are looking for an undergraduate student with coding experience, preferably with python. The project would consist of producing python scripts that use Mininet's APIs to generate custom SDN network topologies for testing different cyber attacks scenarios. In this position, the student will be exposed to Software Defined Networking and data generation for machine learning models and have the ability to further their programming experience. We are looking for someone interested in SDN, cyber attacks, and Smart Grids. There is a potential opportunity to continue participating in our work beyond the initial scope of this project.

Minimum Qualifications

- Experience in Python
- Basic understanding of programming and network devices
- Desire to learn more about Software-Defined Networking and Smart Grids

Responsibilities

(1) Attend all required meetings
    a. Project group meetings and WAM Systems Lab meetings*
    b. Individual meetings (with Dr. McNair or PhD student supervisor)
(2) Present progress reports and project updates at project group and lab meetings.
(3) Maintain and regularly check your gatorlink email
(4) Submit your reports to WAM Systems Lab MS Teams site, using your gatorlink access.

**Except when lab/individual meetings conflict with SURF scheduled meeting or exam times. Lab, individual and project meeting schedules will be determined at the beginning of the term.*