Proceedings of the Singapore Scientific Conference – Forging a Sustainable Future Through Science & Technology

doi: 10.3850/081125_SSC2025_OR-02-0378

SSC2025

SSC2025 Category/Theme:: Environment — Shaping a Resilient Planet

A Scalable Framework for Security Monitoring and Vulnerability Assessment in Smart Cities

Heng Chuan Tan[1], Zbigniew Kalbarczyk[1,2], David M. Nicol[1,2]
[1] Illinois Advanced Research Science Center at Singapore, Singapore
[2] Department of Electrical and Computer Engineering, University of Illinois at Urbana-Champaign, USA

Keywords: Cyber-Security, System Security, Vulnerability Assessment, Critical Node Identification

BACKGROUND AND MOTIVATION

Smart cities are vulnerable to cyber threats due to shared infrastructure, heterogeneous networks, and increasing connectivity. While current security solutions can detect vulnerabilities, they often lack the scalability to analyze coordinated attacks across large, interconnected systems. Furthermore, addressing and patching every vulnerability is impractical given the scale of smart cities and the limited resources available. To overcome these challenges, we propose a security monitoring framework that combines graph-based vulnerability analysis and attack path modeling so that system operators can prioritize vulnerabilities and defense strategies more effectively.

OUR FRAMEWORK

Our framework consists of three key components: a security monitoring platform, a Temporal Graph Convolutional Network (T-GCN), and an attack graph generator. The monitoring platform, which supports a wide range of protocol parsers, uses Zeek [1], Prometheus, and Grafana pipeline to monitor and visualize the network traffic for vulnerabilities. To support monitoring at scale, the monitoring platform can be deployed in a distributed manner to analyze the traffic jointly. The T-GCN model is a deep learning model that integrates graph convolutional networks with temporal sequence learning [2]. It is designed to capture both the structural dependencies (i.e., how devices are connected in a network) and the temporal dynamics (i.e., how traffic patterns evolve). Using this model, our framework predicts node criticality by analyzing traffic patterns and connectivity across the smart city network. High criticality scores indicate that nodes are highly reachable and therefore more attractive to attackers. Consequently, our framework guides system operators to concentrate their defense efforts on those nodes. Finally, the attack graph generator, built on and extended from the MulVAL framework [3], models how an attacker might exploit vulnerabilities across interconnected systems to reach the critical nodes. These attack paths allow operators to reason about the reachability of attack goals, understand possible exploitation scenarios, and design targeted defense strategies before the attack propagates.

EVALUATION

We validated our framework using real-world datasets from the CREATE Tower building management system, an environment similar to a smart city. The evaluation demonstrated the framework's effectiveness in providing real-time insights into system connectivity, protocol-level behavior, and vulnerability exposure. The T-GCN model not only identified critical nodes for preventive actions but also detected shifts in node rankings over time, enabling system operators to investigate whether such changes are due to system upgrades, device reconfigurations, or cyberattacks so that proactive measures can be taken to mitigate the associated risks. Furthermore, the attack graph tool revealed how vulnerabilities could be exploited, pinpointing weak points in the network that require attention and underscoring the importance of developing targeted defense strategies to protect against multi-stage attacks.

CONCLUSION

Our framework enhances vulnerability assessment beyond traditional CVSS-based scoring by incorporating node connectivity and traffic patterns to determine criticality. This approach provides actionable insights that help system operators prioritize limited resources and defense strategies more effectively, laying the foundation for scalable security monitoring in smart city environments.

REFERENCES

[1] Paxson, V. (1999). Bro: a system for detecting network intruders in real-time. *Computer networks*, *31*(23-24), 2435-2463.
[2] Zhao, L., Song, Y., Zhang, C., Liu, Y., Wang, P., Lin, T., ... & Li, H. (2019). T-GCN: A temporal graph convolutional network for traffic prediction. *IEEE transactions on intelligent transportation systems*, *21*(9), 3848-3858.
[3] Ou, Xinming, Sudhakar Govindavajhala, and Andrew W. Appel. "MulVAL: A logic-based network security analyzer." In *USENIX security symposium*, vol. 8, pp. 113-128. 2005.
[4] iTrust Testbeds, https://itrust.sutd.edu.sg/itrust-labs_overview/ Accessed [Sept-20