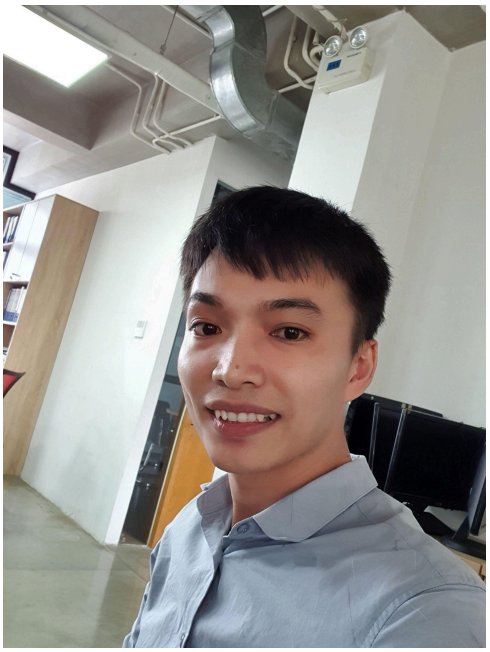
THÔNG TIN CHUNG CỦA NHÓM

- Link YouTube video của báo cáo (tối đa 5 phút): *https://youtu.be/KztXwyXLJSE*
- Link slides (dạng .pdf đặt trên Github của nhóm): *https://github.com/tta602/CS2205.FEB2025-AECR-ML.git*
- *Mỗi thành viên của nhóm điền thông tin vào một dòng theo mẫu bên dưới*
- *Sau đó điền vào Đề cương nghiên cứu (tối đa 5 trang), rồi chọn Turn in*
- *Lớp Cao học, mỗi nhóm một thành viên*

- Họ và Tên: Nguyễn Hữu Tài
- MSSV: 240101068



- Lớp: CS2205.FEB2025
- Tự đánh giá (điểm tổng kết môn): 8.0/10
- Số buổi vắng: 0
- Số câu hỏi QT cá nhân: 4
- Số câu hỏi QT của cả nhóm: 4
- Link Github: https://github.com/mynameuit/CS2205.xxx/

ĐỀ CƯƠNG NGHIÊN CỨU

TÊN ĐỀ TÀI (IN HOA)

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

TÊN ĐỀ TÀI TIẾNG ANH (IN HOA)

AECR-ML FOR IOT ATTACK DETECTION IN EVS

TÓM TẮT *(Tối đa 400 từ)*

Sự phát triển của xe điện (EV) cùng với việc tích hợp IoT đã tạo ra nhiều tiện ích nhưng cũng tiềm ẩn rủi ro bảo mật nghiêm trọng, đặc biệt là các cuộc tấn công mạng nhằm vào hệ thống cảm biến, có thể gây ra hậu quả lớn. Nhằm giải quyết thách thức này, nghiên cứu đề xuất một mô hình phát hiện hành vi bất thường và tấn công mạng, nâng cao an ninh cho hệ thống IoT trên xe điện. Đề tài tập trung vào bốn nội dung chính. Đầu tiên, khảo sát và phân tích các kỹ thuật tấn công phổ biến (Man-in-the-Middle, giả mạo dữ liệu, DoS) cùng các hệ thống bảo mật hiện có. Thứ hai, đề xuất mô hình phát hiện tấn công bằng cách kết hợp các thuật toán học máy (Random Forest, SVM, Deep Learning) với mô hình AECR – một hệ thống sử dụng mô hình ngôn ngữ lớn để trích xuất thông tin tình báo kỹ thuật tấn công từ báo cáo CTI. Thứ ba, triển khai môi trường thử nghiệm với các nền tảng như Raspberry Pi và Arduino để kiểm thử mô hình trong các kịch bản tấn công giả lập. Cuối cùng, đánh giá hiệu quả của mô hình dựa trên các tiêu chí: độ chính xác, hiệu suất xử lý và khả năng mở rộng. Kết quả kỳ vọng bao gồm mô hình phát hiện bất thường có độ chính xác cao, hệ thống giám sát bảo mật được triển khai trên nền tảng mô phỏng, và phân tích so sánh hiệu quả với các giải pháp bảo mật truyền thống. Đề tài góp phần vào việc nâng cao an toàn thông tin trong hệ sinh thái xe điện – một lĩnh vực ngày càng quan trọng trong kỷ nguyên giao thông thông minh.

GIỚI THIỆU *(Tối đa 1 trang A4)*

Xe điện (EV) và hệ thống IoT tích hợp đang định hình tương lai giao thông, nhưng đồng thời đối mặt với các nguy cơ tấn công mạng tinh vi. Các lỗ hổng bảo mật trong

IoT trên EV có thể bị khai thác để giả mạo dữ liệu, chiếm quyền điều khiển, hoặc gây gián đoạn hoạt động, dẫn đến rủi ro nghiêm trọng về an toàn. Nhằm giải quyết thách thức này, nghiên cứu tập trung phát triển một mô hình phát hiện hành vi bất thường và tấn công mạng cho hệ thống IoT trên xe điện. Điểm đột phá là sự kết hợp giữa các thuật toán học máy tiên tiến và mô hình AECR – một hệ thống sử dụng ngôn ngữ tự nhiên để tự động trích xuất thông tin tình báo kỹ thuật tấn công từ các báo cáo CTI. Cách tiếp cận này giúp hệ thống phản ứng nhanh với mối đe dọa mới và xây dựng cơ sở tri thức phòng thủ. Đề tài không chỉ đặt trọng tâm vào việc xây dựng mô hình lý thuyết mà còn hướng tới triển khai thực nghiệm trong môi trường mô phỏng, nhằm kiểm chứng tính khả thi và hiệu quả trong thực tế. Đầu vào của đề tài bao gồm dữ liệu cảm biến và thông tin từ các báo cáo CTI, trong khi đầu ra là mô hình phát hiện bất thường và hệ thống bảo mật tích hợp cho IoT trên xe điện. Những kết quả này kỳ vọng sẽ đóng góp vào xu hướng phát triển giao thông thông minh và an toàn trong tương lai gần.

MỤC TIÊU *(Viết trong vòng 3 mục tiêu)*

- Đánh giá rủi ro bảo mật của các thiết bị IoT trên xe điện.
- Phát triển mô hình học máy để phát hiện hành vi bất thường và tấn công mạng dựa trên dữ liệu cảm biến.
- Đề xuất và triển khai giải pháp bảo vệ thiết bị IoT trên xe điện, kiểm thử hiệu quả bảo mật của hệ thống.

NỘI DUNG VÀ PHƯƠNG PHÁP

1. Khảo sát và phân tích:

- **Tìm hiểu các mô hình tấn công:** Phân tích các kỹ thuật tấn công phổ biến đối với thiết bị IoT trên xe điện như tấn công Man-in-the-Middle, tấn công giả mạo cảm biến, và tấn công DoS.
- **Đánh giá hệ thống hiện có:** Khảo sát các giải pháp bảo mật hiện nay đang được áp dụng trên hệ thống IoT của xe điện.
- **Phân tích dữ liệu cảm biến:** Thu thập và phân tích dữ liệu từ các cảm biến phổ biến như cảm biến tốc độ, định vị, môi trường (CO2, PM2.5).
- **Khảo sát mô hình AECR:** Nghiên cứu cách thức AECR tự động trích xuất

thông tin kỹ thuật tấn công từ các báo cáo CTI.

2. Đề xuất giải pháp bảo mật:

- **Phát triển mô hình phát hiện bất thường:**
  - Sử dụng mô hình học máy (Random Forest, SVM, Deep Learning) để phân tích và nhận diện bất thường từ dữ liệu cảm biến.
  - Áp dụng AECR để trích xuất các dấu hiệu tấn công từ các báo cáo tình báo mối đe dọa mạng.
- **Xây dựng hệ thống giám sát:**
  - Tích hợp mô hình phát hiện vào hệ thống giám sát mạng IoT của xe điện.
  - Xác định các thông số quan trọng để giám sát như độ lệch chuẩn, tốc độ truyền dữ liệu, và độ tin cậy của cảm biến.
- **Kỹ thuật mã hóa:**
  - Triển khai mã hóa dữ liệu và xác thực để đảm bảo an toàn trong quá trình truyền tải.
- **Bảo vệ giao thức truyền thông:**
  - Nâng cao bảo mật cho các giao thức như CAN, MQTT để tránh bị tấn công.

3. Triển khai mô hình thử nghiệm:

- **Thiết lập môi trường giả lập:**
  - Xây dựng hệ thống mô phỏng giao tiếp IoT trên xe điện.
  - Sử dụng các nền tảng như Raspberry Pi, Arduino để giả lập các cảm biến.
- **Kiểm tra và đánh giá:**
  - Đưa mô hình vào thử nghiệm với các tình huống tấn công như xâm nhập và DoS.
  - Đo lường độ chính xác của mô hình trong việc phát hiện các bất thường.
- **Tích hợp với hệ thống thực:**
  - Kết nối mô hình vào hệ thống thực để đánh giá tính khả thi và hiệu quả bảo mật.

4. Đánh giá:

- **Hiệu quả phát hiện tấn công:**
  - Đo lường độ chính xác, độ nhạy và độ đặc hiệu của mô hình phát hiện bất thường**.**
- **Hiệu suất hệ thống:**

    - Kiểm tra tốc độ xử lý dữ liệu trong các kịch bản tấn công.
- **Khả năng mở rộng:**
    - Đánh giá khả năng áp dụng trên nhiều loại cảm biến và nền tảng khác nhau.
- **Phân tích hiệu quả giải pháp bảo mật:**
    - So sánh với các mô hình bảo mật truyền thống và các phương pháp phát hiện tấn công khác.

KẾT QUẢ MONG ĐỢI

Nghiên cứu hướng tới xây dựng mô hình phát hiện bất thường cho xe điện với độ chính xác cao, đồng thời triển khai giải pháp bảo mật IoT trên nền tảng mô phỏng để kiểm chứng thực tế. Kết quả bao gồm báo cáo kiểm thử các tình huống tấn công, đánh giá hiệu quả bảo vệ và đề xuất cải tiến nhằm nâng cao tính ứng dụng trong tương lai.

TÀI LIỆU THAM KHẢO *(Định dạng DBLP)*

[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.