TRƯỜNG ĐẠI HỌC SÀI GÒN
KHOA CÔNG NGHỆ THÔNG TIN

ĐỀ CƯƠNG PHƯƠNG PHÁP NGHIÊN CỨU KHOA HỌC

ĐỀ TÀI:

Cải thiện hiệu suất phát hiện tấn công thông qua lựa chọn đặc trưng và so sánh mô hình trên dữ liệu RT-IoT2022

Giảng viên hướng dẫn:

TS. Đỗ Như Tài

Sinh viên thực hiện:

Tạ Hồng Quí
MSSV: 3122410348

Tháng 05 - 2025

Mục lục

Danh sách bảng

Danh sách hình vẽ

I Lý do chọn đề tài

Hiện nay, việc một hệ thống bị tấn công thông qua không gian mạng ngày càng phổ biến. Chúng ta thường phát hiện ra hệ thống của mình bị tấn công khi các thiết bị quá tải hoặc sập, do đó việc phát hiện và ngăn chặn các cuộc tấn công trước khi xảy ra là một điều vô cùng cấp thiết. Trong bối cảnh các hệ thống phát hiện và phân tích dữ liệu thời gian thực ngày càng đóng vai trò quan trọng trong các ứng dụng như an ninh mạng, giám sát giao thông và quản lý hệ thống công nghiệp, việc tối ưu hóa hiệu suất của các mô hình máy học trở thành một yêu cầu cấp thiết. Tập dữ liệu RT-IoT 2022[1] (Real Time Internet Of Things 2022), với đặc điểm phức tạp và đa dạng, cung cấp một cơ hội lý tưởng để nghiên cứu và cải thiện các phương pháp phát hiện dựa trên dữ liệu thời gian thực. Tuy nhiên, khối lượng đặc trưng lớn và sự dư thừa thông tin trong tập dữ liệu này có thể làm giảm hiệu suất của các mô hình, đồng thời tăng chi phí tính toán.

Lựa chọn đặc trưng là một bước quan trọng nhằm loại bỏ các đặc trưng không liên quan hoặc dư thừa, từ đó cải thiện độ chính xác và hiệu quả của mô hình. Bên cạnh đó, việc so sánh các mô hình máy học khác nhau giúp xác định phương pháp phù hợp nhất cho từng kịch bản cụ thể, đặc biệt khi xử lý dữ liệu thời gian thực với các yêu cầu nghiêm ngặt về tốc độ và độ chính xác. Do đó, nghiên cứu này được thực hiện nhằm khám phá, tìm ra các đặc trưng quan trọng và so sánh mô hình để nâng cao hiệu suất phát hiện trên tập dữ liệu RT-IoT2022 [1], góp phần cung cấp các giải pháp hiệu quả cho các ứng dụng thực tiễn.

II Tổng quan quan vấn đề nghiên cứu.

1 Tình hình nghiên cứu hiện tại:

Trong những năm gần đây, các hệ thống phát hiện dựa trên dữ liệu thời gian thực đã trở thành một lĩnh vực nghiên cứu sôi nổi, với các ứng dụng trải rộng từ an ninh mạng, giám sát công nghiệp đến quản lý giao thông thông minh.RT-IoT2022, một tập dữ liệu độc quyền có nguồn gốc từ cơ sở hạ tầng IoT thời gian thực, được giới thiệu như một nguồn tài nguyên toàn diện tích hợp nhiều loại thiết bị IoT và phương pháp tấn công mạng tinh vi. Tập dữ liệu này bao gồm cả hành vi mạng bình thường và đối kháng, cung cấp một biểu diễn chung về các tình huống trong thế giới thực. Kết hợp dữ liệu từ các thiết bị IoT như ThingSpeak-LED, Wipro-Bulb và MQTT-Temp, cũng như các tình huống tấn công mô phỏng liên quan đến các cuộc tấn công Brute-Force SSH, các cuộc tấn công DDoS sử dụng Hping và Slowloris và các mẫu Nmap, RT-IoT2022 cung cấp một góc nhìn chi tiết về bản chất phức tạp của lưu lượng mạng. Các thuộc tính hai chiều của lưu lượng mạng được ghi lại một cách tỉ mỉ bằng công cụ giám sát mạng Zeek và plugin Flowmeter. Các nhà nghiên cứu có thể tận dụng tập dữ liệu RT-IoT2022 để nâng cao khả năng của Hệ

thống phát hiện xâm nhập (IDS), thúc đẩy sự phát triển của các giải pháp bảo mật mạnh mẽ và thích ứng cho các mạng IoT thời gian thực [1]. Bộ đã thu hút sự chú ý nhờ tính đa dạng và phức tạp, phản ánh các thách thức trong môi trường thực tế. Nhiều nghiên cứu đã tập trung vào việc áp dụng các mô hình máy học như Random Forest, và mạng nơ-ron sâu (Deep Neural Networks) để xử lý dữ liệu RT-IoT2022, nhưng hiệu suất của các mô hình này thường bị ảnh hưởng bởi số lượng đặc trưng lớn và sự dư thừa thông tin.

Về lựa chọn đặc trưng, các phương pháp như Principal Component Analysis (PCA), Recursive Feature Elimination (RFE), và các kỹ thuật dựa trên độ quan trọng đặc trưng (feature importance) đã được áp dụng rộng rãi để giảm chiều dữ liệu và cải thiện hiệu suất mô hình. Tuy nhiên, các nghiên cứu hiện tại chủ yếu tập trung vào một số thuật toán cụ thể hoặc không xem xét đầy đủ sự kết hợp giữa lựa chọn đặc trưng và so sánh mô hình trên các tập dữ liệu thời gian thực như RT-IoT2022. Hơn nữa, việc đánh giá toàn diện hiệu quả của các phương pháp này trong các kịch bản thực tế vẫn còn hạn chế, đặc biệt khi cân nhắc các yếu tố như thời gian xử lý và độ chính xác.

2 Hướng tiếp cận đề tài:

Trong bài nghiên cứu này, chúng tôi tập trung vào nghiên cứu việc giảm chiều trên bộ dữ liệu RT-IoT2022 bằng các phương pháp như chọn đặc trưng quan trọng, chọn ngưỡng tương quan. Trước khi giảm chiều, chúng tôi sử dụng phương pháp SMOTE giảm sự mất cân bằng dữ liệu.

Sử dụng các đặc trưng đó để đánh giá hiệu suất mô hình như LinearSVC, XGBoost, Logistic Regression, KNN, Random Forest, Neural Network và đánh giá hiệu suất mô hình dựa trên các thang đo độ chính xác (Accuracy), F1-Score, Precision, và Recall.

III Mục đích và nhiệm vụ nghiên cứu

1 Mục đích nghiên cứu:

Nghiên cứu nhằm xác định các đặc trưng quan trọng từ tập dữ liệu RT-IoT2022 để nâng cao khả năng phát hiện tấn công mạng thời gian thực và cải thiện hiệu suất mô hình về độ chính xác và chi phí tính toán so với sử dụng toàn bộ thuộc tính.

2 Nhiệm vụ nghiên cứu:

1. Áp dụng kỹ thuật SMOTE để xử lý mất cân bằng dữ liệu trong tập RT-IoT2022.
2. Chuẩn hóa dữ liệu bằng StandardScaler để đảm bảo tính nhất quán.
3. Sử dụng các phương pháp lựa chọn đặc trưng như Feature Importance, và ngưỡng tương quan (>0.8).

4. Huấn luyện các mô hình học máy (LinearSVC, XGBoost, Logistic Regression, KNN, Random Forest, Neural Network) với các đặc trưng được chọn.

5. Đánh giá hiệu suất mô hình bằng các thang đo Accuracy, F1-Score, Precision, và Recall.

6. Chia dữ liệu 80% huấn luyện và 20% kiểm tra, so sánh hiệu suất mô hình trước và sau khi chọn đặc trưng bằng các chỉ số hiệu suất.

IV Đối tượng và phạm vi nghiên cứu.

1. Tiền xử lý dữ liệu: Sử dụng SMOTE để cân bằng dữ liệu và StandardScaler để chuẩn hóa.

2. Lựa chọn đặc trưng: Áp dụng Feature Importance, và ngưỡng tương quan (>0.8) để giảm từ 85 đặc trưng xuống khoảng 40 đặc trưng liên quan đến lưu lượng mạng và hành vi tấn công.

3. Huấn luyện mô hình:LinearSVC, XGBoost, Logistic Regression, KNN, Random Forest, Neural Network trên dữ liệu chia 80% huấn luyện, 20% kiểm tra, sử dụng 5-fold cross-validation.

4. Đánh giá hiệu suất: Đánh giá bằng Accuracy, F1-Score, Precision, Recall, và thời gian xử lý; so sánh hiệu suất trước/sau khi chọn đặc trưng bằng biểu đồ ROC và thống kê.

V Phương pháp nghiên cứu

Luận văn áp dụng phương pháp nghiên cứu kết hợp giữa phương pháp lý thuyết,phương pháp thực nghiệm, và phương pháp chuyên gia, nhằm đảm bảo tính hệ thống, khoa học và hiệu quả trong quá trình thực hiện.

1 Phương pháp lý thuyết:

- Tìm hiểu các nghiên cứu liên quan đến tập dữ liệu RT-IoT2022 và các phương pháp lựa chọn đặc trưng (Feature Importance, ngưỡng tương quan) từ sách chuyên ngành, bài báo trên IEEE Xplore, SpringerLink, và hội nghị an ninh mạng (USENIX Security, NDSS).

- Nghiên cứu thư viện scikit-learn để triển khai LinearSVC, XGBoost, Logistic Regression, KNN, Random Forest, Neural Network, và TensorFlow hoặc PyTorch để xây dựng mạng nơron sâu (DNN).

- Lựa chọn tài liệu uy tín để đảm bảo cơ sở lý thuyết vững chắc.

2 Phương pháp thực nghiệm:

- Sử dụng Python với scikit-learn, TensorFlow, PyTorch để cài đặt mô hình và thuật toán.
- Tiền xử lý dữ liệu RT-IoT2022 bằng SMOTE để cân bằng dữ liệu và StandardScaler để chuẩn hóa, đảm bảo đáp ứng yêu cầu đầu vào.
- Áp dụng phương pháp Feature Importance, và ngưỡng tương quan (>0.8) để giảm từ 85 đặc trưng xuống khoảng dưới 40 đặc trưng.
- Huấn luyện LinearSVC, XGBoost, Logistic Regression, KNN, Random Forest, (trên scikit-learn), và Neural Network (trên TensorFlow/PyTorch) với dữ liệu chia 80% huấn luyện, 20% kiểm tra.
- Đánh giá hiệu suất bằng Accuracy, Precision, Recall, F1-Score, so sánh trước và sau khi lựa chọn đặc trưng bằng phương thống kê chỉ số hiệu suất.

3 Phương pháp chuyên gia:

- Trao đổi thường xuyên với giảng viên hướng dẫn để làm rõ các vấn đề khoa học liên quan, nhận phản hồi và định hướng cho từng giai đoạn nghiên cứu.
- Dựa trên ý kiến của giảng viên, điều chỉnh cách tiếp cận, tối ưu hóa quá trình triển khai thực nghiệm, và đảm bảo tiến độ thực hiện luận văn.

Phương pháp nghiên cứu này kết hợp chặt chẽ giữa lý thuyết và thực nghiệm, cùng với sự hỗ trợ từ chuyên gia, nhằm đảm bảo kết quả nghiên cứu có tính khoa học, khả thi và giá trị ứng dụng cao.

VI Giả thuyết khoa học

Việc áp dụng áp các phương pháp chọn đặc trưng (Feature Important và Chọn ngưỡng tương quan) sẽ cải thiện Accuracy, F1-Score, Precision, Recall, và thời gian xử lý, của các mô hình học máy trong phát hiện tấn công mạng thời gian thực so với sử dụng toàn bộ đặc trưng.

VII Những đóng góp của đề tài

Đề tài đóng góp vào việc sử dụng kỹ thuật SMOTE để xử lý mất cân bằng lớp và áp dụng các phương pháp lựa chọn đặc trưng (Feature Importance, ngưỡng tương quan) trên tập dữ liệu RT-IoT2022, từ đó tìm ra những đặc trưng quan trọng, cải thiện độ chính xác (Accuracy), F1-Score, và hiệu quả tính toán cho các mô hình LinearSVC, XGBoost, Logistic Regression, KNN, Random Forest, (trên scikit-learn), và Neural Network so với sử dụng toàn bộ đặc trưng. Đóng góp này hỗ trợ phát hiện các cuộc tấn công như DDoS, Brute-Force trong hệ thống IoT, cung cấp giải pháp an ninh mạng hiệu quả.

VIII Dự kiến nghiên cứu

STT	**Nội dung**	**Thời gian dự kiến**
1	Nghiên cứu, chọn đề tài, xây dựng đề cương luận văn	2 tuần
2	Nộp đề cương, sửa chữa hoàn thiện đề cương	1 tuần
3	Nghiên cứu, viết hoàn thiện luận văn Bìa báo cáo Mục lục Tóm tắt (Abstract) Chương 1: tổng quan vấn đề Chương 2: Lược khảo tài liệu Chương 3: Phương pháp nghiên cứu Chương 4: Thực nghiệm và thảo luận Chương 5: Kết luận và hướng phát triển Tài liệu tham khảo (Reference)	 1 tuần 2 tuần 1 tuần 1 tuần

Bảng 1: Kế hoạch thực hiện luận văn

9. Nội dung dự kiến của luận văn

Tóm tắt (Abstract)

- Tóm tắt nghiên cứu (150–250 từ).
- Gồm: Lý do, mục tiêu, phương pháp, kết quả (nếu có), kết luận.

Chương 1: Tổng quan vấn đề

- Lý do chọn đề tài.

- Vấn đề nghiên cứu, mục tiêu, câu hỏi nghiên cứu.
- Phạm vi nghiên cứu.

Chương 2: Lược khảo tài liệu

- Cơ sở lý thuyết: **scikit-learn**, **PyTorch**.
- Các mô hình: LinearSVC, XGBoost, Logistic Regression, KNN, Random Forest, và Neural Network.
- Chỉ số đánh giá: Accuracy, Precision, Recall, F1-score.
- Các phương pháp lựa chọn đặc trưng: Feature Important, ngương tương quan
- Các phương pháp cân bằng dữ liệu: SMOTE

Chương 3: Phương pháp nghiên cứu (Methodology)

- Mô tả cách huấn luyện mô hình.
- Thiết kế kịch bản thực nghiệm:
  - Chuẩn bị dữ liệu: Tiền xử lý, chia tập huấn luyện và kiểm thử.
  - Cài đặt mô hình: Sử dụng thư viện scikit-learn, PyTorch.
- Đề xuất quy trình tối ưu hóa và huấn luyện mô hình.

Chương 4: Thực nghiệm và Thảo luận

- Trình bày và phân tích kết quả thu được.
- Sử dụng biểu đồ, bảng biểu, hình ảnh minh họa (nếu cần).
- Đánh giá và giải thích kết quả nghiên cứu.
- So sánh với các nghiên cứu trước.
- Nêu ý nghĩa thực tiễn của nghiên cứu.
- Nêu hạn chế và đề xuất hướng nghiên cứu tiếp theo.

Chương 5: Kết luận và Hướng phát triển

- Tóm tắt những điểm chính đã đạt được.
- Trả lời các câu hỏi nghiên cứu.
- Đề xuất giải pháp hoặc hướng nghiên cứu tiếp theo.

Tài liệu tham khảo (References)

- Liệt kê đầy đủ theo chuẩn trích dẫn (APA, MLA, Harvard, v.v.).
- Bao gồm: sách, bài báo khoa học, website, báo cáo, v.v.

Tài liệu

[1] S. Bhunia and R. Nagapadma. RT-IoT2022. UCI Machine Learning Repository, 2023. https://doi.org/10.24432/C5P338.