STEVENS
INSTITUTE OF TECHNOLOGY
1870

Ph.D. DISSERTATION DEFENSE

Candidate:	Fan Yang
Degree:	Doctor of Philosophy
School/Department:	Department of Electrical & Computer Engineering
Date:	Tuesday, July 30th, 2024
Time/Location:	11:00 a.m./ https://stevens.zoom.us/j/98381298872
Title:	Resource Allocation and Privacy for Next-generation Wireless Ad hoc Networks
Chairperson:	Dr. Cristina Comaniciu, Department of Electrical & Computer Engineering
Committee Members:	Dr. Yu-Dong Yao, Department of Electrical & Computer Engineering Dr. Koduvayur Subbalakshmi, Department of Electrical & Computer Engineering Dr. Yu Gan, Department of Biomedical Engineering

ABSTRACT

Efficient resource utilization and privacy assurance are essential for enabling secure and high-performance ad hoc network deployments for both military and civilian applications. This dissertation addresses these challenges through the development of innovative game-theoretic, adversarial machine learning, and federated learning approaches.

The first part of the thesis addresses the problem of designing distributed mission slice allocation and management in tactical ad hoc networks, optimizing jointly the resource allocation and privacy. The solution is based on a novel game theoretic framework that formulates the slice allocation problem as a multi-agent non-cooperative game. In this game, Application Slice Agents (ASAs) compete for shared computational and bandwidth resources, maximizing an utility function that captures network connectivity, energy and computational constraints, and security. The framework allows for a dynamic self-configuration of slices, quantifying security-efficiency tradeoffs based on a model that capture timing side-channel leak mitigation.

In the second part of the thesis, I focus on the timing side-channel leak mitigation, proposing a fast and efficient method for traffic obfuscation using adversarial machine learning. This work addresses the vulnerability of encrypted traffic to pattern analysis, which can reveal sensitive information about the type of traffic in the network. My proposed deep neural network model, generates tailored manipulations for traffic features to obfuscate adversaries, overcoming the limitations of previous padding and impersonation techniques. The novel solution I proposed achieves higher obfuscation success rates with significantly reduced computational overhead compared to existing adversarial learning methods, demonstrating a 3000-fold improvement in processing speed.

The final part of the thesis integrates concepts from the previous two studies to address challenges of implementing collaborative intrusion detection across heterogeneous edge devices in an ad hoc network. A multi-armed bandwidth model is fitted to solve a joint optimization for resource allocation and privacy for a federated learning framework. My novel solution dynamically adjust the computational resources allocated for heterogeneous edge devices to enforce an optimal adaptive data selection across the nodes based on the quality of the model, essentially accelerating training, minimizing latency and increasing model accuracy, while preserving data privacy in federated learning environments.