GIẢM THIỂU TẤN CÔNG DOS/DDOS SỬ DỤNG KỸ THUẬT NEURAL NETWORKS KẾT HỢP ADAM

MITIGATE DOS/DDOS ATTACK USING ADAM COMBINED NEURAL NETWORK TECHNIQUE

Lê Linh Sơn
[1]Khoa Công nghệ thông tin, Thành phố Hồ chí Minh, Việt Nam, sonll20@uef.edu.vn

***Tóm tắt**: Trong thời đại nền công nghiệp 4.0 như hiện nay, thời đại của internet, dữ liệu số và trí tuệ nhân tạo, ngày càng nhiều công nghệ mới ra đời dẫn đến các cuộc tấn công mạng bằng nhiều cách thức khác nhau cũng ngày một tăng lên. Một trong số những phương pháp tấn công lâu đời nhưng vẫn còn tồn tại và ngày càng phức tạp và tinh vi hơn đó là phương pháp tấn công DOS (Denial of Service) và DDOS (Distributed Denial of Service). Trong bài báo này, chúng tôi sử dụng thuật toán máy học Neural Networks và thuật toán tối ưu học máy Adam để phân loại lưu lượng mạng và phát hiện các biểu hiện của tấn công DDoS, chúng tôi tiến hành các thử nghiệm và đánh giá hiệu suất của các mô hình máy học trên bộ dữ liệu và đạt được độ chính xác khả quan là 98,6%.*

***Từ khóa**: Máy học, tấn công mạng, từ chối dịch vụ,*

***Abstract**: In the current era of industry 4.0, the era of the internet, digital data and artificial intelligence, more and more new technologies are being born, leading to an increase in cyber attacks in many different ways. go up. One of the oldest attack methods that still exists and is increasingly more complex and sophisticated is the DOS (Denial of Service) and DDOS (Distributed Denial of Service) attack methods. In this article, we use Neural Networks machine learning algorithm and Adam machine learning optimization algorithm to classify network traffic and detect manifestations of DDoS attacks, we conduct experiments and evaluations. performance of the machine learning models on the dataset and achieved a satisfactory accuracy of 98.6%.*

***Keywords**: Cybersecurity, DoS, DDoS, machine learning,*

1. Giới thiệu

Trong thời đại kết nối vạn vật như hiện nay, mạng lưới internet đóng vai trò quan trọng, chẳng còn là một phần mở rộng của cuộc sống, mà còn là cột mốc đánh dấu sự tiến bộ và kết nối toàn cầu. Cùng với những lợi ích đáng kể mà internet mang lại, xuất phát từ sự thuận tiện trong giao tiếp đến khả năng tiếp cận thông tin, nó cũng mở ra những thách thức đầy thách thức liên quan đến an ninh mạng. Trong môi trường mạng ngày nay, tấn công DDoS không chỉ là một hiện tượng cơ bản mà đã trở thành một đe dọa nguy hiểm, đặt ra những thách thức đối với sự liên tục và an toàn của hệ thống. Khả năng của nó để tạo ra làn sóng lưu lượng giả mạo và tấn công từ nhiều nguồn đồng thời, khiến cho nguồn tài nguyên của hệ thống bị quá tải và dẫn đến sự cố truy cập, đã đặt ra mối đe dọa không lường trước được đối với các tổ chức và doanh nghiệp [1].

Theo thống kê được đăng trên trang "stormwall.network","instagalleryapp.com" số vụ tấn công DDoS vào quý 1 năm 2023 đã tăng hơn 28% so với năm 2022, các cuộc tấn công lớp cơ sở hạ tầng tăng 16%, các cuộc tấn công dựa trên sự phản chiếu tăng 4% và các cuộc tấn công ở tầng ứng dụng tăng 38%. Trong năm 2023 cũng đã ghi nhận cuộc tấn công DDoS dài nhất tính từ 2015 đến nay xảy ra vào quý 4 năm 2023 và kéo dài trong 329 giờ, tức là gần 2 tuần. Dự kiến các vụ tấn công DDOS sẽ có xu hướng tăng trong năm 2024 [2].

Trong nhiều năm qua, các thuật toán học máy với khả năng học từ dữ liệu và nhận biết các mô hình phức tạp, có tiềm năng đặc biệt để phát hiện những biểu hiện tiền đề của tấn công DDoS. Sự linh hoạt và khả năng thích ứng của máy học giúp nhanh chóng nhận diện các mô hình tấn công mới mà không cần phải cập nhật thủ công [3]. Trong bài báo này, chúng tôi sử

dụng kỹ thuật Neural Network kết hợp với Adam để phát hiện các dấu hiệu của tấn công DoS, DDoS nhằm đảm bảo hệ thống mạng tránh khỏi các đợt tấn công. Phần còn lại được trình bày như sau: Phần 2 trình bày các nghiên cứu liên quan, mô hình và phương pháp đề xuất được trình bày trong phần 3. Phần 4 trình bày và phân tích két quả thực nghiệm. Cuối cùng, phần 5 tổng kết các vấn đề của đề tài và trình bày hướng phát triển trong tương lai.

2. Các công trình liên quan

Sambangi S và cộng sự (2020) [4] đã nghiên cứu vấn đề phát hiện tấn công DDoS trong môi trường Cloud bằng cách xem xét bộ dữ liệu điểm chuẩn CICIDS 2017 phổ biến nhất và áp dụng nhiều phân tích hồi quy để xây dựng mô hình học máy để dự đoán các cuộc tấn công DDoS và Bot thông qua việc xem xét nhật ký lưu lượng truy cập. Nhóm tác giả áp dụng kỹ thuật lựa chọn tính năng và xác định các thuộc tính quan trọng cho mô hình dự đoán. Họ sử dụng bộ dữ liệu nhật ký với 225746 gói lưu lượng, kết quả thực nghiệm có độ chính xác 73,79%.

Ali TE và cộng sự (2023) [5] đã sử dụng phương pháp (ML/DL)[1] để xác định các cuộc tấn công DDoS trong mạng SDN [2]từ năm 2018 đến đầu tháng 11 năm 2022. Họ đã phân tích các nghiên cứu liên quan và phân loại kết quả của SLR [3]thành 4 lĩnh vực: (1) Các loại phát hiện tấn công DDoS khác nhau trong các phương pháp ML/DL; (2) các phương pháp, điểm mạnh và điểm yếu của các phương pháp ML/DL hiện có để phát hiện các cuộc tấn công DDoS; (3) các bộ dữ liệu được chuẩn hóa và các lớp tấn công trong các bộ dữ liệu được sử dụng trong các tài liệu hiện có; (4) các chiến lược tiền xử lý, giá trị siêu tham số, thiết lập thử nghiệm và số liệu hiệu suất được sử dụng trong tài liệu hiện có; Nhóm tác giả sử dụng kỹ thuật CNN[4], DNN [5]và CNN-LSTM [6]để thực nghiệm trên bộ dữ liệu CICIDS2017 và kết quả có độ chính xác đạt 99%.

Islam U và cộng sự (2022) [6] đã áp dụng các kỹ thuật học máy như: SVM[7], KNN [8]và RF [9]để phát hiện các cuộc tấn công DDoS. Kết quả thực nghiệm của tác giả lần lượt tương với các thuật toán trên là: 99.5%, 97.5% và 98.7%. Có thể thấy thuật toán SVM đạt độ chính xác cao nhất trong các thuật toán.

Qua các công trình trên, chúng tôi có một sô nhận xét và sau dó đưa ra phương pháp đề xuất nhằm cải thiện các nhược điểm của các thuật toán. Bảng 1 thể hiện chi tiết các ưu và nhược điểm của các thuật toán.

***Bảng 1**. So sánh ưu điểm nhược điểm của các thuật toán*

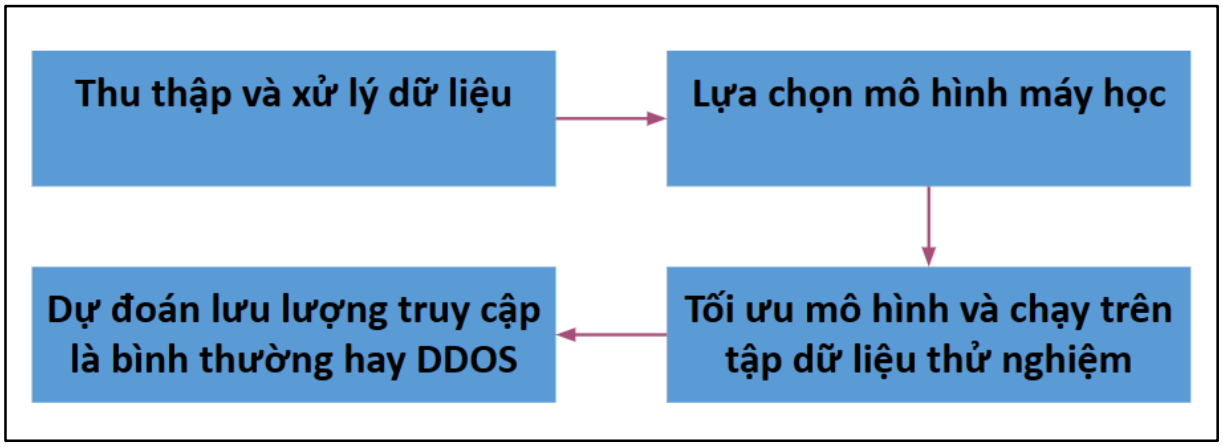
Thuật toán	Ưu điểm	Nhược điểm
KNN	Đơn giản và dễ hiểu. Hiệu suất tốt đối với dữ liệu có cấu trúc đơn giản.	Nhạy cảm với nhiễu và chiều cao của dữ liệu. Hiệu suất kém khi số chiều của dữ liệu lớn.
SVM	Hoạt động hiệu quat trong không gian có số chiều lớn. Tạo ra các đường phân loại chính xác và tổng quát. Có thể mở rộng để hỗ trợ phân loại đa lớp	Nhạy cảm với nhiều và yêu cầu một lượng dữ liệu đủ lớn để hoạt động hiệu quả. Khó khăn khi xử lý dữ liệu không cân bằng, nơi số lượng mẫu của các lớp khác nhau không đồng đều

[1] ML/DL: Machine learning/ Deep Learning
[2] SDN : Software-Defined Networking
[3] SLR : Simple Linear Regression
[4] CNN: Convolutional Neural Network
[5] DNN: Deep Neural Network
[6] CNN-LSTM: Convolutional Neural Network - Long Short-Term Memory
[7] SVM: Support Vector Machine
[8] KNN: K-Nearest Neighbors
[9] RF: Random Forest

FR	Hoạt động hiệu quả trên dữ liệu có đa dạng đặc trưng và lớn Dễ triển khai và có khả năng xử lý dữ liệu không cân bằng	Khó giải thích so với cây quyết định đơn lẻ. Với việc mở rộng hơn từ DT thì RF cần thêm tài nguyên tính toán hơn.
NN	Hiệu suất tốt trên dữ liệu lớn và phức tạp. Có thể học các biểu diễn phức tạp của dữ liệu	Hiệu suất tốt trên dữ liệu lớn và phức tạp. Có thể học các biểu diễn phức tạp của dữ liệu

3. Phương pháp đề xuất

3.1. Mô hình



Hình 1. *Mô hình phát hiện tấn công DDOS bằng máy học*

Bước 1: Chúng tôi tiến hành thu thập dữ liệu gồm lưu lượng truy cập bình thường và lưu lượng là DDOS sau đó chia dữ liệu thành hai tập bao gồm tập huấn luyện và tập thử nghiệm. Sau khi có bộ dữ liệu chúng tôi tiến hành xử lý loại bỏ các đặc trưng không cần thiết, chuẩn hóa dữ liệu, giảm nhiễu và dán nhãn cho dữ liệu là bình thường (1) hay DDOS (-1).

Bước 2: Tiếp đến chúng tôi sử dụng các mô hình máy học như KNN, SVM, RF, NN để thực nghiệm độ chính xác, sau đó chọn ra mô hình tối ưu nhất với độ chính xác cao nhất.

Bước 3: Sau khi lựa chọn được mô hình máy học phù hợp chúng tôi tiếp tục tối ưu nó bằng các thuật toán tối ưu học máy như Adam và triển khai huấn liệu trên tập dữ liệu huấn luyện và lưu lại mô hình huấn luyện.

Bước 4: Tiến hành chạy thực nghiệm trên tập dữ liệu thử nghiệm (test data) và đưa ra dự đoán đây là truy cập bình thường hay là truy cập dạng tấn công DDOS.

Mô hình Neural Network (NN) là một phương pháp học máy được lấy cảm hứng từ cách hoạt động của não người. Một NN bao gồm một hoặc nhiều lớp (layers) của các nơ-ron (neurons), mỗi lớp kết nối với lớp liền kề bằng các trọng số.

NN có khả năng học được biểu diễn phức tạp và tổng quát hóa tốt trên dữ liệu mới. Đối với các mô hình lớn, đòi hỏi lượng dữ liệu lớn để tránh overfitting. NN có nhiều siêu tham số để điều chỉnh, bao gồm số lượng lớp, số lượng nơ-ron trong mỗi lớp, hàm kích hoạt, và tốc độ học. Neural Network đã chứng minh sức mạnh của mình trong nhiều ứng dụng, bao gồm nhận dạng hình ảnh, xử lý ngôn ngữ tự nhiên, và nhiều bài toán học máy khác.

Thuật toán tối ưu hóa Adam (Adaptive Moment Estimation) là một trong những thuật toán tối ưu hóa phổ biến được sử dụng trong đào tạo mô hình máy học và học sâu. Nó kết hợp các ưu điểm của hai thuật toán khác là RMSprop (Root Mean Square Propagation) và Momentum để cải thiện tốc độ hội tụ và hiệu suất của quá trình đào tạo.

Momentums (Động lượng): Adam sử dụng động lượng để giữ định hướng của quá trình tối ưu hóa. Động lượng giúp giảm độ dao động và tăng tốc quá trình hội tụ. Adam tính toán giá trị động lượng bằng cách sử dụng thông tin từ gradient của các tham số trước đó.

RMSprop (Root Mean Square Propagation): Nó giúp điều chỉnh kích thước của bước cập nhật cho từng tham số dựa trên độ lớn của gradient tương ứng với tham số đó. Điều này giúp ổn định quá trình học bằng cách giảm độ dao động đối với các tham số có gradient lớn.

Adaptive Learning Rate: Adam sử dụng learning rate được điều chỉnh tự động cho từng tham số. Nó tính toán learning rate cụ thể cho từng tham số dựa trên giá trị kỳ vọng của bình phương gradient và động lượng.

Bias Correction: Adam thêm một bước điều chỉnh để hiệu chỉnh sự chệch của ước lượng đối với độ lớn của gradient và động lượng. Điều này giúp làm cho ước lượng đồng đều hơn và tăng tính chính xác của thuật toán.

3.2. **Bộ dữ liệu**

Chúng tôi sử dụng 2 bộ dữ liệu CICIDS2017 và CICDDoS2019 được cung cấp bởi trang Kaggle. Kaggle là một trang web nổi tiếng chuyên về khoa học dữ liệu và các cuộc thi máy học, đây cũng là một trong những trang cung cấp các bộ dữ liệu (data set) uy tín và được nhiều người tin dùng.
Dưới đây là thông tin của 2 bộ dữ liệu chúng tôi đã sử dụng trong dự án này:

CICIDS2017: Viện An ninh mạng Canada (CIC) đã sản xuất bộ dữ liệu này vào năm 2017. Các cuộc tấn công thực tế mới và các luồng điển hình đều được bao gồm. CICFlowMeter sử dụng dữ liệu từ các bản ghi, địa chỉ IP nguồn và đích, giao thức và các cuộc tấn công để đánh giá lưu lượng mạng. CICIDS2017 bao gồm các trường hợp tấn công điển hình như Tấn công vũ phu, Tấn công HeartBleed, Botnet, DoS phân tán (DDoS), Từ chối dịch vụ (DoS), Tấn công web và Tấn công xâm nhập.

CICDDoS2019: Sharafaldin et al. đả tạo bộ dữ liệu CICDDoS2019 (2019). Hơn 80 đặc điểm lưu lượng truy cập đã được lấy từ thông tin ban đầu bằng cách sử dụng chương trình CICFlowMeter-V3 để trích xuất các tính năng. CICDoS2019 chứa các cuộc tấn công DDoS điển hình an toàn và hiện tại. Tập dữ liệu này, được tạo bằng lưu lượng truy cập thực tế, chứa nhiều cuộc tấn công DDoS được tạo bằng giao thức TCP / UDP.

4. Kết quả thực nghiệm

Chúng tôi đánh giá kết quả thực nghiệm dựa trên các tiêu chí:

Accuracy (ACC) tính toán trực tiếp bằng cách chia số lượng dự đoán đúng cho số lượng tất cả các dự đoán.

$$ACC = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{TP} + \mathrm{TN} + \mathrm{FP} + \mathrm{FN}}$$

Precision là tỷ lệ các mẫu có liên quan trong số tất cả các mẫu được dự đoán thuộc về một lớp nhất định.

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

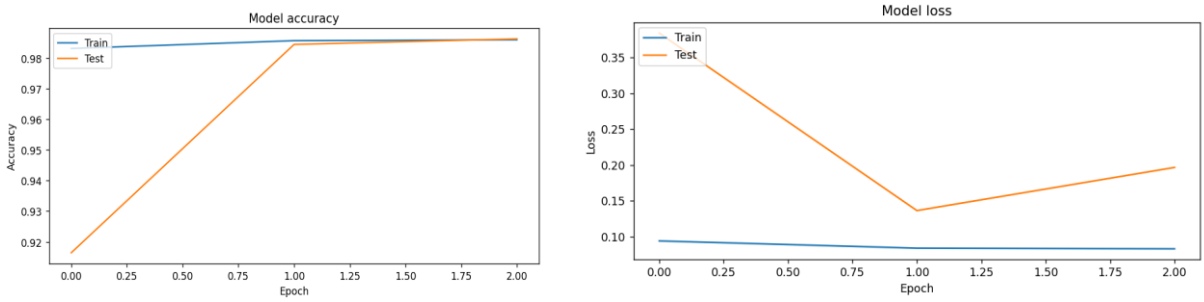
Giá trị Recall được định nghĩa là tỷ lệ các mẫu được dự đoán thuộc về một lớp so với tất cả cá mẫu thực sự thuộc về lớp đó.

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

Kết quả thực nghiệm cho thấy phương pháp đề xuất đạt độ chính xác lên đến 98.6% và độ mất mát (loss) là 0.15 - 0.4. Bảng 2 thể hiện chi tiết kết quả của thuật toán đề xuất:

Bảng 2. *Kết quả thực nghiệm*

Thuật toán	Accuracy	F1-Score	Recall	Precision
Phương pháp đề xuất test lần 1	98.60%	98.50%	98.63%	98.61%
Phương pháp đề xuất test lần 2	98.43%	98.15%	98.43%	97.46%
Phương pháp đề xuất test lần 3	98.58%	98.34%	98.58%	98.15%



Hình 2. *Đồ thị accuracy và loss của mô hình*

5. Kết luận

Trong bài báo này, chúng tôi đã đề xuất kỹ thuật kết hợp giữa thuật toán Neural kết hợp với Adam để phát hiện tấn công DDoS. Kết quả thực nghiệm cho thấy được tính khả thi và tính ổn định của phương pháp tiếp cận máy học trong việc đối phó với những thách thức bảo mật ngày càng phức tạp. Tạo ra tài liệu học thuật có ích cho các nghiên cứu về ứng dụng học máy, học kết hợp trong phát hiện tấn công DoS/DDoS.

Trong tương lai, chúng tôi sẽ cải tiến mô hình, thu thập thêm nhiều dữ liệu DDOS thực tế để mô hình có khả năng học tập được nhiều dữ liệu hơn góp phần làm tăng khả năng dự đoán chính xác của mô hình. Ngoài ra chúng tôi cũng sẽ tối ưu các thuật toán và quá trình dự đoán để giảm thời gian phát hiện DDOS của mô hình.

Tài liệu tham khảo

[1] Zlomislić, V., Fertalj, K., & Sruk, V. (2014). Denial of service attacks: An overview. In 2014 9th Iberian Conference on Information Systems and Technologies (CISTI) (pp. 1-6). Barcelona, Spain. doi: 10.1109/CISTI.2014.6876979.

[2] instagalleryapp.com. (n.d.). Sự kiện công nghệ: Số liệu thống kê và sự kiện cọng dột dựa trên thời gian. https://instagalleryapp.com/bo-mt-thong-tin/s-liu-thng-ke-va-s-kin-tn-cong-ddos-cho-nm

[3] Gniewkowski, M. (2020). An overview of DoS and DDoS attack detection techniques. In W. Zamojski, J. Mazurkiewicz, J. Sugier, T. Walkowiak, & J. Kacprzyk (Eds.), Theory and Applications of Dependable Computer Systems. DepCoS-RELCOMEX 2020 (Vol. 1173, Advances in Intelligent Systems and Computing). Springer. https://doi.org/10.1007/978-3-030-48256-5_23

[4] Sambangi, S., & Gondi, L. (2020). A machine learning approach for DDoS (Distributed Denial of Service) attack detection using multiple linear regression. Proceedings, 63(1), 51. https://doi.org/10.3390/proceedings2020063051

[5] Ali, T. E., Chong, Y.-W., & Manickam, S. (2023). Machine learning techniques to detect a DDoS attack in SDN: A systematic review. Applied Sciences, 13(5), 3183. https://doi.org/10.3390/app13053183

[6] Islam, U., Muhammad, A., Mansoor, R., Hossain, M. S., Ahmad, I., Eldin, E. T., Khan, J. A., Rehman, A. U., & Shafiq, M. (2022). Detection of distributed denial of service (DDoS) attacks in IoT based monitoring system of banking sector using machine learning models. Sustainability, 14(14), 8374. https://doi.org/10.3390/su14148374

[7] CICIDS2017. (n.d.). Kaggle. https://www.kaggle.com/datasets/cicdataset/cicids2017

[8] CICIDS2019. (n.d.). Kaggle. https://www.kaggle.com/datasets/tarundhamor/cicids-2019-dataset