STUDYING A SOLUTION FOR EARLY DETECTION OF DDOS ATTACKS BASED ON MACHINE LEARNING ALGORITHMS

Le Hoang Hiep[1*], Le Xuan Hieu[2], Ho Thi Tuyen[1], Duong Thi Quy[1]
[1]*TNU - University of Information and Communication Technology*
[2]*Thai Nguyen University*

ARTICLE INFO

Received: 11/7/2022
Revised: 05/8/2022
Published: 05/8/2022

KEYWORDS

Denial of service
Cyber attack
Network security
Machine learning
DDoS attack

ABSTRACT

This paper focused on researching and proposing to build a system that acts as a sensor that can be installed anywhere on the network and performs online traffic classification. The proposed system used basic machine learning techniques for network anomaly detection and data dimensionality reduction techniques to remove features that are not significant in anomaly detection. The main goal of the proposed system was to reduce the computation time to help detect the attack early but still ensure the accuracy of anomaly detection. The obtained results showed that the model using the KNN algorithm combined with the feature extraction technique had relatively stable accuracy for all data sets (lowest is 99.15% on NSL-KDD set, highest is 99.73% in simulation dataset) with fast execution time (since the data is reduced in size, making the calculation faster).

NGHIÊN CỨU PHƯƠNG PHÁP PHÁT HIỆN SỚM XÂM NHẬP BẤT THƯỜNG MẠNG DDOS DỰA TRÊN CÁC THUẬT TOÁN HỌC MÁY

Lê Hoàng Hiệp[1*], Lê Xuân Hiếu[2], Hồ Thị Tuyến[1], Dương Thị Quy[1]
[1]*Trường Đại học Công nghệ thông tin và Truyền thông – ĐH Thái Nguyên*
[2]*Đại học Thái Nguyên*

THÔNG TIN BÀI BÁO

Ngày nhận bài: 11/7/2022
Ngày hoàn thiện: 05/8/2022
Ngày đăng: 05/8/2022

TỪ KHÓA

Từ chối dịch vụ
Tấn công mạng
An ninh mạng
Học máy
Tấn công DDoS

TÓM TẮT

Bài báo này tập trung nghiên cứu đề xuất xây dựng hệ thống hoạt động như một cảm biến có thể được cài đặt ở bất kỳ đâu trên mạng và thực hiện phân loại lưu lượng truy cập trực tuyến. Hệ thống đề xuất sử dụng các kỹ thuật về học máy cơ bản để phát hiện xâm nhập bất thường mạng và các kỹ thuật giảm chiều dữ liệu để loại bỏ các đặc trưng không có nhiều ý nghĩa trong việc phát hiện bất thường. Mục tiêu chính của hệ thống đề xuất là giảm thời gian tính toán giúp phát hiện sớm tấn công nhưng vẫn đảm bảo độ chính xác của việc phát hiện bất thường. Qua kết quả đạt được cho thấy mô hình sử dụng thuật toán KNN kết hợp với kỹ thuật trích chọn đặc trưng cho độ chính xác tương đối ổn định với tất cả các bộ dữ liệu (thấp nhất là 99,15% trên bộ NSL-KDD, cao nhất là 99,73% tại bộ dữ liệu mô phỏng) với thời gian thực thi nhanh (do dữ liệu được giảm chiều khiến cho việc tính toán nhanh hơn).

DOI: https://doi.org/10.34238/tnu-jst.6248

[*] Corresponding author. *Email: lhhiep@ictu.edu.vn*

1. Giới thiệu

Thử thách lớn nhất trong việc chống lại DDoS là việc phải phát hiện sớm các cuộc tấn công và giảm thiểu tấn công nhanh nhất có thể. Đã có nghiên cứu chỉ ra tính không hiệu quả của việc phát hiện và giảm thiểu các cuộc tấn công DDoS có liên quan trực tiếp đến việc cấu hình hệ thống sai và sự tốn thời gian do thiếu công cụ theo dõi lưu lượng động trên mạng nếu thiếu sự giám sát của con người. Các phương pháp phát hiện xâm nhập truyền thống chủ yếu được chia thành phát hiện bất thường và phát hiện dựa theo dấu hiệu. Phát hiện bất thường chủ yếu sử dụng kinh nghiệm chuyên môn và các phương pháp suy luận. Trong đó phương pháp thống kê và thuật toán Bayers là các thuật toán điển hình đại diện được sử dụng. Phương pháp này nhìn chung giúp phát hiện và chống lại các cuộc tấn công mạng khá tốt nhưng với các kĩ thuật công nghệ cao như ngày nay và sự phát triển về các kỹ thuật tấn công ngày càng mạnh và tinh vi thì các phương pháp này cũng rất khó đáp ứng được việc ngăn chặn và phát hiện sớm. Một số công bố liên quan tới nghiên cứu này gần đây như: Phương pháp D-FACE [1], [2]; Một kỹ thuật dựa trên Giao thức HTTP [3], [4]; Kỹ thuật Multiple – Features - Based Constrained – *K* – Means [5]-[7]; Phương pháp *K*-nearest neighbor classifier (KNNC) [9]-[11] đã có những ưu điểm như: có thể phát hiện các cuộc tấn công DDoS nhưng lại đòi hỏi mức độ tương thích IPS cao nên nó hạn chế sử dụng cho giải pháp chung và phương pháp này dường như không thể áp dụng trong các hệ thống giảm thiểu tự động, đặc biệt là trong môi trường sản xuất không hỗ trợ tỷ lệ lấy mẫu cao hoặc trình phát hiện tốn kém về mặt tính toán để thực hiện trong thời gian thực khi số lượng quá trình đồng thời tăng lên.

Trong nghiên cứu này, nhóm tác giả đề xuất xây dựng hệ thống hoạt động như một cảm biến có thể được cài đặt ở bất kỳ đâu trên mạng và phân loại lưu lượng truy cập trực tuyến bằng chiến lược dựa trên các thuật toán học máy (Machine Learning) giúp phân loại các mẫu lưu lượng ngẫu nhiên được thu thập trên các thiết bị mạng thông qua giao thức truyền phát. Phương pháp đề xuất tương thích với cơ sở hạ tầng Internet và không yêu cầu nâng cấp phần mềm hoặc phần cứng [12]. Bên cạnh đó, quyền riêng tư dữ liệu của người dùng được đảm bảo ở tất cả các giai đoạn vận hành hệ thống. Hệ thống đề xuất sử dụng các kỹ thuật về học máy cơ bản để phát hiện xâm nhập bất thường mạng (DDoS) và các kỹ thuật giảm chiều dữ liệu để loại bỏ các đặc trưng không có nhiều ý nghĩa trong việc phát hiện bất thường. Mục tiêu chính của hệ thống đề xuất là giảm thời gian tính toán giúp phát hiện sớm tấn công nhưng vẫn đảm bảo độ chính xác của việc phát hiện bất thường.

2. Cơ sở nghiên cứu và ứng dụng

2.1. Các thuật toán học máy

Các thuật toán học máy có thể ứng dụng trong việc phát hiện tấn công DDoS hoặc dùng trong một số hệ thống phát hiện xâm nhập như [3]-[11]: Thuật toán ***K-nearest neighbor (KNN)*** là một trong những thuật toán học có giám sát (Supervised-Learning) đơn giản nhất (mà hiệu quả trong một vài trường hợp) trong học máy. Khi huấn luyện (training), thuật toán này không học một điều gì từ dữ liệu training (đây cũng là lý do thuật toán này được xếp vào loại máy lười học/Lazy Learning), mọi tính toán được thực hiện khi nó cần dự đoán kết quả của dữ liệu mới. K-nearest neighbor có thể áp dụng được vào cả hai loại của bài toán Supervised learning là Classification (phân loại) và Regression (hồi quy về các giá trị). Thuật toán ***Random Forests (RF)*** là một phương pháp Supervised Learning do vậy có thể xử lý được các bài toán về Classification (phân loại) và Regression (dự báo về các giá trị). Về cơ bản thì Random forests là phương pháp xây dựng một tập hợp rất nhiều cây quyết định (Decision Tree) và sử dụng phương pháp bầu chọn để đưa ra quyết định về biến mục tiêu (target) cần được dự báo. Số lượng cây quyết định trong RF được khống chế theo mong muốn của người sử dụng nó. Thuật toán ***AdaBoost*** liên quan đến việc sử dụng các cây quyết định rất ngắn (một cấp), được gọi là decision stumps như những weak learner được thêm liên tục vào nhóm. Mỗi mô hình tiếp theo cố gắng sửa các dự đoán được thực

hiện bởi mô hình trước khi nó trong chuỗi. Từ đó kết quả thu được sẽ là kết quả tốt nhất có thể; Thuật toán ***Support Vector Machine (SVM)*** là một phương pháp học có giám sát trong các mô hình nhận dạng mẫu. Nó không chỉ hoạt động tốt với các dữ liệu được phân tách tuyến tính mà còn tốt với cả dữ liệu phân tách phi tuyến.

2.2. Một số kỹ thuật giảm chiều dữ liệu

2.2.1. Kỹ thuật Principal Component Analysis (PCA)

PCA là một thuật toán thống kê sử dụng phép biến đổi trực giao để biến đổi một tập hợp dữ liệu từ một không gian nhiều chiều sang một không gian mới ít chiều hơn nhằm tối ưu hóa việc thể hiện sự biến thiên của dữ liệu. Phép biến đổi tạo ra những ưu điểm sau đối với dữ liệu:

- Giảm số chiều của không gian chứa dữ liệu khi nó có số chiều lớn.
- Xây dựng những trục tọa độ mới, có khả năng biểu diễn dữ liệu tốt tương đương, và đảm bảo độ biến thiên của dữ liệu trên mỗi chiều mới.
- Tạo điều kiện để các liên kết tiềm ẩn của dữ liệu có thể được khám phá trong không gian mới, mà nếu đặt trong không gian cũ thì khó phát hiện vì những liên kết này không thể hiện rõ.
- Đảm bảo các trục tọa độ trong không gian mới luôn trực giao đôi một với nhau, mặc dù trong không gian ban đầu các trục có thể không trực giao.

2.2.2. Kỹ thuật Feature Importance

Feature Importance đề cập đến các kỹ thuật gán điểm (chỉ số "importance") cho các đặc trưng đầu vào dựa trên mức độ hữu ích của chúng trong việc dự đoán một giá trị mục tiêu. Chỉ số "importance" rất hữu ích và có thể được sử dụng trong một loạt các tình huống trong một vấn đề mô hình dự đoán, chẳng hạn như:

- Hiểu rõ hơn về dữ liệu; Hiểu rõ hơn về một mô hình.
- Giảm số lượng các đặc trưng đầu vào: Điều này có thể đạt được bằng cách sử dụng chỉ số "*importance*" để chọn các đặc trưng cần xóa ("importance" thấp) hoặc các đặc trưng cần giữ ("importance" cao). Đây là một loại lựa chọn đặc trưng và có thể đơn giản hóa vấn đề đang được mô hình hóa, tăng tốc quá trình mô hình hóa (xóa các đặc trưng được gọi là giảm kích thước) và trong một số trường hợp, cải thiện hiệu suất của mô hình.

2.2.3. Kỹ thuật Univariate Selection

Univariate Selection kiểm tra từng đặc trưng riêng lẻ để xác định độ mạnh của mối quan hệ giữa đặc trưng với giá trị trả lời. Các phương pháp này đơn giản để thực hiện và khá tốt để có được sự hiểu biết tốt hơn về dữ liệu, tìm ra được đặc trưng nào có quan hệ tốt cho việc tìm ra giá trị trả lời. Sau đó, giữ lại số lượng các đặc trưng mong muốn để làm đặc trưng đầu vào cho một mô hình dự đoán.

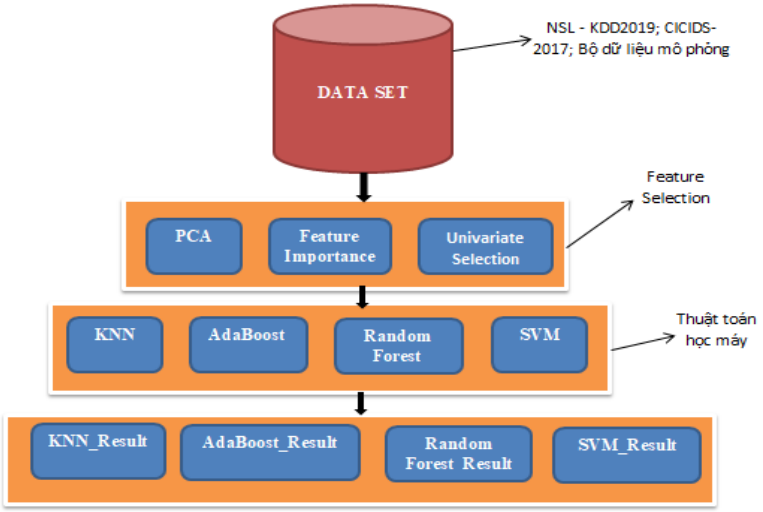
2.3. Phát biểu bài toán và ứng dụng

Với cơ sở lý thuyết về các thuật toán học máy cơ bản và kỹ thuật giảm chiều dữ liệu, chúng ta có thể áp dụng vào hệ thống phát hiện xâm nhập mạng dựa trên bất thường. Hệ thống đề xuất [12]:

- Sử dụng phương pháp Rescaling sử dụng MiMaxScaler có sẵn trong thư viện sklearn.
- Sử dụng các kỹ thuật giảm chiều dữ liệu xử lý các dữ liệu đầu vào.
- Sử dụng các giải thuật học máy để phát hiện các cuộc tấn công nhờ vào khả năng phân loại của chúng.

Hệ thống phát hiện xâm nhập mạng IDS đề xuất là một hệ thống lai có đặc điểm:

- Bộ dữ liệu chữ ký Signature Dataset (SDS): phát hiện xâm nhập dựa trên chữ ký.
- Sử dụng kỹ thuật Recursive Feature Elimination with Cross Validation để lựa chọn các đặc trưng quan trọng, sau đó huấn luyện qua thuật toán Random Forest.



Hình 1. *Mô hình phát hiện tấn công sử dụng kết hợp giải thuật học máy và kỹ thuật giảm chiều dữ liệu*

Chi tiết mô hình thực hiện như trong hình 1 như sau:

▪ ***Khối lựa chọn đặc trưng***: Sau khi nhận được dữ liệu, khối chức năng này tập trung sử dụng ba kỹ thuật lựa chọn đặc trưng khác nhau PCA, Feature Importance (Sử dụng Extra tree và SelectFromModel của thư viện scikit-learn), Univariate Selection (Sử dụng SelectKBest với thuật toán chi-squared). Trong đó:

✓ ***PCA:*** tính toán lại mối quan hệ giữa các đặc trưng và giảm số chiều dữ liệu về số lượng mà chúng ta mong muốn. Để tìm ra được số chiều phù hợp thì cần thử nghiệm nhiều lần.

✓ ***Feature Importance và Univariate Selection:*** tuy có cách đánh giá đặc trưng khác nhau nhưng hai kỹ thuật này đều tính "điểm" cho từng đặc trưng và sau đó giữ lại những đặc trưng có "điểm" cao hơn ngưỡng đặt ra.

▪ ***Khối học máy:*** sau khi xử lý giảm chiều dữ liệu với các kỹ thuật trên, ta nhận được bộ dữ liệu mới với số chiều nhỏ hơn số chiều của dữ liệu ban đầu. Huấn luyện bộ dữ liệu này lần lượt với từng giải thuật học máy (KNN, AdaBoost, Random Forest, SVM) để phân loại được lưu lượng tấn công và lưu lượng bình thường.

- Hệ thống đề xuất đem lại một số ưu điểm như sau:

✓ Kết hợp kỹ thuật giảm chiều dữ liệu giúp tăng tốc độ xử lý sao cho phù hợp, đảm bảo được độ chính xác khi phát hiện các lưu lượng bất thường.

✓ Khi giảm chiều dữ liệu đầu vào cho các thuật toán, thời gian tính toán của các giải thuật có thể giảm đi, tăng khả năng phát hiện ra bất thường sớm, tăng hiệu năng phòng chống tấn công DDoS.

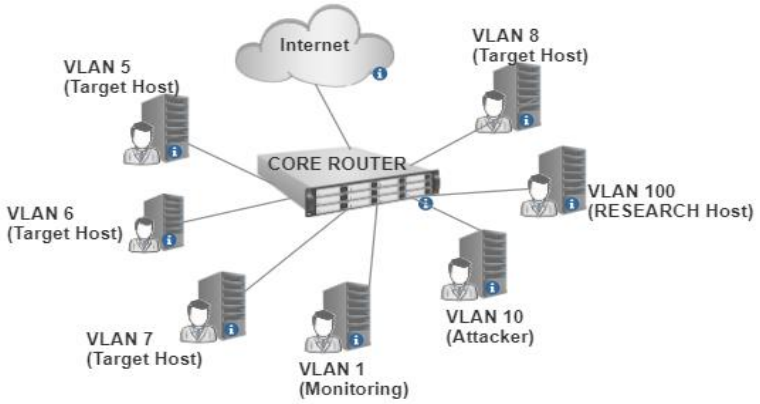
✓ Với các kỹ thuật trích chọn đặc trưng như Feature Importance và Univariate Selection, sau khi tìm được các đặc trưng phù hợp để giữ lại thì những đặc trưng dư thừa khác có thể bỏ đi. Điều này giúp cho việc giám sát lưu lượng mạng đạt hiệu quả hơn, chỉ cần theo dõi và thiết lập luật bắt các đặc trưng cần thiết khi có một lưu lượng mới đi vào hệ thống. Không cần giám sát toàn bộ những đặc trưng của lưu lượng, từ đó giảm thiểu được độ lớn dữ liệu đầu vào cho hệ thống phát hiện tấn công.

3. Triển khai đánh giá trên bộ dữ liệu mạng mô phỏng

3.1. Bộ dữ liệu

Về bộ dữ liệu sử dụng huấn luyện: bộ dữ liệu được tự tạo ra theo như mô hình mạng hình 2. VLAN 5, 6, 7 và 8 được sử dụng làm các máy nạn nhân. VLAN 100 dành riêng cho người dùng của một đơn vị học thuật. VLAN 10 được sử dụng làm máy chủ tấn công, giám sát tại VLAN 1. Tất cả các mạng đều có quyền truy cập thường xuyên vào Internet. Kế hoạch tấn công cứ sau 30

phút lại tạo ra một cuộc tấn công, 48 sự kiện tấn công trong 24 giờ, bắt đầu từ 00h00m00s và kết thúc ở 23h59m00s. Tất cả các cuộc tấn công đã được thực hiện bởi máy chủ tấn công (thuộc VLAN 10), trong thời gian đó nó không truyền lưu lượng truy cập hợp pháp cho các nạn nhân. Các công cụ tấn công được tham số hóa để tạo ra chế độ sneaky low-volume, medium-volume hoặc light mode, và massive high-volume attacks. Bộ dữ liệu ban đầu gồm 73 đặc trưng cho một bản ghi, và được gán nhãn là "normal" và "attack" rõ ràng.



Hình 2. *Cấu trúc mạng xây dựng bộ dữ liệu*

Bộ dữ liệu này được xây dựng khá gần với một môi trường mạng hoạt động trong thực tế. Từ đó, sử dụng bộ dữ liệu này để kiểm thử với mô hình đề xuất sẽ giúp ta đánh giá được sự hiệu quả của hệ thống. Nhưng bộ dữ liệu này chưa đủ lớn, bao gồm 45500 bản ghi (trong đó có 22412 tấn công và 23088 bản ghi bình thường). Đây là cơ sở để tham khảo và xây dựng một bộ dữ liệu lớn hơn để có thể phát triển hệ thống sau này [13] – [17].

3.2. Đánh giá kết quả thu được

Các kết quả thu được là giá trị trung bình sau 15 lần huấn luyện và kiểm thử.

3.2.1. Sau khi thực hiện giảm chiều dữ liệu sử dụng PCA

Bảng 1. *Kết quả kiểm thử trên bộ dữ liệu mô phỏng với giảm chiều sử dụng PCA*

Thuật toán	Độ chính xác ban đầu (%)	Độ chính xác sau khi giảm chiều dữ liệu (%)	Thời gian thực thi ban đầu (ms)	Thời gian thực thi sau khi giảm chiều dữ liệu (ms)
KNN	99,91	99,89	6850,37	1428,85
AdaBoost	99,92	99,92	536,28	964,01
Random Forest	99,85	99,83	4121,91	6626,19
SVM	99,85	99,91	997,18	907,55

Phần tính toán thời gian sau khi giảm chiều dữ liệu đã tính cả thời gian xử lý với kỹ thuật PCA. Bởi bản chất của kỹ thuật này là tính toán lại quan hệ giữa các đặc trưng để chuyển từ không gian nhiều chiều về ít chiều dữ liệu hơn. Vì vậy, mỗi lần có một lưu lượng mạng đi qua thì hệ thống cần thay đổi chiều dữ liệu của lưu lượng đó, sau đó phân tích xem lưu lượng là hợp lệ hay tấn công. Theo quan sát như trong Bảng 1 ta nhận thấy, ngoại trừ thuật toán Random Forest và AdaBoost có thời gian thực thi tăng lên tương đối nhiều, còn lại thời gian thực thi đều giảm tương đối mạnh. Nguyên nhân do PCA đã chuyển bộ dữ liệu thành một bộ dữ liệu mới làm cho cấu trúc các cây mới được xây dựng khác với cây ban đầu. Nhìn chung thì độ chính xác sẽ giảm đi sau khi giảm chiều dữ liệu. Nhưng việc giảm đi này là có thể chấp nhận được so với thời gian thực thi. Nhận thấy thuật toán KNN rất phù hợp với bộ dữ liệu huấn luyện này bởi sau khi được

huấn luyện bởi bộ dữ liệu đã giảm chiều dữ liệu thì thời gian thực hiện nhanh hơn hẳn và vẫn cho ra được hệ thống có độ chính xác tương đối cao.

3.2.2. Sau khi thực hiện giảm chiều dữ liệu sử dụng Feature Importance

Thực hiện giảm chiều dữ liệu với kỹ thuật Feature Importance sử dụng Extra Tree để tính toán Importance của từng đặc trưng sau đó sử dụng thuật toán SelectFromModel để lựa chọn các đặc trưng thỏa mãn điều kiện người dùng thiết lập. Thực hiện giảm chiều dữ liệu nên loại bỏ được 53 đặc trưng, chỉ còn 20 đặc trưng được sử dụng. Đặc trưng còn lại sau khi sử dụng Feature Importance*: 'tcp_dataofs_median', 'tcp_dataofs_mean', 'tcp_flags_mean', 'ip_proto', 'ip_ttl_cv', 'tcp_flags_rte', 'ip_len_std', 'ip_ttl_std', 'tcp_flags_median', 'ip_len_entropy', 'sport_entropy', 'tcp_seq_mean', 'tcp_dataofs_rte', 'ip_len_cv', 'ip_ttl_cvq', 'tcp_ack_entropy', 'tcp_flags_cv', 'tcp_seq_entropy', 'tcp_ack_cvq', 'ip_len_mean'.*

Bảng 2. *Kết quả kiểm thử trên bộ dữ liệu mô phỏng với giảm chiều sử dụng Feature Importance*

Thuật toán	Độ chính xác ban đầu (%)	Độ chính xác sau khi giảm chiều dữ liệu (%)	Thời gian thực thi ban đầu (ms)	Thời gian thực thi sau khi giảm chiều dữ liệu (ms)
KNN	99,86	99,81	6166,43	808,75
AdaBoost	99,87	99,89	527,46	131,59
Random Forest	99,99	99,93	4123,88	1894,85
SVM	99,82	99,79	1017,15	389,93

Theo quan sát trong Bảng 2 ta nhận thấy, kết quả thu được là rất khả quan. Độ chính xác của từng mô hình chỉ giảm nhẹ nhưng thời gian thực hiện của mô hình lại giảm mạnh. Ngoài ra, khi sử dụng kỹ thuật Feature Importance, ta thu được kết quả chỉ còn lại 20 đặc trưng được sử dụng. Từ đó, khi quản trị hệ thống IDS, người quản trị chỉ cần thiết lập luật sao cho chỉ cần lấy đúng 20 đặc trưng trên cho một luồng dữ liệu đi vào, giảm thời gian lấy mẫu dữ liệu, tăng tốc độ xử lý cho cả hệ thống. Phương pháp giảm chiều dữ liệu giúp cho mô hình phát hiện xâm nhập mạng áp dụng các thuật toán học máy cơ bản đạt được mục tiêu đề ra của nghiên cứu. Thời gian thực thi càng ngắn thì càng sớm phát hiện được tấn công, đảm bảo được độ chính xác khi phân loại tấn công.

3.2.3. Sau khi thực hiện giảm chiều dữ liệu sử dụng Univariate Selection

Thực hiện giảm chiều dữ liệu với kỹ thuật Univariate Selection sử dụng thuật toán chi-squared để tính toán chi bình phương cho từng đặc trưng trong bộ dữ liệu và sắp xếp chúng theo thứ tự giảm dần. Sau đó thiết lập tham số đặc trưng muốn giữ lại cho SelectKBest, các đặc trưng được lấy từ cao xuống thấp theo chỉ số chi bình phương đã tính cho đến khi đủ. Thực hiện giảm chiều dữ liệu bằng phương pháp trên loại bỏ 53 đặc trưng, chỉ còn 20 đặc trưng được sử dụng. Đặc trưng còn lại sau khi sử dụng Univariate Selection: *'ip_ttl_cv', 'ip_len_cv', 'ip_len_cvq', 'ip_ttl_cvq', 'tcp_ack_rte', 'tcp_seq_cvq', 'tcp_seq_rte', 'tcp_dataofs_median', 'tcp_dataofs_mean', 'tcp_window_median', 'dport_cv', 'tcp_window_mean', 'tcp_flags_mean', 'tcp_flags_median', 'tcp_ack_cvq', 'tcp_seq_mean', 'tcp_seq_median', 'tcp_seq_cv', 'ip_ttl_std', 'ip_len_std'.*

Bảng 3. *Kết quả kiểm thử trên bộ dữ liệu mô phỏng với giảm chiều sử dụng Univariate Selection*

Thuật toán	Độ chính xác ban đầu (%)	Độ chính xác sau khi giảm chiều dữ liệu (%)	Thời gian thực thi ban đầu (ms)	Thời gian thực thi sau khi giảm chiều dữ liệu (ms)
KNN	99,84	99,87	6765,63	1434,09
AdaBoost	99,93	99,91	443,72	174,44
Random Forest	99,88	99,86	4077,38	2441,35
SVM	99,92	99,90	1047,19	303,09

Theo quan sát trong Bảng 3 ta nhận thấy, kết quả thu được là rất khả quan. Độ chính xác của mô hình giảm nhẹ nhưng thời gian thực hiện mô hình lại giảm mạnh. Ngoài ra, khi sử dụng kỹ thuật Feature Importance, ta thu được kết quả chỉ còn lại 20 đặc trưng được sử dụng. Từ đó, khi quản trị hệ thống IDS, người quản trị chỉ cần thiết lập luật sao cho chỉ cần lấy đúng 20 đặc trưng trên cho một luồng dữ liệu đi vào, giảm thời gian lấy mẫu dữ liệu, tăng tốc độ xử lý cho cả hệ thống.

4. Kết luận

Với bộ dữ liệu chỉ có hai nhãn dán là bình thường và tấn công, bộ dữ liệu mô phỏng trong bài báo này thì các mô hình đề xuất đều đem lại kết quả tốt. Đảm bảo việc phát hiện xâm nhập mạng kịp thời (thời gian phân loại tấn công và lưu lượng thường nhanh) nhưng vẫn cho ra được độ chính xác của hệ thống tương đối cao. Hệ thống đưa ra phân loại lưu lượng thường tương đối chính xác, nhưng khi đánh giá độ chính xác khi phân loại từng loại tấn công cụ thể thì độ chính xác thấp, đưa ra các cảnh báo sai. Hệ thống đề xuất phù hợp với các bộ dữ liệu được đánh nhãn để phân loại giữa lưu lượng tấn công và lưu lượng thường. Hai mô hình sử dụng KNN và Random Forest kết hợp với các kỹ thuật giảm chiều dữ liệu đều cho kết quả tốt về cả độ chính xác và thời gian thực hiện. Tổng hợp tất cả các kết quả thu được, ta thấy hệ thống đề xuất đạt kết quả tốt nhất trên cả ba bộ dữ liệu là việc kết hợp giữa giải thuật KNN và kỹ thuật giảm chiều dữ liệu Feature Importance. Sau khi tính toán và trả về số lượng đặc trưng quan trọng trong việc phát hiện tấn công bởi kỹ thuật Importance thì hiệu năng của giải thuật KNN được cải thiện. Vì chỉ giữ lại các đặc trưng quan trọng, số chiều dữ liệu càng giảm thì khả năng tính toán của KNN càng nhanh. Vì vậy, tuy độ chính xác có giảm nhẹ nhưng thời gian tính toán thì giảm đi rất nhiều. Điều này là có thể chấp nhận được.

TÀI LIỆU THAM KHẢO/ REFERENCES

[1] Y. Cao, "Understanding Internet DDoS Mitigation from Academic and Industrial Perspectives," *IEEE Acess*, vol. 6, pp. 66641-66648, 2018.

[2] B. Sunny, "D-FACE: An anomaly based distributed approach for early detection of DDoS attacks," *Journal of Network and Computer Applications*, vol. 111, pp. 49-63, 2018.

[3] H. HadianJazi, "Detecting HTTP-based application layer DoS attacks on web servers in the presence of sampling," *Journal of Computer Networks*, vol. 121, pp. 25-36, 2017.

[4] N. Muraleedharan and B. Janet, "A deep learning based HTTP slow DoS classification approach using flow data," *ICT Express*, vol. 7, no. 2, pp. 210-214, 2021.

[5] Y. Zhen, "A systematic literature review of methods and datasets for anomaly-based network intrusion detection," *Journal of Computers & Security*, vol. 116C, pp. 1-10, 2022.

[6] E. Alhajjar, "Adversarial machine learning in Network Intrusion Detection Systems," *Expert Systems with Applications*, vol. 186, pp. 1-10, 2021.

[7] Y. Gu, "Multiple-Features-Based Semisupervised Clustering DDoS Detection Method," *Mathematical Problems in Engineering*, vol. 2017, pp. 1-10, 2017.

[8] K. Saravanan, "Detection mechanism for distributed denial of service (DDoS) attacks for anomaly detection system," *Journal of Theoretical and Applied information Technology*, vol. 60, pp. 174-178, 2014.

[9] Y. Liao and R. V. Vemuri, "Use of K-Nearest Neighbor classifier for intrusion detection," *Computers & Security*, vol. 21, no. 5, pp. 439-448, 2002.

[10] M. Aamir and S. M. A. Zaidi, "Clustering based semi-supervised machine learning for DDoS attack classification," *Journal of King Saud University - Computer and Information Sciences*, vol. 33, no. 4, pp. 436-446, 2021.

[11] F. A. F. Silveira, A. M. B. Junior, G. V. Solar, and L. F. Silveira, "Smart Detection: An Online Approach for DoS/DDoS Attack," *Security and Communication Networks*, vol. 2019, pp. 1-15, 2019.

[12] J. Long, "TR-IDS: Anomaly-Based Intrusion Detection through Text-Convolutional Neural Network and Random Forest," *Security and Communication Networks*, vol. 2018, no. 1, pp. 1-9, 2018.

[13] A. Maraj, "Testing of network security systems through DoS attacks," in *Embedded Computing (MECO), 6th Mediterranean Conference on IEEE*, pp. 368-373, 2017.

[14] T. T. Tran and H. H. Le, "Study technique to limit bandwidth spending from DDoS attacks," *Dalat University Journal of Science*, vol. 7, pp. 52-61, 2020.
[15] H. H. Le, "Improve network security system in Vietnam using reverse method," *TNU Journal of Science and Technology*, vol. 225, no. 09, pp. 125-133, 2020.
[16] H. H. Le, "Study to applying Blockchain technology for preventing of spam email," *TNU - Journal of Science and Technology*, vol. 208, no. 15, pp. 161-167, 2019.
[17] H. H. Le, "Study the method of implementation of Border Gateway Protocol on IPv4 and IPv6 infrastructure by analysis and evaluate of some properties affecting protocol performance," *TNU Journal of Science and Technology*, vol. 226, no. 11, pp. 149-157, 2021.