BIOGRAPHICAL SKETCH

A H M Jakaria has been pursuing his Ph.D. degree in Computer Science at Tennessee Tech University, USA since January 2016. He was actively involved with CEROC at Tennessee Tech as a graduate assistant. He received his BS in Computer Science and Engineering from Bangladesh University of Engineering and Technology, Dhaka in 2009. He earned his MS in Computer Science in 2019 from Tennessee Tech.

Jakaria's primary research area includes information and network security for NFV and SDN. He is also interested in resiliency issues in cyber-physical systems such as the SCADA network in Smart Grids, collaborative UAV networks, and IoT networks. He focuses on the formal modeling of the problems and solving them efficiently for automated synthesis of network topology and management strategies. Alongside his primary research in formal methods, he is also interested in Machine Learning-based analysis and security technologies for enterprise network systems.

EDUCATION

Ph.D. Engineering
Tennessee Tech University, 2016-2020 (expected)

M.S. Computer Science
Tennessee Tech University, 2016-2019

B.S. Computer Science & Engineering
Bangladesh University of Engineering & Technology, 2004-2009.

FUNDING ACKNOWLEDGEMENTS

I would like to acknowledge the Center for Energy Systems Research (CESR), Cybersecurity Education, Research and Outreach Center (CEROC), and the Department of Computer Science for their support.

College of Engineering

TENNESSEE TECH

The Department of

Computer Science

Announces the Dissertation Defense

A H M Jakaria

of

In Partial Fulfillment of the Requirements

For the degree of

Doctor of Philosophy in Engineering

April 3, 2020

3:00 pm

Held in

Prescott Hall 208

Tennessee Tech University

Zoom Link: https://tntech.zoom.us/j/709650056

FIELD OF STUDY

Computer Science

DISSERTATION TOPIC

Formal Techniques for Automated Design of Adaptive Networked Systems based on Security and Resiliency Requirements

EXAMINING COMMITTEE

Dr. Ambareen Siraj (Chairperson)

Dr. Mohammad Rahman

Dr. William Eberle

Dr. Sheikh Ghafoor

Dr. Mike Rogers

Dr. Mohamed Mahmoud

ABSTRACT

With the ever-growing need for connectivity in this era of smart and autonomous systems, we are observing an extensive use of network services. However, the increasing use of cyber technology leads to the proliferation of security threats. Therefore, it is very important to design a secure and resilient architecture for networked systems. Moreover, due to the diversified and dynamic nature of the emerging cyber usages as well as security requirements, adaptive and ad-hoc networking solutions are increasingly being adopted. While dynamic and adaptive networking provides many flexibilities, it requires to be properly (re)configured considering the changed context and dependability aspects. Organizations are seeking more reliable and automated design strategies that can meet the operational goals and security requirements within the budget and capability constraints, which is a multi-objective and combinatorially hard constraint satisfaction problem. This dissertation addresses this problem by proposing a suite of network synthesis techniques using formal methods which can automatically synthesize dependable networks satisfying the given requirements. This research considers three configuration synthesis problems that cover different security and resiliency perspectives of automated design of adaptive networked systems.

The first problem addresses the configuration synthesis for a network functions virtualization (NFV)-based network with respect to a security objective that requires the appropriate deployment of virtual machines (VMs) on physical servers. NFV, one of the fastest emerging topics in networking, reduces the limitations of vendor-specific proprietary hardware with the flexibility of virtual network architecture and the elasticity in handling various dynamic traffic patterns. The features of NFV can be utilized to build defense mechanisms against sophisticated cyberattacks such as DDoS by dynamically creating virtual network functions (VNFs) that can detect and prevent malicious traffic. NFV allows flexible and dynamic implementation of VNFs in virtual machines running on commercial-off-the-shelf (COTS) servers. However, allocating resources to these virtual machines is an NP-hard problem. The proposed solution to this problem determines the number and placement of the VMs hosted on COTS servers.

Secondly, we study the formal analysis for incremental deployment of software-defined networking (SDN), which is a closely related topic to NFV. We choose the context of security and resiliency of a smart grid system. The supervisory control and data acquisition (SCADA) network in a smart grid requires to be reliable and efficient to transmit the real-time data to the controller, especially when the system is under contingencies or cyberattacks. Introducing SDN into a SCADA network helps in deploying novel grid control operations as well as their secure and resilient management. As the overall smart grid network cannot be transformed to have only SDN-enabled devices overnight, a systematic deployment methodology is needed. We present a novel framework that can design a hybrid network consisting of both legacy forwarding devices and programmable SDN-enabled switches. The design satisfies the security and resiliency requirements of the SCADA network, which are specified with respect to a set of identified threat vectors. The SDN deployment plan primarily includes the best placements of the SDN-enabled switches (replacing the legacy switches). The plan may include one or more links to be installed newly to provide flexible or alternate routing paths.

The final problem is to design resilient communication for a collaborative network of the unmanned aerial vehicles (UAVs) which involves the planning of UAV trajectories. As the cost of UAVs is decreasing with novel technologies, other than military operations, their popularity is increasing rapidly in data collection for surveillance, disaster management, agriculture, and many more operations. The collected data are often time-sensitive and require to be transmitted to a data processing center. The collaborative nature of the UAVs also requires that they maintain proper communication with each other while in flight. However, planning the trajectory of a collaborative UAV swarm depends on multi-fold constraints in terms of communication requirements, data collection objectives, fuel outage and mid-air collision avoidance, UAV maneuvering capacity, and budget limitations. The collaborative UAVs, with respect to the mission objective, need to be resilient to the unavailability of one or more UAVs that can be caused due to cyberattacks or technical failures. It is required to create efficient spatio-temporal trajectories of the UAVs so that they can efficiently cover necessary data sources maintaining necessary communication infrastructure. We present a verification framework to determine the resiliency of the communication network among UAVs. The resiliency is determined in terms of the number of UAVs, which if malfunction, leave other UAVs in the network vulnerable.

To solve the above-mentioned problems, this research proposes to design and implement automated frameworks that formally model the system specifications, operator requirements, and budget and network constraints. The formal models are encoded and solved using efficient logic formulas based on satisfiability modulo theories (SMT). The solution to the model will synthesize the necessary network configuration parameters. We also present simulated experiments to demonstrate the scalability and usability of the proposed solutions.