PHÁT HIỆN TẤN CÔNG IOT TRÊN XE ĐIỆN BẰNG AECR-ML

Nguyễn Hữu Tài - 240101068

Tóm tắt

- Lớp: CS2205.FEB2025
- Link Github: https://github.com/tta602/CS2205.FEB2025-AECR-ML.git
- Link YouTube video: https://youtu.be/KztXwyXLJSE
- Nguyễn Hữu Tài - 240101068

Giới thiệu

- Xe điện (EV) với IoT tích hợp đang định hình tương lai giao thông.
- Tuy nhiên, tồn tại nguy cơ tấn công mạng tinh vi:
  - Giả mạo dữ liệu cảm biến
  - Chiếm quyền điều khiển hệ thống
  - Gây gián đoạn hoạt động
- Rủi ro nghiêm trọng đến an toàn giao thông

Hướng tiếp cận của đề tài

- Phát triển mô hình học máy phát hiện tấn công
- Tích hợp với mô hình AECR: trích xuất thông tin tấn công từ báo cáo CTI
- Mô hình được kiểm chứng trong môi trường mô phỏng

Mục tiêu

- Đánh giá rủi ro bảo mật của thiết bị IoT trên xe điện
- Phát triển mô hình học máy phát hiện hành vi bất thường từ dữ liệu cảm biến
- Đề xuất và triển khai hệ thống bảo mật IoT, kiểm thử hiệu quả thực tế

Nội dung và Phương pháp

- Khảo sát và phân tích
  - Phân tích các kiểu tấn công IoT trên EV (MITM, DoS, giả mạo cảm biến)
  - Nghiên cứu mô hình AECR trích xuất thông tin tấn công từ báo cáo CTI
  - Phân tích dữ liệu cảm biến (tốc độ, GPS, môi trường)
- Xây dựng mô hình phát hiện tấn công
  - Áp dụng ML/DL (RF, SVM, DNN)
  - Kết hợp dữ liệu cảm biến và thông tin CTI

Nội dung và Phương pháp

- Triển khai mô hình mô phỏng
  - Mô phỏng EV-IoT với Raspberry Pi, Arduino
  - Tái hiện các tình huống tấn công
- Đánh giá và tối ưu
  - Đo độ chính xác, hiệu suất mô hình
  - Kiểm tra khả năng mở rộng và ứng dụng thực tế

Kết quả dự kiến

- Mô hình phát hiện bất thường chính xác cao
- Triển khai giải pháp bảo mật IoT trên nền tảng mô phỏng thực tế
- Báo cáo đánh giá hiệu quả trước các kịch bản tấn công
- Đề xuất phương pháp nâng cao khả năng bảo vệ và tối ưu hóa hệ thống

Tài liệu tham khảo

[1] Minghao Chen, Kaijie Zhu, Bin Lu, Ding Li, Qingjun Yuan, Yuefei Zhu.
AECR: Automatic attack technique intelligence extraction based on fine-tuned large language model. Computers & Security, 150:104213, 2025.
[2] Nirav Doshi, Rakesh M. Verma, Liang Cheng.
Security analysis of IoT protocols in electric vehicles: A survey. IEEE Access, 10:62133–62151, 2022.
[3] Ali Alqahtani, Mohamed Amine Ferrag, Leandros Maglaras, Helge Janicke.
Detecting DoS attacks in IoT environments using deep learning models. Journal of Information Security and Applications, 55, 2020.
[4] Tariq Alshammari, Andrew Nix.
Analysis of WiFi and Bluetooth attacks against EV-based IoT networks. Ad Hoc Networks, 123, 2021.
[5] Yong Yu, Min Chen, Yiqiao He, Yunjie Ge, Kecheng Liu.
Anomaly detection for IoT time series based on sliding-window GAN. Future Generation Computer Systems, 131:297–312, 2022.