RESEARCH ON TECHNIQUES TO ENHANCE DDoS ATTACK PREVENTION USING CUMULATIVE SUM AND BACKPROPAGATION ALGORITHMS

Hoang Thi Phuong

University of Economics - Technology for Industries, Hanoi, Vietnam

ARTICLE INFORMATION

Journal: *Vinh University Journal of Science Natural Science, Engineering and Technology*
p-ISSN*: 3030-4563*
e-ISSN: *3030-4180*

Volume: 53
Issue: 4A
****Correspondence:***
htphuong@uneti.edu.vn

Received: *25 August 2024*
Accepted: *11 October 2024*
Published: *20 December 2024*

Citation:
Hoang Thi Phuong (2024). Research on techniques to enhance DDoS attack prevention using cumulative Sum and backpropagation algorithms. ***Vinh Uni. J. Sci.*** *Vol. 53 (4A), pp. 69-78 doi: 10.56824/vujs.2024a091a*

ABSTRACT

This paper focuses on enhancing DDoS attack prevention capabilities through the combination of the Cumulative Sum (CUSUM) algorithm and the Backpropagation method, aiming to detect attack indicators early and accurately. The CUSUM algorithm is used to monitor and analyze network traffic over time, identifying unusual fluctuations in traffic without requiring prior knowledge of attack types. Meanwhile, the Backpropagation method is applied to optimize neural networks, enabling the system to learn from previous traffic data and distinguish clearly between legitimate traffic and attack traffic. Compared to previous research methods, this combined approach offers several significant advantages. First, CUSUM provides high-accuracy attack detection, allowing the system to respond promptly. Second, Backpropagation enables the system to improve automatically over time, reducing false alarm rates and enhancing prevention effectiveness. Finally, the feasibility and effectiveness of the solution are demonstrated through real-world experiments, showing improved detection rates and faster response times compared to traditional methods.

Keywords: Network attack; CUSUM algorithm; Backpropagation algorithm; Anti-spoofing; DDoS attack.

1. Introduction

DDoS (Distributed Denial of Service) attacks are a common form of cyberattack aimed at disrupting system services by overwhelming them with a high volume of traffic from multiple sources, causing the target server or network to become overloaded. A key characteristic of DDoS attacks is their distributed nature, which often leverages botnets to control compromised devices remotely. The impacts of DDoS attacks can include website or online service outages, financial losses, data breaches, reputational damage, and the consumption of system resources needed for recovery. To counter DDoS attacks, numerous research groups have focused on developing detection and mitigation solutions. Detection mechanisms typically monitor network traffic parameters

across various points; these parameters are periodically collected and processed through algorithms to identify potential attacks. Once detected, specific measures are implemented to filter out malicious traffic, thus protecting servers and services.

DDoS attack detection methods can be categorized into three main groups: signature-based detection, statistical anomaly-based detection, and data mining-based approaches. Signature-based detection methods store the traffic characteristics of known attacks in a database and compare them with current traffic parameters. If a match is found, the system identifies an attack [1]. However, this approach is limited in detecting new attack types, and as the database grows more complex, processing time increases. Data mining-based methods use artificial intelligence, soft computing, and machine learning algorithms, often deployed in a distributed manner to prevent devices from becoming part of a botnet [2], [3]. Statistical methods rely on monitoring traffic changes over time, with unusual spikes indicating an attack. The effectiveness of these methods depends on the parameters and algorithms used for monitoring, as shown in [4], [5], [6]. However, these methods typically require systems capable of collecting large volumes of traffic and sophisticated algorithms, which makes real-time deployment challenging.

DDoS attacks pose significant risks to organizations by disrupting critical services, making rapid and accurate detection essential. The CUSUM algorithm has proven effective in identifying abnormal fluctuations in network traffic, while Backpropagation can be used to optimize decision-making in defensive processes [7], [8], [9], [10], [11]. In this paper, we propose a novel solution using a statistical approach that adjusts neural network weights based on the error between the model's predicted output and the desired output. Specifically, we apply the CUSUM (Cumulative Sum) algorithm to detect early signs of a DDoS attack and enhance the Backpropagation protocol to improve mitigation, even when an attacker spoofs IP addresses. Placing filters close to the attack source through the Backpropagation protocol represents an optimal method in current DDoS prevention protocols.

2. Theoretical Foundation for DDoS Attack Prevention

2.1. Cumulative Sum (CUSUM) Algorithm

The Cumulative Sum (CUSUM) algorithm detects changes in a data sequence by calculating the cumulative sum of deviations between observed and expected values. When this cumulative sum surpasses a predetermined threshold, it signals an abnormal change. CUSUM is widely used in quality monitoring and network intrusion detection due to its ability to detect early, subtle, yet consistent variations. However, the algorithm may experience detection delays if fluctuations are too small or sudden, potentially impacting its effectiveness in real-time applications.

2.2. Source IP Address Monitoring

The Source IP Address Monitoring (SIM) algorithm operates by tracking and evaluating new IP addresses, comprising two primary phases: offline training and detection with learning. In the offline training phase, SIM monitors and analyzes IP addresses over a specified period, storing frequently accessed addresses in the IP Address Database (IAD).

To conserve memory, the database is optimized by removing expired addresses and updating it with new IP addresses. The IAD is updated offline to ensure that no malicious IP addresses are included. During the detection and learning phase, SIM compiles traffic statistics over time, comparing incoming IP addresses to the IAD to identify new ones. These new IPs are evaluated using a specific function that leverages the CUSUM algorithm; if observed changes exceed a defined threshold, the system concludes an attack has occurred.

2.3. Backpropagation Algorithm

Backpropagation is a critical algorithm in deep learning used to optimize artificial neural network models by adjusting weights based on the error between the model's predicted and desired outputs. The backpropagation process consists of two key steps:

- **Forward Propagation**: Input data is passed through the layers of the neural network, and the predicted output is computed.

- **Backpropagation**: After calculating the loss (error) between the predicted and actual output, the algorithm computes the gradient of the error with respect to each weight in the model. The weights are then adjusted in a backward manner to minimize the error.

This algorithm is based on the chain rule of calculus, allowing efficient gradient computation to optimize models through gradient descent.

The backpropagation protocol also serves as a defensive mechanism against DDoS attacks through a reactive and distributed approach, relying on three key principles:

- Using filters on routers to block DDoS packets.

- Employing a “backpropagation” mechanism to shift filtering tasks to routers closer to the attacker.

- Utilizing algorithms to enhance performance and counter deception.

The backpropagation protocol activates when the victim shows signs of a denial of service (DoS) attack. At the victim's gateway, filters are activated to block all incoming attack packets. The gateway identifies the network interface receiving the attack traffic and sends a request to the neighboring router through that interface, activating the filter and continuing monitoring at subsequent routers. This process repeats sequentially, moving closer to the attack source. The protocol works in reverse, and through network interface monitoring, it can trace back to the attack source, even when IP addresses are spoofed.

3. Development of an Automated DDoS Attack Detection and Prevention System and Discussion

This paper presents the development and implementation of a reverse propagation protocol, enhanced with an anti-deception mechanism to improve DDoS attack detection and prevention [2], [3], [4], [5], [6]. The main components are as follows:

- **Cumulative Sum (CUSUM) Algorithm**: This algorithm monitors network traffic patterns over time. When it detects significant changes in traffic behavior, CUSUM triggers an alert, prompting the system to respond.

- **Backpropagation Method**: Neural networks trained with the backpropagation method are used to recognize patterns in both normal and abnormal traffic, enhancing the system’s capability to detect and respond to potential attacks.

This approach integrates real-time traffic monitoring with adaptive learning to improve the effectiveness of DDoS attack prevention.

3.1. Anti-Spoofing Attributes

An attacker may take control of a router along the transmission path, refusing to apply the filter as requested by the preceding router, or manipulate the Agent Gateway *(Agent_GW)* to implement the filter only temporarily, for a duration *tcheat*, shorter than the initially requested filtering time *tlong*. Once the Victim Gateway *(Victim_GW)* disconnects, assuming the filter is active, the attacker resumes the attack. This time difference introduces a security gap, making it challenging for the system to respond promptly and exposing potential vulnerabilities.

3.2. Implementation Solutions

When a reverse propagation request is sent to *Agent_GW*, a verification program is activated to ensure *Agent_GW* complies with the specified filtering duration. If traffic from the attacker persists within the predefined timeframe, the *Agent* will automatically activate the filter locally. This mechanism ensures that, even if deception occurs during filtering, the attack is blocked directly at the Agent. By addressing attempts to manipulate the filtering duration, the system's security is strengthened.

3.3. Algorithm Description

Upon receiving a data stream sent from the client to *LTN_Server*, the system retrieves the IP address of the server and forwards this stream to the neighboring router. If the neighboring router does not support the reverse propagation protocol or shows signs of IP address spoofing, the filter is activated immediately. If no anomalies are detected, the data stream continues to the server.

Meanwhile, the system continuously monitors the log file at */var/log/message*, gradually reducing the initial filter duration. This log checking process uses the grep command to verify the source and destination IP addresses, as well as the sequence number. If the sequence number differs from the last recorded sequence number when the filter was activated at the router closest to the *Agent*, it indicates that packets from the *Agent* have passed through. This suggests the neighboring router may have been compromised, potentially setting a shorter filter duration or falsely claiming to have activated it. In this case, the system promptly resets the filter for the remaining duration.

3.4. Implementation

The model used in this paper is deployed on the following devices and targets (Figure 1) [7], [8], [9], [10], [11], [12], [13]:

- **Server S1** is the victim.
- **R2** is the victim's gateway.
- **R3** and **R4** are core routers.
- **R5**, **R6**, **R7**, and **R8** serve as gateway routers corresponding to **R3** and **R4**.
- **C9**, **C10**, **C11**, **C12**, **C13**, **C14**, **C15**, and **C16** are machines accessing the victim.

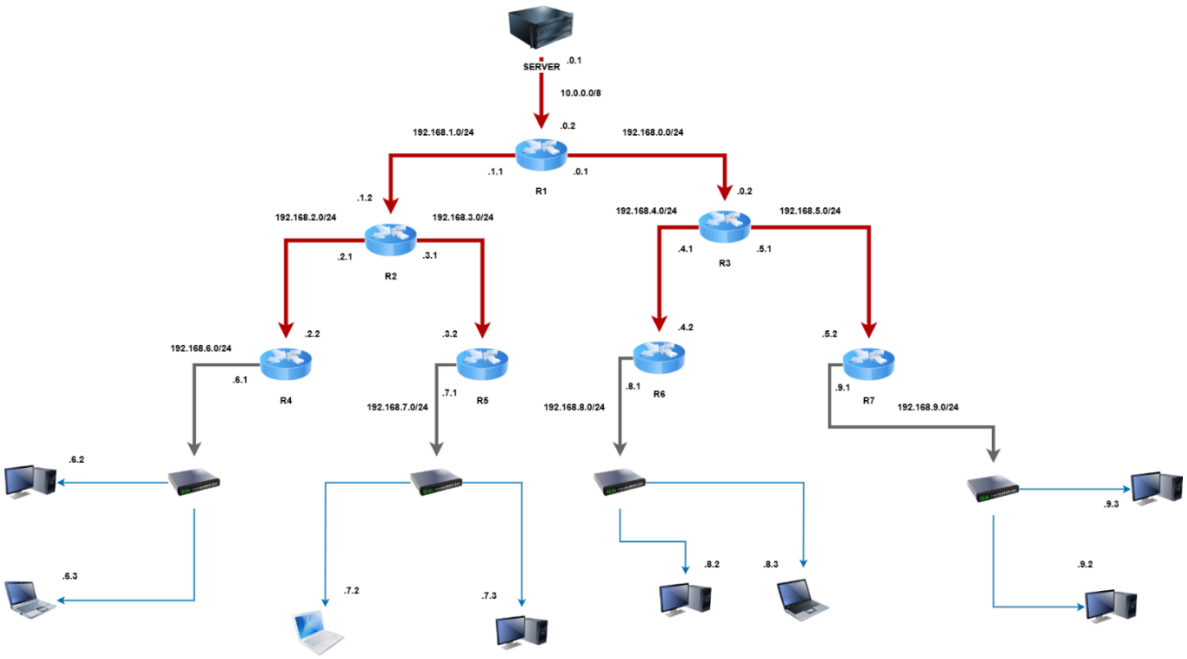

Figure 1: *Model for Implementing Anti-Spoofing Mechanisms*

This setup forms the foundation for implementing and testing the defense mechanism against DDoS attacks, as outlined in the paper.

Since identifying frequently accessed IP addresses requires substantial time, this model sets the time parameter to 5 minutes. During this period, the system captures packets using IPTraf software. Machines **C9**, **C10**, **C11**, and **C12** continuously ping **S1** throughout the 5-minute interval. At the end of this period, the system stores the collected IP addresses - including 172.16.6.2, 172.16.6.3, 172.16.7.2, and 172.16.7.3 - into the IP Address Database (IAD) (Figure 2).

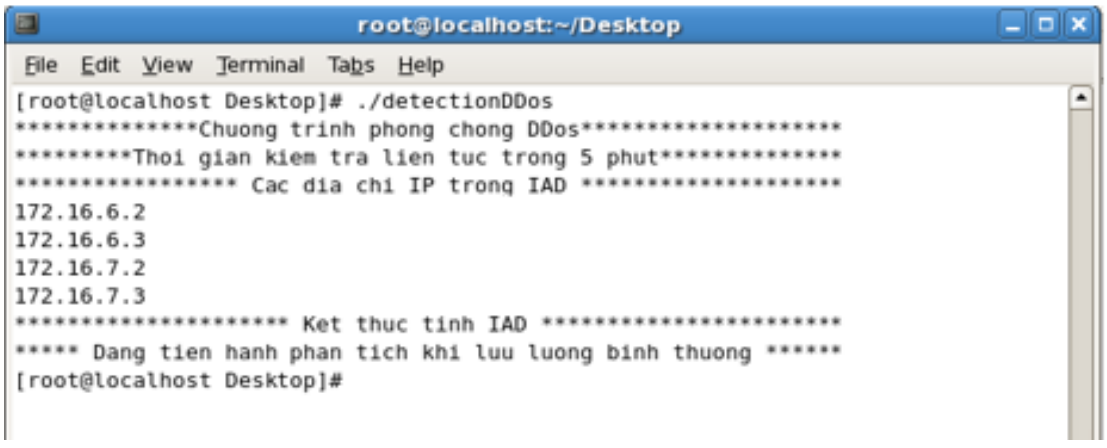

Figure 2: *Building the IP Address Database (IAD)*

Assuming that **C13** pings **S1** under normal traffic conditions, the system calculates and determines the average value μ of the sequence $\{X_n\}$ during normal network conditions. Consequently, all values of Y are equal to 0, as illustrated in Figure 3.

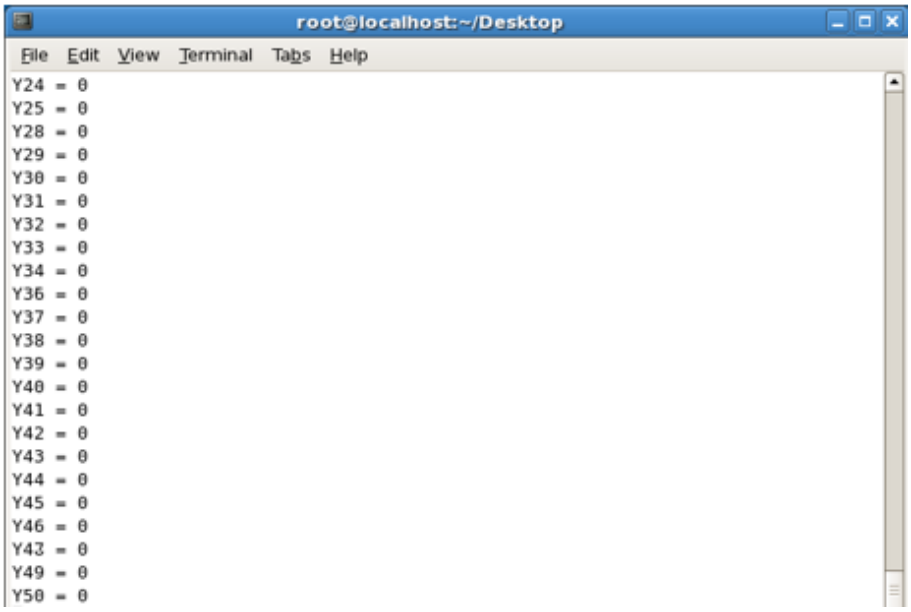

Figure 3: *The value of Y during normal network traffic*

Subsequently, machines **C14**, **C15**, and **C16** initiate ping requests to **S1** while **C9**, **C10**, **C11**, and **C12** continue to ping **S1** under normal conditions. The system at **S1** detects an attack as the values of Y rise rapidly, exceeding the threshold $N = 0.05$, as shown in Figure 4.

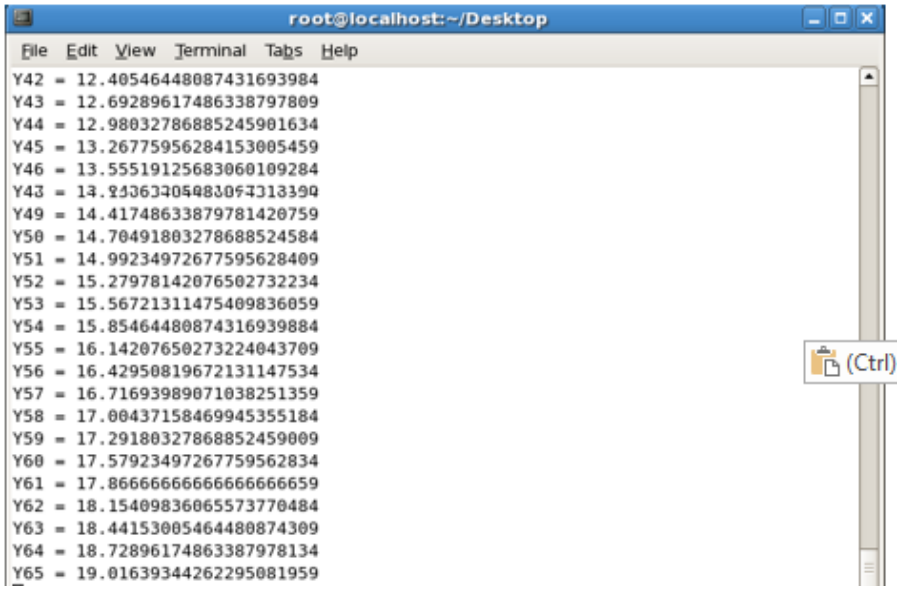

Figure 4: *The value of Y during an attack*

The system then proceeds to block the IP addresses of **C14**, **C15**, and **C16** using the backpropagation protocol, as these addresses are new. Meanwhile, **C9**, **C10**, **C11**, and **C12** continue to ping **S1** without interruption, as their IPs are recognized as frequent visitors, as illustrated in Figure 5. The results, as shown in Figure 5, demonstrate the system's high effectiveness in detecting and preventing attacks.

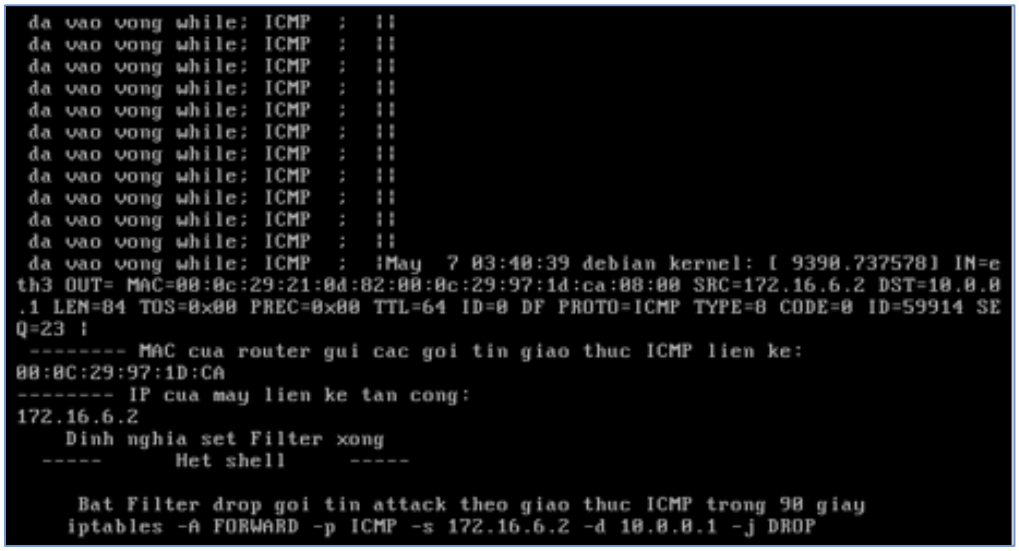

Figure 5: *Blocking new IPs using the backpropagation protocol*

In a scenario where **C9** and **C10** (designated as Agents) send ping requests to **S1** (the victim), the reverse propagation protocol triggers a filter setup at **R5**, the router closest to the attack source. The filter at **R5** is configured with a cheat time t_{cheat} set to 20 seconds, which is less than the long time t_{long} set to 40 seconds. When the reverse propagation reaches **R5**, **R3** activates the time-checking mechanism for **R5**'s filter. After t_{cheat} expires, **R5** removes the filter, allowing packets to pass through. At this point, **R3** detects packets from **C9** and **C10** being transmitted while the filter's request time is still active. **R3** immediately re-establishes the filter for the remaining duration of $t_{long} - t_{cheat}$ (20 seconds) to block packets from **C9** and **C10**, effectively implementing the anti-spoofing mechanism. The inspection mechanism at **R3** is illustrated in Figure 6.

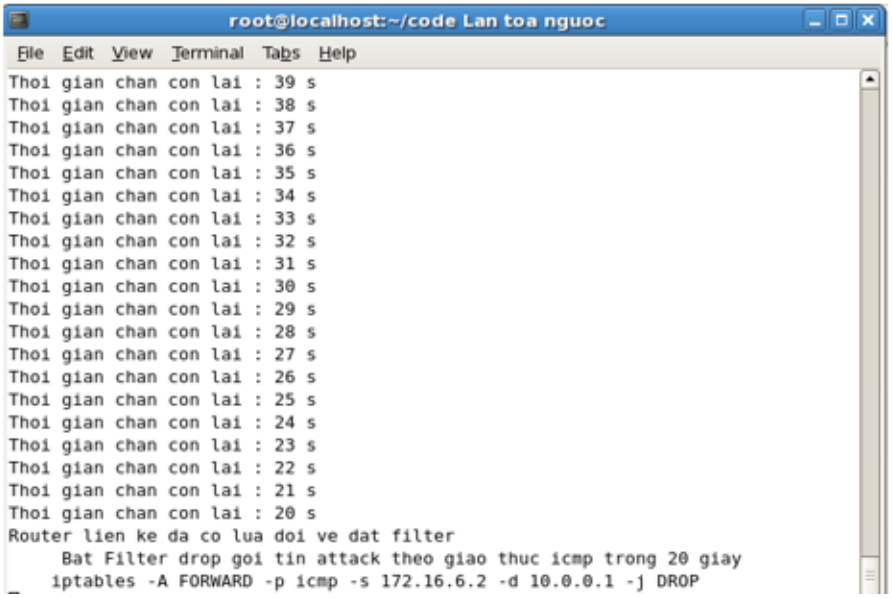

Figure 6: *Experimental results on anti-spoofing*

4. Conclusion

Due to the distributed nature and severity of DDoS attacks, fully preventing them remains a significant challenge. In practice, a DDoS attack can involve thousands of servers simultaneously targeting a single victim. This paper presents an application of the CUSUM algorithm to detect early signs of a DDoS attack. The accuracy of detection, combined with a reverse propagation protocol, has significantly enhanced the system's effectiveness. This detection and automated prevention system is designed to be deployed at the victim's site, where the reverse propagation protocol mechanism can redirect the attack back to its source, strengthening the system's defensive capabilities.

The integration of these two methods offers notable benefits, including: automatic alerts upon detecting a DDoS attack, automatic blocking of new IP addresses during an attack, IP spoofing prevention, and consistent functionality even when neighboring routers do not support reverse propagation. However, the system has certain limitations. First, the reverse propagation protocol is complex and requires installation on routers, which can complicate deployment and maintenance. Second, the automatic blocking mechanism could potentially block new IP addresses, possibly resulting in false positives for infrequently accessed IPs. Although this risk is minimized by using an IP Address Database (IAD) technique, it is not eliminated entirely. Another consideration is that, since the system operates autonomously, the reverse propagation protocol will be configured with the "all" parameter, with a fixed time parameter to ensure consistent operations.

This research demonstrates that combining the CUSUM algorithm with the Backpropagation method is highly effective in detecting and mitigating DDoS attacks. It provides a robust approach for DDoS attack detection and opens new directions in cybersecurity research, encouraging the application of machine learning and deep learning algorithms to enhance system security. Future research could further explore the application of deep learning algorithms to improve the system's ability to rapidly identify and respond to network threats.

REFERENCES

[1] H. S. Dhadhal and P. P. Kotak, "DDoS attack detection using enhanced neural network algorithm in software-defined networks," *Journal of Computer Science*, vol. 19, no. 6, pp. 749-759, 2023. DOI: 10.3844/jcssp.2023.749.759

[2] M. S. Elsayed, "Ddosnet: A deep-learning model for detecting network attacks," In *2020 IEEE 21st International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, 2020, pp. 391-396. DOI: 10.1109/WoWMoM49955.2020.00072

[3] A. A. Najar and S. Manohar, "Cyber-secure SDN: A CNN-based approach for efficient detection and mitigation of DDoS attacks," *Comput. Secur.*, vol. 139, p. 103716, 2024. DOI: 10.1016/j.cose.2024.103716

[4] Q. Li and Y. A. Jiang, "A comprehensive survey on DDoS defense systems: New trends and challenges," *Comput. Netw.*, vol. 233, p. 109895, 2023. DOI: 10.1016/j.comnet.2023.109895

[5] F. Chbib and A. E. Attar, "Detecting DDoS attacks using adversarial neural network," *Comput. Secur.*, vol. 127, p. 103117, 2023. DOI: 10.1016/j.cose.2023.103117

[6] P. Pawar, "A lightweight model for DDoS attack detection using machine learning techniques," *Appl. Sci.*, vol. 13, p. 9937, 2023. DOI: 10.3390/app13179937

[7] M. A. A. Al-Ghamdi, "Robust DDoS attack detection using piecewise Harris hawks optimizer with deep learning for a secure internet of things environment," *Mathematics*, vol. 11, p. 4448, 2023. DOI: 10.3390/math11214448

[8] P. Shukla, "EIoT-DDoS: Embedded classification approach for IoT traffic-based DDoS attacks," *Clust. Comput.*, vol. 27, no. 2, pp. 1471-1490, 2024. DOI: 10.1007/s10586-023-04027-5

[9] S. B. Erukala, "A lightweight multi-vector DDoS detection framework for IoT-enabled mobile health informatics systems using deep learning," *Inf. Sci.*, vol. 662, p. 120209, 2024. DOI: 10.1016/j.ins.2024.120209

[10] P. Machaka, "Using the cumulative sum algorithm against distributed denial of service attacks in internet of things," In *International Conference on Context-Aware Systems and Applications*, vol. 1, 2016, pp. 1-10. DOI: 10.1007/978-3-319-29236-6_7

[11] M. Arunadevi and V. Sathya, "DDoS attack detection using back propagation neural network optimized by bacterial colony optimization," *Int. J. Intell. Eng. Syst.*, vol. 16, no. 5, pp. 301-312, 2023. DOI: 10.22266/ijies2023.1031.26

[12] K. J. Singh, K. Thongam, and T. De, "Entropy-based application layer DDoS attack detection using artificial neural networks," *Entropy*, vol. 18, no. 10, p. 350, 2016. DOI: 10.3390/e18100350

[13] C. Gomathi, "Financial prediction using back propagation neural networks with opposition-based learning," In *Journal of Physics: Conference Series*, vol. 1142, no. 1, 2018. DOI: 10.1088/1742-6596/1142/1/012008

TÓM TẮT

NGHIÊN CỨU KỸ THUẬT CẢI THIỆN KHẢ NĂNG PHÒNG CHỐNG TẤN CÔNG DDoS SỬ DỤNG GIẢI THUẬT CUMULATIVE SUM VÀ BACKPROPAGATION

Hoàng Thị Phượng
Trường Đại học Kinh tế - Kỹ thuật Công nghiệp, Hà Nội, Việt Nam
Ngày nhận bài 25/8/2024, ngày nhận đăng 11/10/2024

Bài báo này tập trung vào việc cải thiện khả năng phòng chống tấn công DDoS thông qua kết hợp giải thuật Cumulative Sum (CUSUM) và phương pháp Backpropagation, nhằm phát hiện sớm và chính xác các dấu hiệu tấn công. Giải thuật CUSUM được sử dụng để theo dõi và phân tích lưu lượng mạng theo thời gian, giúp xác định các biến động bất thường trong lưu lượng mà không cần phải biết trước về kiểu tấn công. Trong khi đó, phương pháp Backpropagation được áp dụng để tối ưu hóa mạng nơ-ron, cho phép hệ thống học từ dữ liệu lưu lượng trước đó, phân biệt rõ ràng giữa lưu lượng hợp lệ và lưu lượng tấn công. So với các phương pháp nghiên cứu trước đây, phương pháp kết hợp này mang lại nhiều ưu điểm nổi bật. Thứ nhất, CUSUM cung cấp khả năng phát hiện tấn công với độ chính xác cao, giúp hệ thống phản ứng kịp thời. Thứ hai, Backpropagation cho phép hệ thống tự động cải thiện theo thời gian, giảm thiểu tỷ lệ báo động sai và nâng cao hiệu quả phòng chống. Cuối cùng, tính khả thi và hiệu quả của giải pháp được chứng minh qua các thử nghiệm thực tế, cho thấy tỷ lệ phát hiện và thời gian phản ứng nhanh hơn so với các phương pháp truyền thống.

Từ khóa: Tấn công mạng; giải thuật CUSUM; giải thuật Backpropagation; phòng chống lừa đảo; tấn công DDoS.