STEVENS
INSTITUTE OF TECHNOLOGY
1870

Ph.D. DISSERTATION DEFENSE

Candidate:	Jingda Yang
Degree:	Doctor of Philosophy
School/Department:	Charles V. Schaefer, Jr. School of Engineering and Science / Department of Systems and Enterprises
Date:	Thursday, July 24th, 2025
Time/Location:	2:00 p.m. / Babbio Center Room 503
Title:	Autonomous NextG System Vulnerability Detection from Protocol Verification to Runtime Validation
Chairperson:	Dr. Ying Wang, Department of Systems and Enterprises, School of Engineering & Science
Committee Members:	Dr. Dinesh Verma, Department of Systems & Enterprises, School of Engineering & Science Dr. Lu Xiao, Department of Systems & Enterprises, School of Engineering & Science Dr. Dave Naumann, Department of Computer Science, School of Engineering & Science Dr. Shucheng Yu, Department of Electrical & Computer Engineering, School of Engineering & Science

ABSTRACT

Vulnerability detection is crucial for defending against cyber threats and protecting wireless communication systems. Despite advancements in robust detection methods, such as machine learning and scalable cloud-based vulnerability detection, existing approaches to automatic vulnerability detection still have several limitations: the lack of fully automated protocol-based vulnerability detection, heavy dependence on computational resources for detecting implementation vulnerabilities, and the inability to update learned attack patterns during runtime.

This proposal aims to develop an advanced vulnerability detection system capable of automatically verifying protocols through formal verification, efficiently validating security in implementations based on formal results, and updating learned patterns during runtime for improved attack prediction. To achieve this goal, we have undertaken three preliminary works. First, to automatically detect formal vulnerabilities in protocols, we proposed a pre-trained large language model-based formal properties extractor. This tool translates protocols into formats suitable for formal verification, achieving over 95% accuracy in classification results on the 3GPP RRC protocol, which ensures the integrity and effectiveness of the protocol analysis and formal verification processes. Secondly, to efficiently identify high-risk vulnerabilities, we introduced a formal-guided fuzz testing framework to detect vulnerabilities on a digital twin platform. Finally, we introduced a probability-based strategy that effectively transforms the growth of time consumption from exponential to linear, significantly reducing the heavy load of computational resources.

To complete our fully automatic vulnerability detection system, we further propose future work in the following two areas: Firstly, we aim to develop a reasoning transformer model, which encodes text to graph

and decodes the graph to text. Through encoded graph, we can visualize the reasoning process and introduce the domain knowledge with knowledge graph. Secondly, we plan to implement a dynamic model that not only detects vulnerabilities based on learned features and patterns during runtime but also updates its dataset with information from zero-day attacks, ensuring continuous refinement of its detection capabilities. Through the strategic integration of feedback loops within its operational framework, the proposed system not only ensures the precise identification of formal properties but also continuously enhances its capability to recognize and address specific vulnerability features and patterns.