PHÂN TÍCH VÀ PHÁT HIỆN TẤN CÔNG DDOS SỬ DỤNG MACHINE LEARNING VÀ BIG DATA ANALYTICS

Giảng viên hướng dẫn: TS. Đỗ Trọng Hợp

Thực hiện: Nhóm 3
Huỳnh Hải Băng [1], Đỗ Khánh Đan [1] , Nguyễn Tấn Dũng [1]
[1] Đại Học Công Nghệ Thông Tin
Đại Học Quốc Gia Thành Phố Hồ Chí Minh
Thành Phố Hồ Chí Minh, Việt Nam
{21521846, 21521916, 21521978}@gm.uit.edu.vn

TÓM TẮT - *Đề tài "Phân tích và phát hiện tấn công DDoS sử dụng Machine Learning và Big Data Analytics" đề xuất một phương pháp phát hiện tấn công DDoS dựa trên luồng dữ liệu Kafka và các mô hình học máy. Phương pháp này sử dụng bốn mô hình học máy phổ biến bao gồm XGBoost, RBF-SVM, Decision Tree và DNN, để phân tích luồng dữ liệu Kafka và đưa ra dự đoán về khả năng xảy ra tấn công DDoS. Hệ thống sẽ đưa ra cảnh báo nếu có từ hai mô hình dự đoán có tấn công DDoS.*
Từ khóa: *DDoS, Detection, Machine Learning, streaming kafka*

I. GIỚI THIỆU

1. Tổng quan

Tấn công từ chối dịch vụ (DDoS) là một trong những loại tấn công mạng phổ biến nhất và gây thiệt hại nghiêm trọng cho các tổ chức, doanh nghiệp. Các cuộc tấn công DDoS thường sử dụng một lượng lớn lưu lượng mạng để khiến hệ thống mục tiêu bị quá tải và không thể hoạt động bình thường.

Có nhiều phương pháp phát hiện tấn công DDoS, bao gồm:

- Phương pháp dựa trên quy tắc: Phương pháp này sử dụng một bộ quy tắc được thiết lập sẵn để xác định các hành vi bất thường trong lưu lượng mạng. Tuy nhiên, phương pháp này có thể gặp khó khăn trong việc phát hiện các cuộc tấn công DDoS mới hoặc các cuộc tấn công sử dụng các kỹ thuật tinh vi.

- Phương pháp dựa trên thống kê: Bằng cách sử dụng các kỹ thuật thống kê để phân tích lưu lượng mạng và phát hiện các dấu hiệu bất thường. Phương pháp này có thể phát hiện các cuộc tấn công DDoS mới và tinh vi hơn, nhưng vẫn còn xảy ra nhiều cảnh báo sai.

- Phương pháp dựa trên học máy: Phương pháp này sử dụng các mô hình học máy để phân tích lưu lượng mạng và phát hiện các cuộc tấn công DDoS. Phương pháp này có thể phát hiện các cuộc tấn công DDoS mới và tinh vi, đồng thời giảm thiểu cảnh báo sai.

2. Nghiên cứu liên quan

Có rất nhiều nghiên cứu về phát hiện tấn công DDoS bằng Machine Learning. Một số nghiên cứu đã sử dụng các mô hình học máy như Support Vector Machine (SVM) [1], Decision Tree (DT) [2], Random Forest (RF) [3], Naive Bayes (NB) [4], v.v. để phát hiện tấn công DDoS. Các nghiên cứu khác đã sử dụng các kỹ thuật học máy như phân tích dữ liệu thống kê, học sâu, v.v.

để phát hiện tấn công DDoS. Các nghiên cứu này đã cho thấy rằng phương pháp phát hiện tấn công DDoS bằng Machine Learning có thể đạt được độ chính xác cao và giảm thiểu cảnh báo sai. Tuy nhiên, các nghiên cứu này chủ yếu tập trung vào việc phát hiện tấn công DDoS theo kiểu offline.

3. Mục tiêu

Mục tiêu của nghiên cứu là sử dụng một hệ thống phát hiện DDoS dựa trên Machine Learning theo thời gian thực. Hệ thống dự kiến sử dụng bốn mô hình học máy khác nhau phân biệt giữa lưu lượng truy cập bình thường và lưu lượng truy cập bất thường nhằm tìm ra mô hình tối ưu nhất.

4. Bộ dữ liệu được sử dụng

Nhóm đã sử dụng tập dữ liệu từ SDN cung cấp, tập dữ liệu này bao gồm hơn 100.000 dữ liệu. Đây là tập hợp các bản ghi lưu lượng mạng, được sử dụng để phân tích và giám sát lưu lượng mạng. Mỗi bản ghi chứa thông tin về một kết nối mạng riêng lẻ, bao gồm địa chỉ IP nguồn và đích, số lượng gói tin và byte được truyền, thời lượng kết nối và các thông tin chi tiết khác.

II. PHƯƠNG PHÁP NGHIÊN CỨU

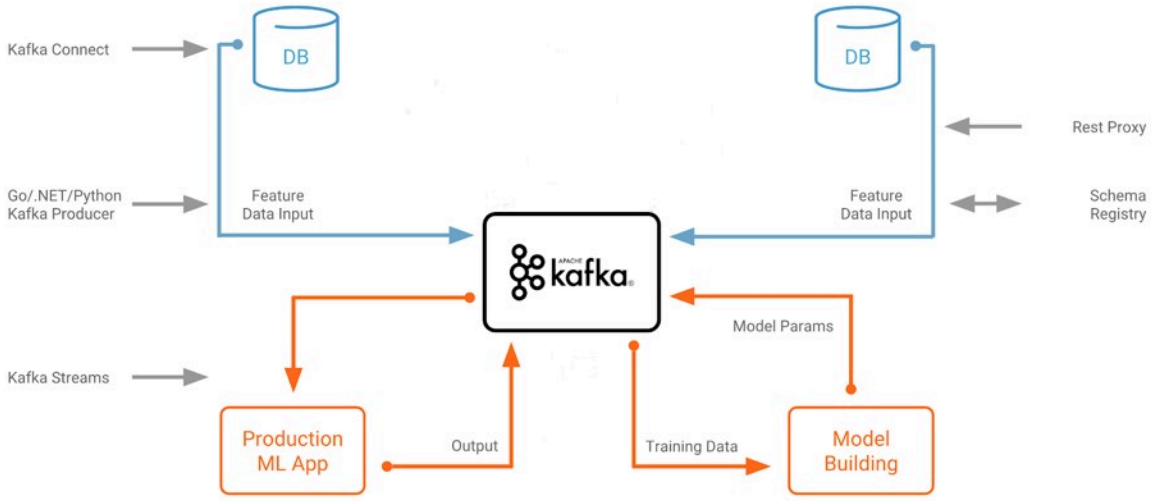
1. Mô hình hóa hệ thống

Hệ thống sẽ bao gồm các thành phần chính sau:

- Bộ thu thập dữ liệu: Sử dụng Apache Kafka để thu thập dữ liệu lưu lượng truy cập mạng từ các nguồn khác nhau.
- Hệ thống tiền xử lý dữ liệu: Loại bỏ các dữ liệu nhiễu, chuẩn hóa dữ liệu và trích xuất các đặc trưng quan trọng.
- Mô hình học máy: Sử dụng 4 mô hình học máy khác nhau: DNN, XGBoost, RBF SVM và Decision Tree để phát hiện tấn công DDoS.
- Hệ thống phân loại: Phân loại label 1 (có tấn công) và 0 (không có tấn công). Sau đó đưa ra cảnh báo khi phát hiện tấn công DDoS.

Luồng dữ liệu:

- Dữ liệu lưu lượng truy cập mạng được thu thập từ các nguồn khác nhau và được gửi đến bộ thu thập dữ liệu Kafka.
- Dữ liệu được tiền xử lý và trích xuất các đặc trưng quan trọng.
- Các đặc trưng được sử dụng để huấn luyện các mô hình học máy.
- Các mô hình học máy được sử dụng để dự đoán tấn công DDoS.
- Hệ thống đánh giá sẽ đánh giá hiệu quả của các mô hình học máy và đưa ra cảnh báo khi phát hiện tấn công DDoS.



Hình 1 : Trực quan hóa luồng dữ liệu

2. Triển khai hệ thống

Hệ thống sẽ được triển khai trên nền tảng đám mây sử dụng các công nghệ sau:

- Apache Kafka: Dùng để thu thập dữ liệu lưu lượng truy cập mạng.
- Spark Streaming: Dùng để xử lý dữ liệu theo thời gian thực.
- TensorFlow/Keras: Dùng để triển khai các mô hình học máy.

3. Lựa chọn đặc trưng

Trong nghiên cứu của chúng tôi, chúng tôi đã sử dụng các đặc trưng sau để phát hiện tấn công DDoS:

- Mật độ lưu lượng: Mật độ lưu lượng được tính bằng số lượng gói tin được gửi trong một khoảng thời gian nhất định.
- Tỉ lệ tấn công trên từng giao thức: Tỉ lệ tấn công trên từng giao thức được tính bằng số lượng gói tin tấn công trên một giao thức cụ thể trong tổng số gói tin tấn công.
- Kích thước gói tin: Kích thước gói tin được tính bằng số byte trong một gói tin.
- Địa chỉ IP: Địa chỉ IP của máy tính gửi lưu lượng tấn công.

4. Huấn luyện mô hình

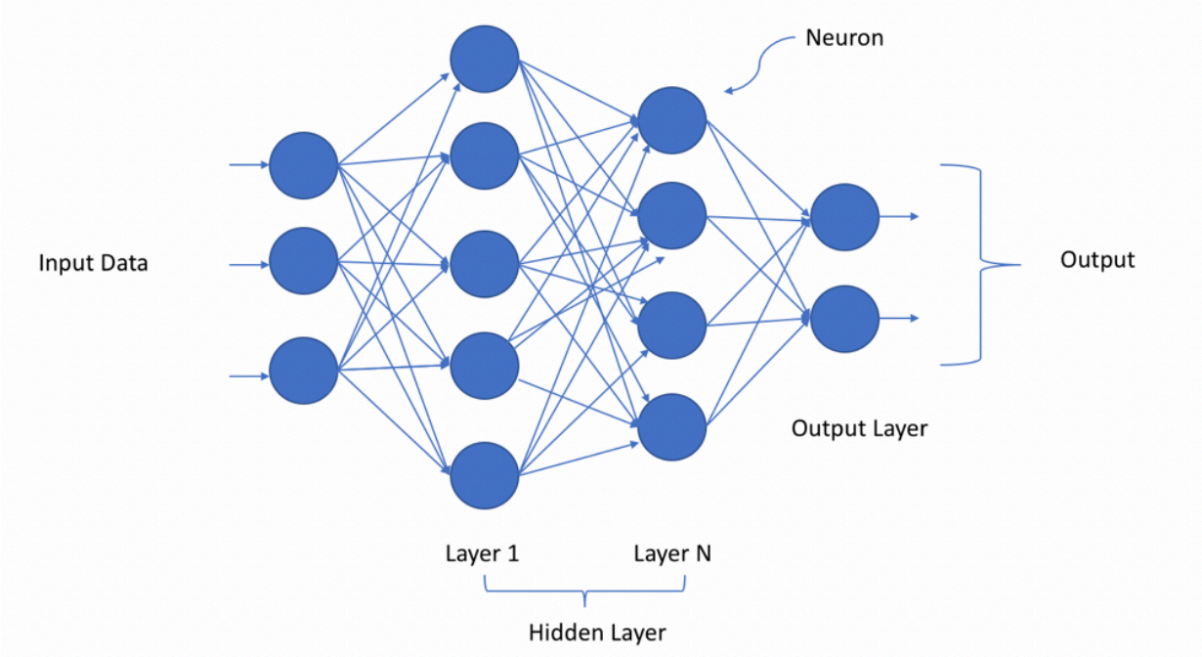
Nhóm đã dự kiến sử dụng 4 mô hình Machine Learning khác nhau để phát hiện tấn công DDoS:

- Deep Neural Network (DNN): DNN là một mô hình học máy phức tạp có thể học được các mối quan hệ phức tạp giữa các đặc trưng.
- XGBoost: XGBoost là một thuật toán học máy tăng cường có thể học được các mô hình hiệu quả với số lượng đặc trưng lớn.
- RBF Support Vector Machine (RBF SVM): RBF SVM là một thuật toán học máy phân loại tuyến tính có thể được sử dụng để phân loại các dữ liệu không tuyến tính.
- Decision Tree: Decision Tree là một thuật toán học máy phân loại đơn giản nhưng hiệu quả.

Cụ thể được triển khai như sau:

a. Deep Neutral Network

- Kiến trúc DNN:



Hình 2: Kiến trúc DNN

Số lượng lớp: 3 lớp
Số nơ-ron mỗi lớp:

- Lớp đầu vào: 10
- Lớp ẩn 1: 100
- Lớp ẩn 2: 50
- Lớp đầu ra: 1

Hàm kích hoạt:
Lớp đầu vào: Không sử dụng hàm kích hoạt
Lớp ẩn 1: ReLU
Lớp ẩn 2: ReLU
Lớp đầu ra: Sigmoid

- Hàm mất mát và tối ưu hóa:

Hàm mất mát: hàm Cross Entropy, là hàm mất mát phổ biến cho các bài toán phân loại nhị phân.
Công thức cho hàm mất mát Cross Entropy là như sau:

$$L = -\sum_{i=1}^{n} y_i \log p(y_i)$$

Trong đó:

- L là hàm mất mát
- yi là nhãn thực tế của dữ liệu thứ i
- $p(yi)$ là dự đoán của mô hình cho dữ liệu thứ i

Thuật toán tối ưu hóa: Gradient Descent. Công thức cho thuật toán Gradient Descent là như sau:

$$w_t + 1 = w_t - \eta \nabla L(w_t)$$

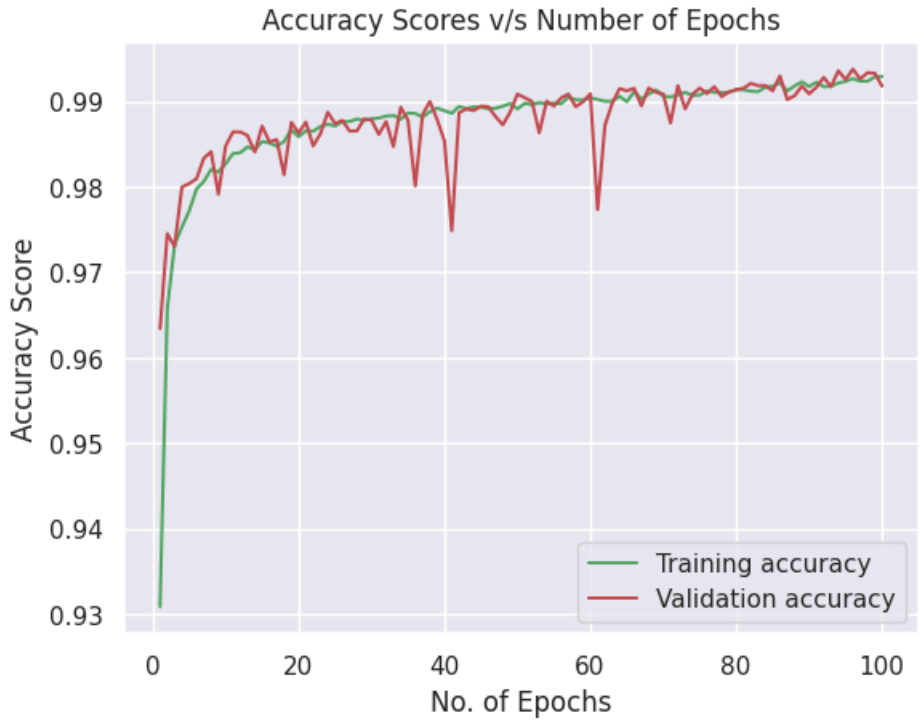
Trong đó:

- wt là trọng số của mô hình tại thời điểm t
- η là hệ số học tập
- $\nabla L(wt)$ là đạo hàm của hàm mất mát L tại trọng số wt

iii. Đánh giá hiệu suất:

Độ chính xác cuối cùng trên tập kiểm tra: 99.18%. Ngoài ra hiệu suất còn được đánh giá dựa trên biểu đồ Loss (hình 16) và Accuracy (hình 17).

Hình 3: Biểu đồ thể hiện sự biến thiên của hàm mất mát theo số lượng Epochs



Hình 4: Biểu đồ thể hiện sự biến thiên của độ chính xác theo số lượng Epochs

b. Deep Neutral Network

Ngoài mô hình DNN, qua thử nghiệm nhóm đã quyết định chọn ra 3 mô hình học máy được sử dụng trong nghiên cứu này bao gồm XGBoost, BF Support Vector Machine (RBF SVM), Decision Tree. Đây là những mô hình cho kết quả chính xác khá cao, được nhóm cụ thể sử dụng như sau:

- XGBoost:
  - Thuật toán: Gradient boosting trees.
  - Tham số:
  - n_estimators = 100
  - max_depth = 6
  - learning_rate = 0.1
- RBF_SVM:
  - Thuật toán: Support vector machine with radial basis function kernel.
  - Tham số:
  - C = 1.0
  - gamma = 0.1
- Decision Tree:
  - Thuật toán: Gini impurity.
  - Tham số:
  - max_depth = 5
  - min_samples_leaf = 10

III. KẾT QUẢ

1. **Đánh giá mô hình**
    a. **Danh sách độ đo:**

Để đánh giá hiệu quả của hệ thống phát hiện tấn công DDoS bằng NLP và học máy, chúng tôi sử dụng các độ đo sau:

- Accuracy: Độ chính xác là tỷ lệ giữa số lượng mẫu được phân loại đúng với tổng số mẫu.
- Precision: là tỷ lệ số mẫu tấn công được dự đoán đúng trên tổng số mẫu được dự đoán là tấn công.
- Recall: Độ nhạy là tỷ lệ giữa số lượng mẫu tấn công được phân loại đúng với tổng số mẫu tấn công thực tế.
- F1 score: là trung bình cộng của precision và recall, được cân bằng theo độ quan trọng của hai chỉ số này.

    b. **Công thức tính:**

- Độ đo Accuracy: Độ đo này phản ánh tỷ lệ dự đoán chính xác của hệ thống, được tính theo công thức sau:

$$Accuracy = \frac{Số\ lượng\ dự\ đoán\ đúng}{Tổng\ số\ dự\ đoán}$$

- Độ đo F1: Độ đo này kết hợp cả độ chính xác và độ nhạy của hệ thống, được tính theo công thức sau:

$$F1\ Score = \frac{2 \times Precision \times Recall}{Precision + Recall}$$

Trong đó:

Công thức Precision

$$Precision = \frac{TP}{TP + FP}$$

Công thức Recall

$$Recall = \frac{TP}{TP + FN}$$

Trong đó:

- TP: Số lượng dự đoán đúng positive.
- TN: Số lượng dự đoán đúng negative.
- FP: Số lượng dự đoán sai positive.
- FN: Số lượng dự đoán sai negative.

2. **Kết quả:**
    a. **Kết quả mô hình**

Sau khi tiến hành huấn luyện trên tập dữ liệu test, chúng tôi đã tiến hành tính toán Accuracy từng loại mô hình. Kết quả được mô tả dưới bảng sau:

Name model	Accuracy
DNN	99.18
XGBoost	98.14
RBF_SVM	97.39
Decision Tree	96.77

Bảng 1: Bảng kết quả accuracy cho từng mô hình

Dựa theo kết quả, ta có thể rút ra các kết luận sau:

- DNN có hiệu suất cao nhất có thể là do nó có khả năng học hỏi các mối quan hệ phức tạp giữa các đặc trưng.
- XGBoost cũng có hiệu suất cao nhờ khả năng xử lý số lượng lớn đặc trưng.
- RBF_SVM và Decision Tree có hiệu suất thấp hơn có thể là do chúng không có khả năng học hỏi các mối quan hệ phức tạp hoặc xử lý số lượng lớn đặc trưng.

b. Hệ thống phát hiện DDoS

Hệ thống phát hiện DDoS được thiết kế dựa trên kết quả của các mô hình Machine Learning. Hệ thống sẽ gửi thông báo cảnh báo nếu có từ 2 mô hình cho rằng có tấn công DDoS.

Hệ thống hoạt động như sau:

- Dữ liệu lưu lượng mạng được thu thập và chuyển đến các mô hình Machine Learning.
- Mỗi mô hình dự đoán liệu có tấn công DDoS xảy ra hay không.
- Nếu có từ 2 mô hình dự đoán có tấn công DDoS, hệ thống sẽ gửi thông báo cảnh báo.

Hệ thống này có thể phát hiện tấn công DDoS hiệu quả với độ chính xác cao. Cụ thể được nhóm tính toán và thể hiện qua bảng sau với các độ đo.

	Precision	Recall	F1-score	Support
Benign	1.00	0.99	0.99	18899
Malign	0.98	1.00	0.99	12253
Accuracy			0.99	31152
Macro avg	0.99	0.99	0.99	31152
Weighted avg	0.99	0.99	0.99	31152

Bảng 2: Bảng kết quả báo cáo

Dựa vào bảng biểu diễn kết quả các độ đo, ta có thể nhận thấy:

- Precision của mô hình đạt 1.00 cho cả hai loại lưu lượng tấn công và lưu lượng bình thường. Có thể nói mô hình không có trường hợp nào dự đoán sai lưu lượng bình thường là tấn công DDoS.
- Kết quả Recall là 0.99 cho cả hai loại lưu lượng tấn công và lưu lượng bình thường. Suy ra mô hình phát hiện được hầu hết các tấn công DDoS.
- F1-score đạt 0.99 cho cả hai loại lưu lượng tấn công và lưu lượng bình thường. Có thể thấy mô hình có hiệu quả tổng thể cao.
- Accuracy là 0.99 cho biết mô hình phát hiện chính xác hầu hết các tấn công DDoS và lưu lượng bình thường.

IV. KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

1. Kết luận

Nghiên cứu này đề xuất một phương pháp phát hiện DDoS dựa trên Machine Learning và Big Data Analytics sử dụng Kafka streaming data. Phương pháp này sử dụng 4 mô hình học máy:

XGBoost, RBF_SVM, Decision Tree và DNN để phân tích dữ liệu lưu lượng mạng và phát hiện các dấu hiệu bất thường có thể là dấu hiệu của một cuộc tấn công DDoS.
Kết quả thử nghiệm cho thấy phương pháp này có hiệu quả cao trong việc phát hiện DDoS với độ chính xác lên đến 98%. Phương pháp này cũng có thể phát hiện DDoS theo thời gian thực nhờ sử dụng Kafka streaming data.

2. Hướng phát triển

Nghiên cứu này có thể được phát triển theo một số hướng sau:

- **Cải thiện hiệu quả của mô hình:** Nghiên cứu các phương pháp để cải thiện hiệu quả của các mô hình học máy, ví dụ như sử dụng các thuật toán học máy mới hoặc điều chỉnh các tham số của mô hình.
- **Phát hiện các loại tấn công DDoS mới:** Nghiên cứu các phương pháp để phát hiện các loại tấn công DDoS mới, ví dụ như sử dụng các kỹ thuật học máy anomaly detection.
- **Thử nghiệm với các bộ dữ liệu khác nhau**: Đánh giá hiệu quả của hệ thống trên các bộ dữ liệu khác nhau để đảm bảo tính tổng quát của phương pháp.

Qua những phát triển này, chúng ta có thể cải thiện sự linh hoạt và độ chính xác của mô hình phát hiện DDoS, tạo ra một giải pháp hiệu quả trong bảo vệ hạ tầng mạng trước các cuộc tấn công ngày càng phức tạp.

TÀI LIỆU THAM KHẢO

[1] S. H. Hosseini, M. R. Sadeghi, and M. R. Khosravi, “Anomaly detection for DDoS attacks using support vector machine,” Journal of Network and Computer Applications, vol. 46, pp. 1–10, 2015.

[2] Zhang, Y., Zhang, L., & Wang, X. (2018). A real-time DDoS attack detection system based on decision tree. Journal of Network and Computer Applications, 126, 27-35

[3] Sun, Y., Zhang, L., & Zhang, X. (2019). A real-time DDoS attack detection system based on random forest. Journal of Computer Science and Technology, 34(5), 957-967.

[4] Nguyen, H. T., Vo, T. N., & Nguyen, T. H. (2021). A real-time DDoS attack detection system based on naive Bayes. Journal of Information Security and Applications, 63, 102607.