HỆ THỐNG PHÁT HIỆN XÂM NHẬP PHI TẬP TRUNG KHẢ DIỄN GIẢI HỖ TRỢ HỌC TIỆM TIẾN

Nguyễn Hữu Quyền - 220202021

Tóm tắt

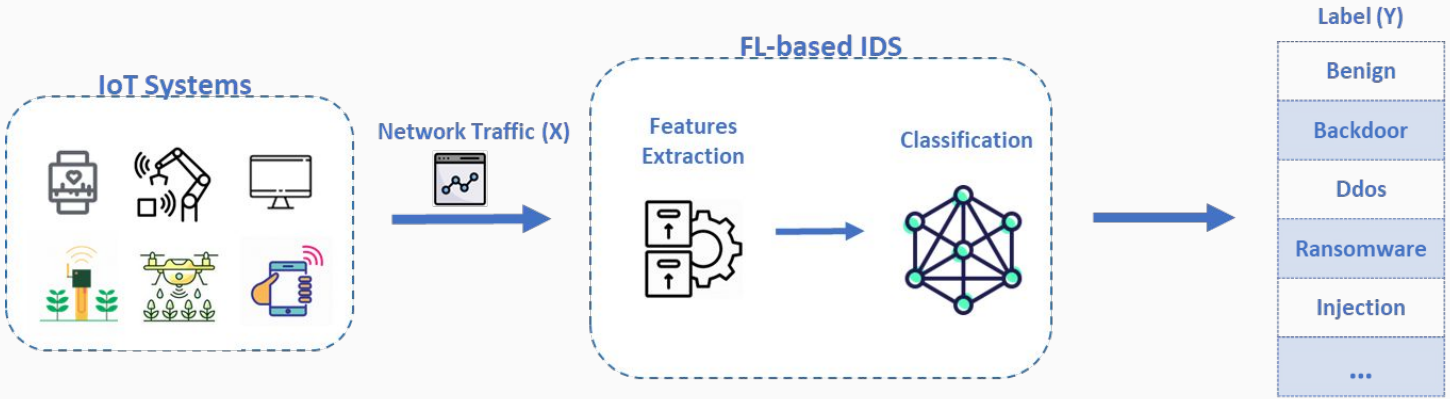
- Lớp: CS2205.CH1702.APR2023
- Link Github: https://github.com/huuquyen2606/CS2205.CH1702.APR2023/
- Link YouTube video: https://youtu.be/SXOHuV5y3XM

Nguyễn Hữu Quyền

Giới thiệu

Hệ thống Phát hiện xâm nhập phi tập trung (Federated Intrusion Detection System - FedIDS):

- ❖ Tận dụng được lượng lớn dữ liệu từ nhiều Mạng thiết bị IoT.
- ❖ Giảm chi phí huấn luyện và tăng cường tính bảo mật cho dữ liệu.

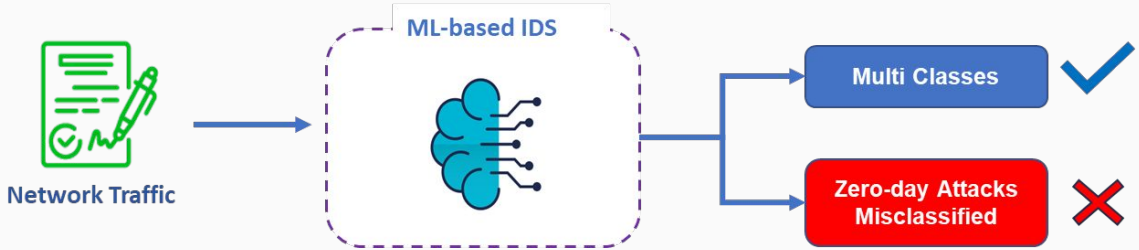


Hình 1: Hệ thống FL-based IDS

Giới thiệu

Vấn đề của các Hệ thống FedIDS:

1. Các lớp (classes) tấn công mới Zero-day thường bị phân lớp sai.
2. Hạn chế tài nguyên ổ cứng lưu trữ các máy cộng tác.
3. Dữ liệu huấn luyện ở các máy cộng tác mất cân bằng (NonIID).
4. Mô hình phân loại vẫn chưa giải thích được lý do cụ thể khi đưa ra các dự đoán.



Hình 2: Phân lớp sai cho các lớp tấn công mới

Mục tiêu

- Xây dựng và đánh giá hiệu năng của mô hình phát hiện xâm nhập khả diễn giải tập trung (**XAI-based IDS**) dựa trên ba bộ dữ liệu CSE-CIC-IDS2018 [4], ToN-IoT [5], Bot-IoT [6]. (Vấn đề 4)
- So sánh hiệu năng của mô hình phát hiện xâm nhập khả diễn giải phi tập trung (**XAI-based FedIDS**) so với mô hình **XAI-based IDS** dựa trên 3 bộ dữ liệu như trên. (Vấn đề 4)
- Đề xuất mô hình phát hiện xâm nhập phi tập trung khả diễn giải hỗ trợ học tiệm tiến (**FedXI-IDS**) và so sánh hiệu suất với mô hình **XAI-based FedIDS** dựa trên 3 bộ dữ liệu như trên. (Vấn đề 1, 2 và 3)

Nội dung và Phương pháp

Nội dung 1: Nghiên cứu xây dựng mô hình phát hiện xâm nhập khả diễn giải.

- Nghiên cứu mô hình **XAI-based IDS** dựa trên phương pháp học khả diễn giải (**Explainable AI**).
- Kết hợp với các mô hình **Word Representations**: Word2Vec, n-grams, BERT để trích xuất các đặc trưng về ngữ cảnh và cấu trúc của dữ liệu mạng.
- Đánh giá hiệu suất của mô hình **XAI-based IDS** trên 3 bộ dữ liệu CSE-CIC-IDS2018, ToN-IoT, Bot-IoT với độ chính xác kì vọng trên **95%**.

Nội dung và Phương pháp

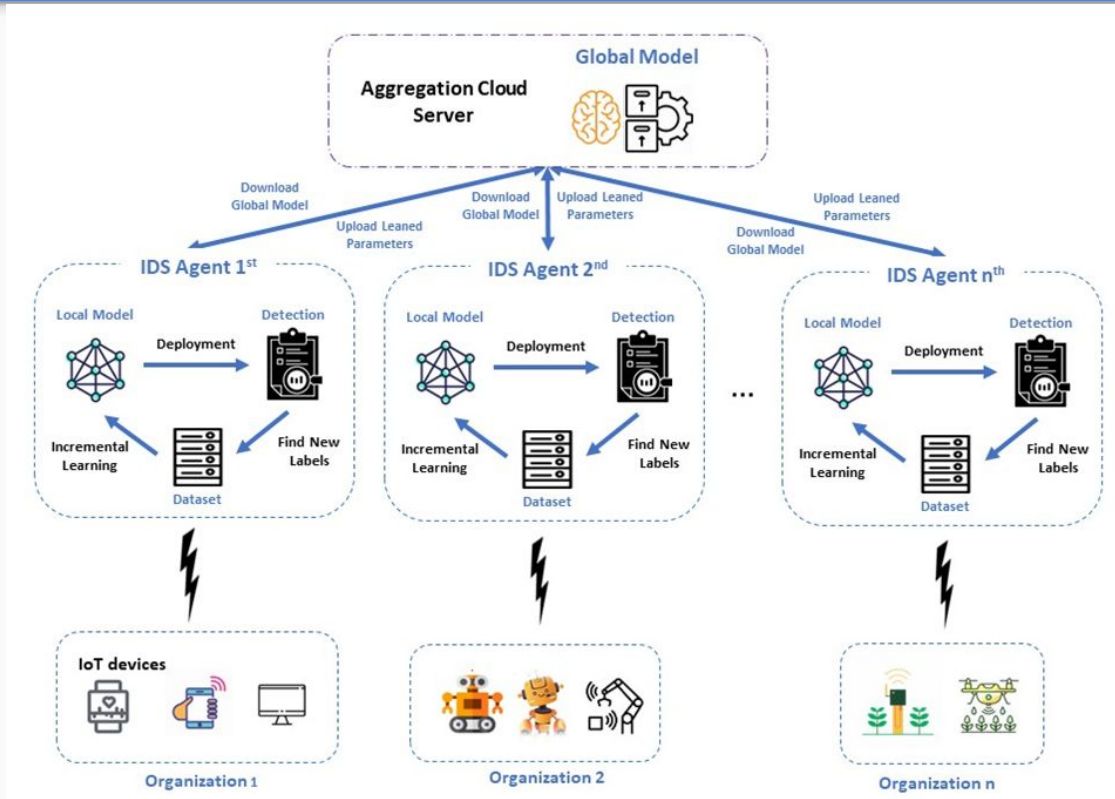
Nội dung 2: Nghiên cứu đề xuất mô hình phát hiện xâm nhập phi tập trung khả diễn giải.

- Nghiên cứu mô hình **XAI-based FedIDS** dựa trên phương pháp **học cộng tác** và mô hình **XAI-based IDS**.
- Thực nghiệm và so sánh hiệu suất khi huấn luyện **XAI-based IDS** tập trung và **XAI-based FedIDS** phi tập trung với 3 bộ dữ liệu như trên.

Nội dung và Phương pháp

Nội dung 3: Nghiên cứu mô hình phát hiện xâm nhập khả diễn giải phi tập trung hỗ trợ học tiệm tiến

- Nghiên cứu mô hình **FedXI-IDS** dựa trên **XAI-based FedIDS** và phương pháp **học tiệm tiến (Incremental learning)**.
- Thực nghiệm và so sánh hiệu suất của **FedXI-IDS** với phương pháp **GLFC[3]** và một số phương pháp SOTA khác dựa trên 3 bộ dữ liệu như trên.



Hình 3: Hệ thống FedXI-IDS

Kết quả dự kiến

Dự kiến kết quả nghiên cứu:

- Xây dựng hoàn thiện một hệ thống phát hiện xâm nhập phi tập trung khả diễn giải hỗ trợ học tiệm tiến đạt được hiệu suất phân loại cao với độ chính xác trên 95%.

Báo cáo kết quả nghiên cứu:

- Dự kiến công bố bài báo khoa học tại Hội nghị chuyên ngành quốc tế Hạng B (theo CORE2021): 01 bài (Với nội dung 1 và 2).
- Dự kiến công bố bài báo khoa học tại Tạp chí chuyên ngành quốc tế Hạng Q1: 01 bài (Với nội dung 1, 2 và 3).

Tài liệu tham khảo

[1]. Bimal Ghimire ,Danda B. Rawat: Recent Advances on Federated Learning for Cybersecurity and Cybersecurity for Federated Learning for Internet of Things. IEEE Internet of Things Journal 2022: 8229 - 8249

[2]. Othmane Friha, Mohamed Amine Ferrag, Lei Shu, Leandros Maglaras, Kim-Kwang Raymond Choo, Mehdi Nafaa: FELIDS: Federated learning-based intrusion detection system for agricultural Internet of Things. Journal of Parallel and Distributed Computing 2022: 17-31

[3]. Jiahua Dong, Lixu Wang, Zhen Fang, Gan Sun, Shichao Xu, Xiao Wang, Qi Zhu: Federated Class-Incremental Learning. CVPR 2022: 10164-10173

[4]. Iman Sharafaldin, Arash Habibi Lashkari, Ali A. Ghorbani: Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. ICISSP 2018: 108-116

[5]. Abdullah Alsaedi, Nour Moustafa, Zahir Tari, Abdun Mahmood, Adnan Anwar: TON_IoT Telemetry Dataset: A New Generation Dataset of IoT and IIoT for Data-Driven Intrusion Detection Systems. IEEE Access 2020: 165130-165150

[6]. Jared M. Peterson, Joffrey L. Leevy, Taghi M. Khoshgoftaar: A Review and Analysis of the Bot-IoT Dataset. SOSE 2021: 20-27

[7]. H. Brendan McMahan, Eider Moore, Daniel Ramage, Seth Hampson, Blaise Aguera y Arca: Communication-Efficient Learning of Deep Networks from Decentralized Data. AISTATS 2017:1273–1282