Proceedings of the 2024 Winter Simulation Conference
H. Lam, E. Azar, D. Batur, S. Gao, W. Xie, S. R. Hunter, and M. D. Rossetti, eds.

SIMULATING CYBERATTACKS AND DEFENSE MECHANISMS AGAINST EMERGENCY VEHICLE PREEMPTION SYSTEMS

Dalal Alharthi[1] and Montasir Abbas[2]

[1]Dept. of Cyber, Intelligence, and Information Operations, University of Arizona, Tucson, AZ, USA
[2]Dept. of Civil and Environmental Eng., Virginia Tech, Blacksburg, VA, USA

ABSTRACT

There are more than 320,000 traffic signals in the US. A significant number of these signals are equipped with emergency vehicle preemption (EVP) systems, where each emergency vehicle (EV) interrupts pre-designed signal operation plans. Recently, the difficulty of configuring EVP operations has been exacerbated by the potential for cybersecurity attacks that can spoof EVP calls or prevent actual calls from reaching the traffic controllers. It is, therefore, critically important to develop robust and efficient EVP systems that can detect cybersecurity attacks and operate the EVP system safely and optimally. This work uses a digital twin of a transportation network to simulate the EVP operation and identify system vulnerabilities and remediation techniques using the AnyLogic agent-based simulation platform. We simulate cyberattacks for both normal traffic and connected automated vehicles (CAVs) scenarios and propose a novel application of Zero-Trust Architecture (ZTA) to enhance the security of the EVP system.

1 INTRODUCTION

A significant number of traffic signals are equipped with emergency vehicle preemption (EVP) systems, where each emergency vehicle (EV) interrupts pre-designed signal operation plans. EVP can be a potential target for cybersecurity attacks that can spoof EVP calls or prevent actual calls from reaching the traffic controllers. Cyberattacks can occur in various forms, including malware attacks, Distributed Denial of Service (DDoS) attacks, physical tampering, Man-in-the-middle (MitM) attacks, exploitation of vulnerabilities, command injections, and GPS spoofing (Anderson et al. 2023). Previous research proposed the development of a comprehensive incident response runbook designed to systematically document and guide the response to each specific attack scenario. The runbook may follow the incident response phases outlined by the National Institute of Standards and Technology (NIST), which are (1) preparation, (2) detection and analysis, (3) containment, eradication, and recovery, and (4) post-incident activities (Alharthi et al. 2020; Alharthi 2023; Alharthi and Regan 2021). Robust defense mechanisms are necessary to protect EVs from these cyber threats. In this paper, we simulate a ZTA policy implementation to defend against EVP-targeted cyberattacks. ZTA was first proposed by NIST in 2020 (Kang et al. 2023). Recently, organizations started using the ZTA, operating on the principle that no entity, whether inside or outside the network perimeter, should be automatically trusted (Teerakanok et al. 2021).

2 DETERMINATION OF ZTA POLICY WITH RL

Our proposed ZTA algorithm utilizes a Reinforcement Learning (RL) algorithm that learns from its experience dealing with EV calls and whether it made the correct decision in previous iterations. In this framework, the RL agent acts as a Policy Decision Point (PDP), dynamically refining rules to assess whether an EV preemption request is trustworthy to mitigate the risk of spoofed calls. A ZTA controller agent will sense the state of the system in relation to the surrounding traffic characteristics. The agent will use its internal policy to determine an appropriate action, such as recognizing the EV call as a legitimate call and initiating a preemption sequence or ignoring the EV call as a spoofed call. The EV will be traced down the preemption path using the controller's sensing system. As the EV exits the system, the controller

will receive information about its travel trajectory and speed on each road segment. The speed information is compared and evaluated for accuracy to provide the controller with a final assessment on whether the EV was legitimate or spoofed (a spoofed EV might disappear along the path or have a non-reasonable speed trajectory variation). The difference between the recognized status of the EV as it approaches the intersection and as it leaves the system is used as a reward value that the controller will use to adjust its ZTA policy. The agent will incorporate this state-action-reward sequence in its RL technique by explicitly defining a structure of rules that guide an agent from every state to the optimal action. This learning process involves two steps: (1) a mapping from any given state to a known action and (2) a probability of the next state given the previous state-action combination and the new ZTA agent's rules.

3 DIGITAL TWIN DEVELOPMENT

The digital twin developed in this research includes a simulation component and an optimizer (OptQuest) in the background. The simulation module uses the optimization input and initial parameters to run the simulation. The average system travel time was used as an objective function output from each simulation run. The preemption (PE) parameters were adjusted by the optimizer and fed into each new simulation iteration. The optimization stops when no better solution can be found within a certain number of iterations. The digital twin consisted of the infrastructure component with three controllers that are capable of running EVP. The base case included EVs entering the system with a 15 EV/hour rate. This phase established a baseline for system performance and behavior under standard EV preemption conditions. The experiment was set up by configuring three scenarios: (1) DDoS attack with Normal Traffic Stream, (2) DDoS attack with CAV Traffic Stream, and (3) ZTA Policy. All scenarios were simulated under consistent DDoS attack conditions, with 800 spoofed EV calls per hour. The results of running the DDoS attack with a normal traffic case scenario show that the system got so congested that only 326 vehicles were able to go through the system. The scenario for DDoS with CAVs shows that the system was bogged down even more, with only 266 total vehicles making it through the system due to continuous preemption calls and the extra spaces that real vehicles are making on the road for the spoofed EVs. Finally, the results of running the disaster response plan show that 1459 vehicles could now clear the system. The average vehicle time in the system was about 3 minutes (176 seconds). This clearly shows the benefit of the ZTA policy in terms of maximizing network throughput.

4 CONCLUSIONS

This paper presents a novel simulation of a Zero-Trust Architecture policy to mitigate the risk of DDoS attacks against transportation systems. The paper presented a methodology that used a digital twin that can be used to evaluate, assess, and provide guidelines for using robust and efficient cybersecurity algorithms that can lead to optimal EVP control. The digital twin was used to simulate the EVP operation and identify system vulnerabilities using the AnyLogic agent-based simulation platform. We simulated three traffic scenarios and emulated the impact of activating a ZTA policy. The results showed that the vehicle time in the system for the disaster response plan resulted in a very significant increase in vehicle throughput.

REFERENCES

Anderson, J., Q. Huang, L. Cheng, and H. Hu. 2023. "A Zero-Trust Architecture for Connected and Autonomous Vehicles". *IEEE Internet Computing* 27(5): 7–14.

Alharthi, D. N., M. M. Hammad, and A. C. Regan. 2020. "A Taxonomy of Social Engineering Defense Mechanisms". In *Advances in Information and Communication: Proceedings of the 2020 Future of Information and Communication Conference (FICC)* 2:27–41.

Alharthi, D. 2023. "Secure Cloud Migration Strategy (SCMS): A Safe Journey to the Cloud".

Alharthi, D., and A. Regan. 2021. "A Literature Survey and Analysis on Social Engineering Defense Mechanisms and InfoSec Policies". *International Journal of Network Security & Its Applications* 13(2): 41-61.

Kang, H., G. Liu, Q. Wang, L. Meng, and J. Liu. 2023. "Theory and Application of Zero Trust Security: A Brief Survey". *Entropy* 25, 1595.

Teerakanok, S., T. Uehara, and A. Inomata. 2021. "Migrating to Zero Trust Architecture: Reviews and Challenges". *Security and Communication Networks* 2021:1–10.