Dataset Exploration and Literature Review on the CIC EV Charger Attack Dataset 2024 (CICEVSE2024)

Omar Ahmed Mohamed Hanafy Mahmoud (220304141)
Fenerbahçe University

Abstract

The rapid growth of Electric Vehicle (EV) infrastructure introduces new cybersecurity threats targeting EV chargers and Vehicle-to-Grid (V2G) systems. The CIC EV Charger Attack Dataset 2024 (CICEVSE2024) provides a comprehensive collection of benign and malicious traffic designed to support the development of machine learning–based intrusion detection systems.

1. Introduction

Electric Vehicle charging stations are critical components of modern smart-grid infrastructure but are vulnerable to cyberattacks. This report explores the selected dataset and reviews related literature.

2. Dataset Overview

The CIC EV Charger Attack Dataset 2024 was developed by the Canadian Institute for Cybersecurity (CIC) to support machine learning research for EV charging security.

3. Feature Description

The dataset includes network traffic features such as timestamps, IP addresses, ports, protocol types, packet lengths, charging parameters, and attack labels.

4. Literature Review

Existing studies apply machine learning models such as Random Forests, Support Vector Machines, and Deep Neural Networks to detect EV charging attacks.

5. Conclusion

This phase explored the dataset and surveyed existing research, forming the foundation for model development in Phase 2.

References

[1] R. Gautham et al., IEEE Access, 2023.
[2] M. Hussain et al., IEEE Transactions on Smart Grid, 2022.
[3] K. Parmar et al., IEEE IoT Journal, 2024.

[4] Canadian Institute for Cybersecurity, 2024.