TỔNG HỢP VỀ TẤN CÔNG MẠNG BẰNG DDoS TRONG SDN

Đào Thị Hường
Khoa Công nghệ thông tin
Email: huongdt@dhhp.edu.vn

Ngày nhận bài: 27/3/2023
Ngày PB đánh giá: 09/5/2023
Ngày duyệt đăng: 15/5/2023

TÓM TẮT: Trong xã hội hiện đại, Internet là một dịch vụ đóng vai trò quan trọng đối với tất cả các tổ chức cũng như cá nhân. Bên cạnh những lợi ích to lớn mà Internet mang lại nó cũng đồng thời phát sinh nhiều vấn đề cần giải quyết, đặc biệt là vấn đề an ninh mạng. Mạng được xác định bởi phần mềm SDN (*Software-Defined Networking - SDN*), được sử dụng một cách phổ biến với những yếu tố điều khiển linh hoạt khi vận hành các dịch vụ mạng. Trong bài báo này, chúng tôi trình bày một cách tổng hợp các cơ chế phát hiện và giảm thiểu thiệt hại đối với tấn công DDoS trong SDN, cụ thể là: phương pháp dựa trên lý thuyết thông tin, phương pháp dựa trên học máy, phương pháp dựa trên mạng Nơron nhân tạo. Chúng tôi cũng giới thiệu các lỗ hổng và thách thức trong việc triển khai các giải pháp phòng chống DDoS đối với kiến trúc SDN.

Từ khóa: tấn công mạng, mạng được xác đinh bởi phần mềm (SDN), tấn công từ chối dịch vụ phân tán (DDoS).

A SYSTEMATIC REVIEW OF CYBER ATTACKS DDoS IN SDN

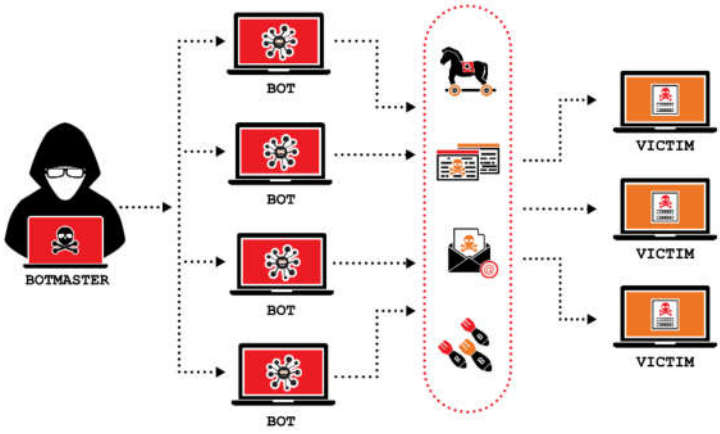
ABSTRACT: In modern society, Internet plays a significant role for all organizations and individuals. Besides the great benefits, Internet also raises many issues that need to be solved, especially in network security. The Software-Defined Networking (SDN) along with a highly flexible capability of control the components when manipulating network services, is being widely adopted. In this paper, we would like to present a synthesis of DDoS attack detection and mitigation mechanisms in SDN, specially, Information theory-based DDoS defence solutions, Machine learning-based DDoS defence solutions, Artificial Neural Network-based defence solutions. We also indicate vulnerabilities as well as challenges in the implementation of DDoS preventing solutions in SDN.

Keywords: cyber attacks, DDoS, SDN.

1. MỞ ĐẦU

Công nghiệp phần mềm đang có sự dịch chuyển không ngừng từ cung ứng dịch vụ truyền thống (cài đặt trên máy tính cá nhân) sang phương thức sử dụng dịch vụ được cung ứng trên mạng Internet (ứng dụng trên nền Web) [4]. Bởi vậy, xuất hiện rất nhiều các bài toán cần giải quyết liên quan đến mạng máy tính, đặc biệt là an toàn và bảo mật thông tin trên Internet. Cho đến này, đã có nhiều cách tấn công trên mạng máy tính như Worns, Trojans, tấn công theo kiểu từ chối dịch vụ (DoS - *Denial of Servive*), … là một số hình thức tấn công phổ biến trên Internet. Tấn công DoS là phương pháp ngăn chặn người dùng hợp pháp truy cập vào tài nguyên trên mạng máy tính bằng cách việc làm cạn kiệt các nguồn tài nguyên và dẫn đến từ chối truy cập.

Với tốc độ phát triển không ngừng của phần cứng, kẻ tấn công đã sử dụng đa thiết bị trong DoS, khi đó chuyển thành các cuộc tấn công từ chối dịch vụ phân tán (*Distributed Denial of Service* - DDoS). Tấn công DDoS tạo ra một đội quân (bao gồm các hệ thống máy tính bị chiếm quyền xâm nhập và điều khiển), được gọi là mạng botnet. Để khởi động một cuộc tấn công DDoS, kẻ tấn công gửi lệnh đến tất cả máy tính bị xâm nhập và kích hoạt yêu cầu từ tất cả các máy tính này gửi đến nạn nhân làm nạn nhân bị quá tải với lưu lượng truy cập vô ích. Do đó, tài nguyên của nạn nhân không thể truy cập được đối với người dùng hợp pháp và nạn nhân được cho là đang bị tấn công DDoS. **Error! R eference source not found.** minh hoạ cơ chế tấn công từ chối dịch vụ phân tán.



Hình 1. Cơ chế tấn công từ chối dịch vụ phân tán

Đã có nhiều phương pháp tiếp cận để phát hiện và giảm thiểu thiệt hại đối với các cuộc tấn công DDoS như mạng có thể lập trình [12] (*Programmable Networks*) và mạng được xác đinh bởi phần mềm [22] (*Software-Defined Networking* - SDN), *v.v*. Trong đó, SDN được coi là một trong những bước tiến đáng kể mang lại hiệu quả cao đối

với cơ sở hạ tầng tại thời điểm hiện tại bởi tính linh hoạt, tốc độ triển khai và khả năng lập trình động và đơn giản hoá quá trình quản lý mạng. Mặc dù, kiến trúc SDN có khả năng tăng cường bảo mật của hệ thống mạng dựa vào bộ điều khiển tập trung nhưng nó cũng có những thách thức riêng cần phải giải quyết. Cụ thể, vì quá trình điều khiển tập trung và chịu trách nhiệm quản lý mạng nên đây cũng sẽ là một lỗ hổng bảo mật trở thành mục tiêu của các cuộc tấn công DDoS.

Shin [6] đã chỉ ra một số cách thức tấn công mạng tương ứng với các tầng khác nhau của kiến trúc SDN, cụ thể là tấn công DDoS trong các lớp ứng dụng, lớp điều khiển và lớp dữ liệu, đây là các mặt phẳng mục tiêu của các cuộc tấn công mạng. Một số nghiên cứu khác cũng đã tập trung vào phát hiện và giảm thiểu tác hại của các cuộc tấn công DDoS trong bối cảnh SDN. Trong nghiên cứu này, chúng tôi tập trung vào các khía cạnh sau:

(i) Trình bày kiến trúc SDN một cách cụ thể kèm với các tính năng chính giúp kiến trúc này mạnh mẽ và linh hoạt hơn so với các mạng dựa trên IP;

(ii) Đánh giá một cách chi tiết các cuộc tấn công DDoS đối với kiến trúc SDN;

(iii) Tổng hợp và phân loại các kỹ thuật phát hiện và giảm thiểu tác hại của các cuộc tấn công DDoS trong SDN.

Các phần tiếp theo của bài báo được cấu trúc như sau, Phần 2, chúng tôi sẽ giới thiệu về kiến trúc SDN cùng với các đặc trưng cơ bản của kiến trúc này. Phần 3 là những nội dung đánh giá một cách chi tiết các cuộc tấn công DDoS đối với kiến trúc SDN. Chúng tôi tiến hành phân loại các phương pháp phát hiện và giảm thiểu tấn công DDoS trong Phần 4. Cuối cùng là kết luận về những vấn đề là thực hiện được cũng như các công việc cần triển khai trong thời gian tiếp theo.

2. KIẾN THỨC CƠ SỞ

Trong phần này, chúng tôi sẽ giới thiệu hai loại kiến trúc mạng cơ bản: (i) Kiến trúc mạng được quản lý dựa trên địa chỉ IPs và (ii) Kiến trúc mạng được xác định bởi phần mềm (SDN).

2.1. Kiến trúc mạng dựa trên địa chỉ IPs

Đối với phương pháp quản lý mạng truyền thống thông qua địa chỉ IP, tầng điều khiển và tầng dữ liệu được tích hợp thành các thiết bị dùng chung, điều này dẫn đến tính thiếu linh hoạt trong triển khai bởi các nhà khai thác mạng cần *cấu hình từng thiết bị mạng* bằng cách sử dụng các lệnh **cấp thấp** để thực hiện các chính sách mạng **cấp cao**. Phương thức quản lý mạng máy tính theo cách này được gọi là tích hợp theo chiều dọc (*vertically integrated*).

2.2. Kiến trúc mạng được xác định bởi phần mềm (SDN)

Kiến trúc mạng được xác định bằng phần mềm (Software-Defined Networking - SDN) là mô hình mạng trong đó tầng điều khiển logic và tầng dữ liệu được tách rời và quá trình giao tiếp giữa hai tầng này được thiết lập bởi các giao diện ứng dụng lập trình (APIs); toàn bộ quá trình điều khiển ứng dụng mạng

được xử lý tập trung. Hình 2 minh hoạ kiến trúc mạng được xác định thông qua phần mềm. Một số thuật ngữ cơ sở trong kiến trúc mạng SDN là:

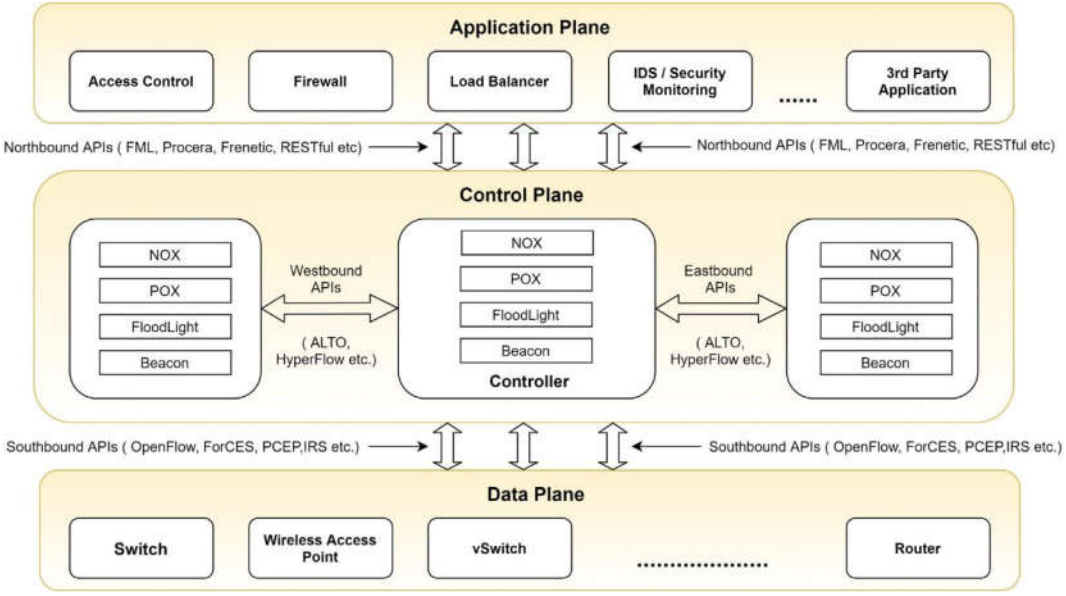
Mặt phẳng dữ liệu: bao gồm các thiết bị chuyển tiếp gói khác nhau như bộ định tuyến, điểm truy cập không dây, bộ chuyển mạch và bộ chuyển mạch ảo. Trong SDN, chúng là các công tắc OpenFlow. Các thiết bị này chứa các bảng lưu lượng để lưu trữ các quy tắc chuyển tiếp các gói, được xác định hoàn toàn bởi mặt phẳng điều khiển và các thiết bị. Mặt phẳng dữ liệu tập trung vào chuyển tiếp các gói tin.

Giao diện hướng Nam: Đây là các giao thức tạo điều kiện kiểm soát hiệu quả trên mặt phẳng dữ liệu (OpenFlow [11], v.v.).

Tầng điều khiển: Liên quan đến bộ điều khiển SDN hoặc NOS (Hệ điều hành mạng) là bộ não của toàn bộ mạng (NOX [2], v.v.). Tầng này chịu trách nhiệm đưa ra các quyết định chuyển tiếp gói và triển khai chúng vào các thiết bị mạng.

Giao diện hướng Bắc: Nó là một giao diện giữa mặt phẳng điều khiển và mặt phẳng ứng dụng. Các API này được cung cấp bởi NOS cho các nhà phát triển ứng dụng và giúp lập trình mạng và ẩn các chi tiết nội bộ của mạng (FML [9], v.v.).

Tầng ứng dụng: Còn được gọi là mặt phẳng quản lý và là mặt phẳng đầu tiên trong kiến trúc SDN. Tất cả các ứng dụng, được viết bởi các nhà phát triển để quản lý mạng, thực thi trên mặt phẳng này. Trong SDN, giám sát lỗi và cấu hình thiết bị mạng được thực hiện thông qua mặt phẳng ứng dụng.

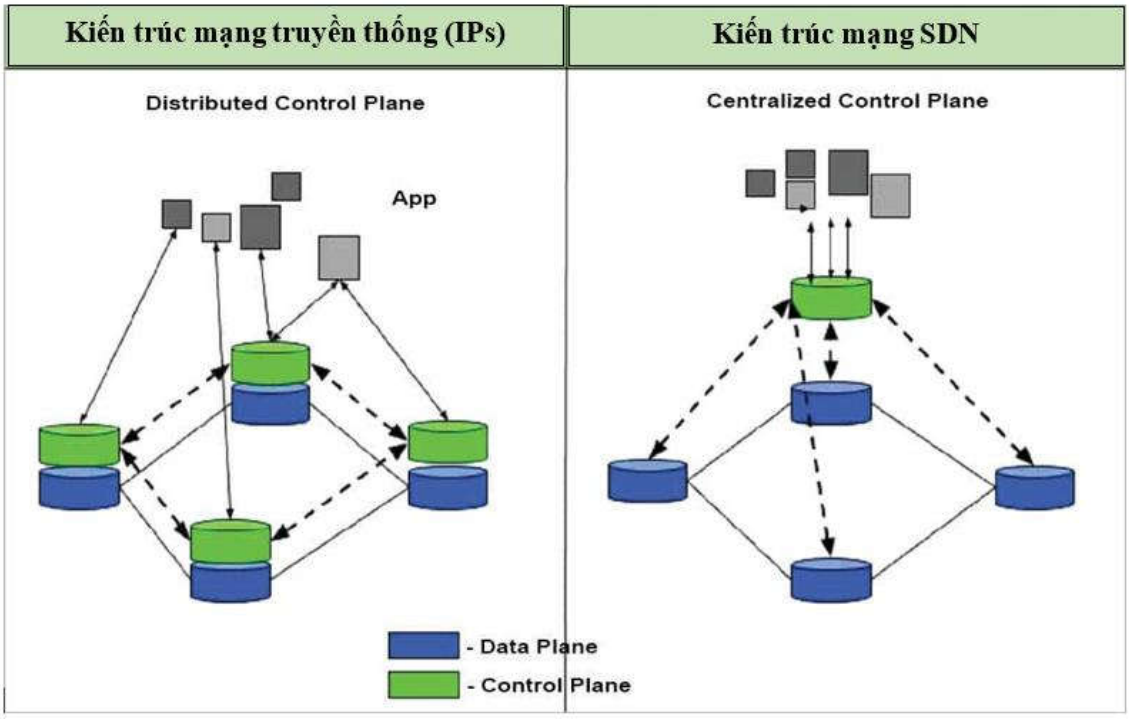


Hình 2. Các tầng kiến trúc mạng SDN

Hướng Đông và hướng Tây: Trong SDN, tất cả các bộ điều khiển mạng được tập trung về mặt logic, nhưng có thể được phân phối về mặt vật lý. Các bộ điều khiển này giao tiếp thông qua các giao diện hướng đông và hướng tây. Vì một bộ điều khiển duy nhất chỉ có thể xử lý một mạng nhỏ, vì vậy nếu nó bị lỗi, toàn bộ mạng sẽ bị xâm phạm. Trong trường hợp này, cần có nhiều bộ điều khiển và nếu một bộ điều khiển bị lỗi, có thể thông báo cho các bộ điều khiển khác để tiếp quản việc xử lý lưu lượng (HyperFlow [3], v.v.).

Kiến trúc của mạng SDN mang lại một **lợi thế** lớn đối với việc phát hiện và phòng thủ các cuộc tấn công DoS và DDoS, cụ thể như sau: (1) Tách biệt mặt phẳng dữ liệu và mặt phẳng điều khiển; (2) Cho phép hiển thị thông tin toàn cục về mạng; (3) Phân tích lưu lượng dựa trên phần mềm; (4) Khả năng lập trình mạng động; (5) Cập nhật chính sách mạng động.

Như vậy, trong phần này chúng tôi đã giới thiệu một cách chi tiết kiến trúc cũng như đặc điểm lợi thế của mạng SDN. Hình 3 minh họa kiến trúc mạng được quản lý bởi địa chỉ IPs (bộ điều khiển phân tán) và kiến trúc mạng sử dụng SDN (bộ điều khiển mạng tập trung).



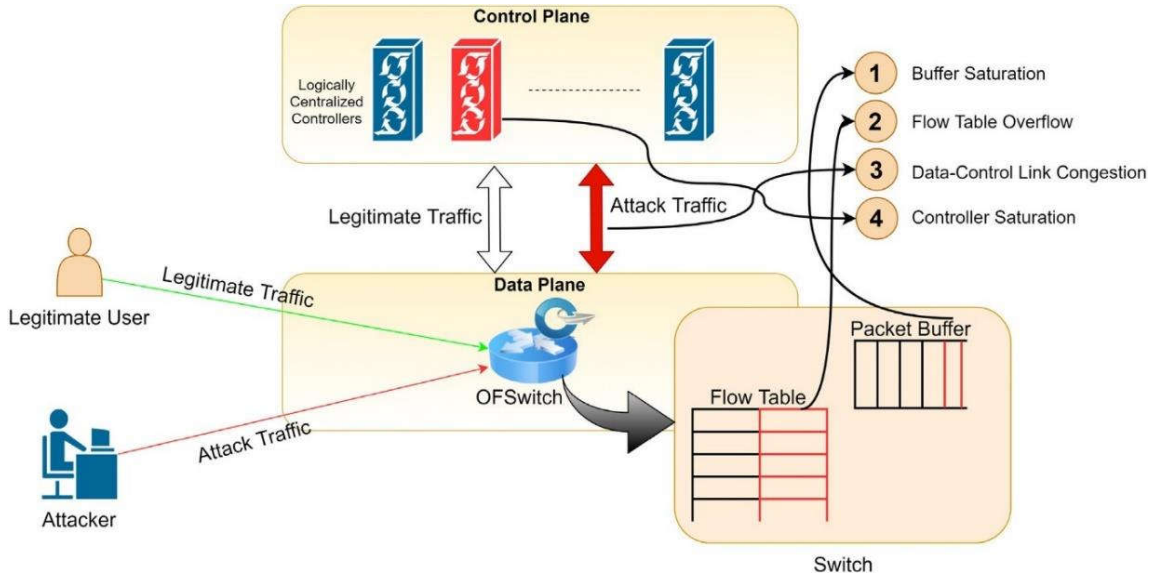
Hình 3. Kiến trúc mạng truyền thống và SDN

3. Tấn công DDoS đối với SDN

Bảng 1. Tổng hợp các lỗ hổng trong kiến trúc SDN

Loại lỗ hổng	Các điểm chú ý
Bão hoà bộ nhớ đệm	Sử dụng lưu trữ tiêu đề gói tin (bộ chuyển mạch) - OpenFlow thiết lập các chính sách cần lưu trữ thông tin trong bộ nhớ đệm.
Tràn bảng lưu lượng	Các bộ chuyển mạch cần có bộ nhớ TCAM để lưu trữ lưu lượng các bảng. Tuy nhiên, bộ nhớ này bị hạn chế bởi giá thành cao.
Tắc nghẽn liên kết giữa mặt phẳng dữ liệu và mặt phẳng điều khiển	Đối với mỗi luồng lưu lượng mới, bộ chuyển mạch cần thiết lập chính sách mới cho Packet_in và Packet_out, điều này dễ dẫn đến tình trạng tắc nghẽn liên kết giữa hai mặt phẳng.
Độ bão của bộ điều khiển	Bộ điều khiển cũng có thể bị bão hoà nếu nó nhiều request độc hại gửi đến cùng lúc.

Kiến trúc SDN được tạo ra để khắc phục các vấn đề còn hạn chế trong bảo mật mạng máy tính truyền thống. Tuy nhiên đến lượt mình, SDN cũng cần phải được khắc phục các vấn đề bảo mật có thể bị khai thác, đặc biệt là các khía cạnh tích hợp theo chiều dọc liên quan đến ba lớp chức năng của kiến trúc mạng. Các lỗ hổng bảo mật này được thể hiện một cách chi tiết trong Hình 4 và Bảng 1.



Hình 4. Sơ đồ mức khái niệm về các lỗ hổng trong kiến trúc SDN

Từ những lỗ hổng trên, kẻ tấn công có thể thực hiện các loại tấn công DDoS đến kiến trúc mạng SDN. Một số loại tấn công cơ bản bao gồm:

1. Làm tràn ngập gói tin (Packet_in flooding): kẻ tấn công gửi nhiều gói tin đến vswitch bằng cách giả mạo IPs và buộc vswitch gửi tin nhắn packet_in số lượng lớn đến bộ điều khiển và làm cho bộ điều khiển trở nên quá tải không còn khả năng xử lý những yêu cầu của người dùng hợp pháp.

2. Giả mạo Switch(Spoofing of Switch): kẻ tấn công giả mạo địa chỉ IPs và thiết lập kênh liên lạc với bộ điều khiển dẫn đến bộ điều khiển sẽ chấm dứt giao tiếp với bộ chuyển mạch hợp pháp để chuyển sang giao tiếp với bộ chuyển mạch độc hại và làm giảm hiệu suất mạng.

3. Tràn bảng lưu lượng (Flow Table Overflow): với phương pháp thiết lập động, OpenFlow trong mặt phẳng điều khiển sẽ liên tục thiết lập những chính sách mới cho các gói tin được chuyển đến, thông tin về chính sách mới được lưu trữ trong các bảng lưu lượng và chỉ có giá trị trong thời gian nhất định. Trong trường hợp, kẻ tấn công gửi nhiều luồng giả mạo đến các bộ chuyển mạch và bảng lưu lượng của switch sẽ hết bộ nhớ trong thời gian ngắn và sẽ chỉ có các quy tắc giả mạo trong đó. Tất cả các mục nhập hợp lệ sẽ bị xóa khỏi bảng quy trình và hạ cấp hiệu suất.

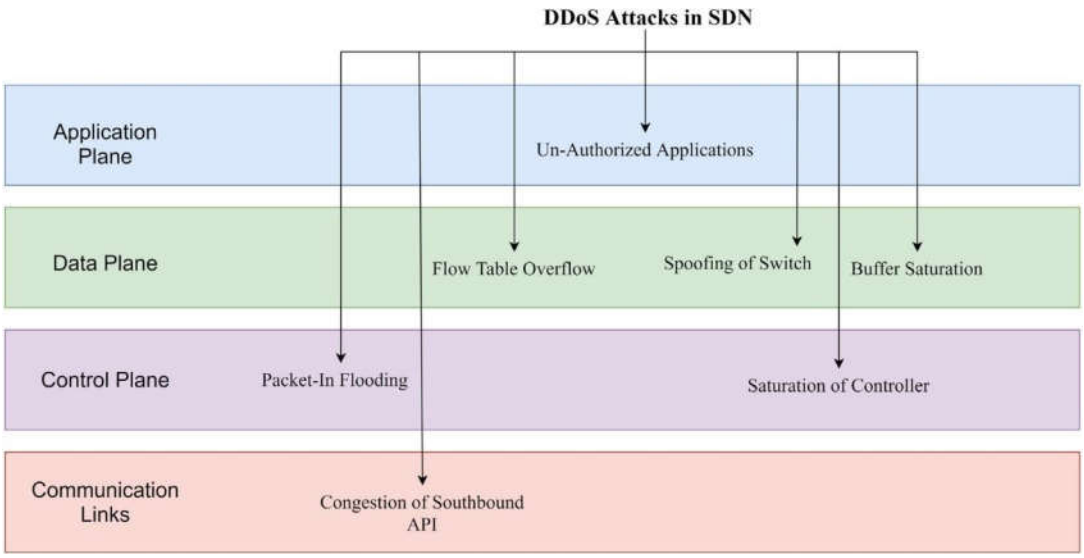
4. Sự tắc nghẽn của các API hướng Nam (Congestion of Southbound APIs): kẻ tấn công gửi nhiều luồng giả mạo đến bộ chuyển mạch làm quá tải băng thông duy nhất được sử dụng bởi các APIs hướng nam và tạo tắc nghẽn.

5. Độ bão hoà của bộ điều khiển (The Controller Saturation: Bộ điều khiển cần làm việc theo thời gian thực để tạo ra các quy tắc điều khiển các gói tin đến, bởi vậy kẻ tấn công có để tạo nhiều luồng giả để làm quá tải bộ điều khiển.

6. Bão hoà bộ nhớ đệm (Buffer Saturation: Bộ nhớ đệm được sử dụng để lưu các packet_in trước trong khi đợi quy tắc mới được thiết lập bởi bộ điều khiển. Khi lượng request quá lớn cũng sẽ dẫn đến bão hoà bộ nhớ đệm.

7. Ứng dụng không được xác thực (Un-authorized Applications: kẻ tấn công có sử dụng một số ứng dụng trái phép truy cập vào tài nguyên của hệ thống thông qua các ứng dụng hợp pháp (đã được cấp phép).

Những phần màu đỏ trong Hình 4 là các lỗ hổng dễ dàng bị khai thác và tấn công; Hình 5 mô tả một cách chính xác vị trí của các lỗ hổng trên các tầng của kiến trúc SDN.



Hình 5. Các kiểu tấn công DDoS ở các lớp khác nhau của SDN

4. CÁC GIẢI PHÁP PHÁT HIỆN VÀ GIẢM THIỂU THIỆT HẠI TẤN CÔNG DDOS TRONG SDN

Đã có rất nhiều nghiên cứu quan tâm đến vấn đề về phát hiện và phòng chống tấn công DDoS trong mạng SDN. Trong phần này, chúng tôi sẽ tổng hợp các kỹ thuật được áp dụng để đưa ra các giải pháp phát hiện và giảm thiểu thiệt hại trong các cuộc tấn công DDoS.

Tuỳ vào tiêu chí và cơ chế được sử dụng, các giải pháp phát hiện DDoS đến nay được phân thành một số loại, cụ thể như sau: (i) Giải pháp phòng chống DDoS dựa trên lý thuyết thông tin, (ii) Giải pháp phòng chống DDoS dựa trên học máy, (iii) Giải pháp phòng chống DDoS dựa trên mạng trí tuệ Nơron nhân tạo. Một số tiêu chí sử dụng trong đánh giá các giải pháp phát hiện DDoS là: *(1) năm xuất bản, (2) phạm vi của giải pháp (phát hiện, giảm thiểu, v.v.), (3) thuật toán/không gian được sử dụng,(4) các thông số được quan tâm, (5) mặt phẳng bị tấn công và (6) nội dung chính của các nghiên cứu.*

4.1. Các giải pháp phát hiện DDoS sử dụng lý thuyết thông tin trong SDN

Lý thuyết thông tin dựa trên các phép đo Entropy và không gian phân kỳ được sử dụng một cách rộng rãi để phát hiện tấn công DDoS trong SDN. Entropy đại diện cho đặc tính ngẫu nhiên về tính năng mạng và không gian phân kỳ cho phép biểu diễn sự giống nhau của hai phân phối xác suất. Bằng cách sử dụng Entropy và không gian phân kỳ trong phân tích số liệu có thể thấy hành vi của mạng hiện tại có sự khác biệt gì so với hành vi của mạng thông thường hay không, từ đó cho thấy những dấu hiệu của các cuộc tấn công DDoS. Bảng 2 tóm tắt các nghiên cứu sử dụng lý thuyết thông tin trong phát hiện và phòng chống các cuộc tấn công DDoS trong SDN

Bảng 2. Một số giải pháp phát hiện tấn công DDoS sử dụng lý thuyết thông tin

STT	Tác giả, năm	Phạm vi	Thuật toán	Thông số	Mặt phẳng tấn công	Nội dung chính
1	Botie và các cộng sự [13] (2017)	Phát hiện Giảm nhẹ	Shannon Entropy	IP nguồn IP đích Cổng Nguồn Cổng Đích	Ứng dụng Điều khiển Dữ liệu	- Mô-đun giám sát dựa trên trạng thái được sử dụng để nắm bắt lưu lượng từ các thiết bị chuyển mạch dựa trên quá trình xử lý trạng thái trong chuyển đổi. - Mô-đun giảm thiểu sẽ cài đặt các quy tắc luồng mới cho các luồng độc hại.
2	Tsai và các cộng sự [7] (2017)	Giảm thiểu Phát hiện	Entropy Shannon	IP đích	Điều khiển	- Ứng dụng chạy trên bộ điều khiển sẽ giám sát lưu lượng truy cập đến và tính toán entropy để tìm độ lệch trong lưu lượng mạng. - Nếu phát hiện ra cuộc tấn công, nó sẽ giúp thực hiện chiến lược giảm thiểu để chặn cổng cụ thể.
3	Kalkan và các cộng sự [10] (2018)	Giảm thiểu Phát hiện	Entropy	IP nguồn IP đích	Điều khiển	- Khi phát hiện tắc nghẽn, switch gửi thông tin của các gói đến bộ điều khiển và bộ điều khiển sẽ tính toán entropy của các cặp và chỉ ra sự khác biệt giữa các giá trị entropy vượt quá ngưỡng, cuộc tấn công DDoS được phát hiện. - Giai đoạn giảm thiểu chủ động thực hiện năm chức năng như Tạo hồ sơ cặp IP đáng ngờ, Tính điểm, Xác định ngưỡng, Tạo quy tắc để giảm thiểu các cuộc tấn công.
4	Sahoo và các cộng sự [5] (2018)	Phát hiện	Entropy tổng quát	IP đích	Điều khiển	- Tác giả sử dụng khoảng cách thông tin như một thước đo để định lượng độ lệch của các luồng lưu lượng mạng.

						- Sử dụng hai mô-đun trong bộ điều khiển, mô-đun thu thập thống kê và mô-đun phát hiện bất thường.
5	Sahoo và các cộng sự [8] (2018)	Phát hiện	Entropy Shannon GE GID KL-phân kỳ	IP đích	Điều khiển	- Sử dụng các thước đo lý thuyết thông tin để phân biệt các sự kiện chớp nhoáng từ các cuộc tấn công DDoS tốc độ cao

4.2. Các giải pháp phát hiện DDoS sử dụng học máy trong SDN

Một số phương pháp thường được sử dụng là Support Vector Machine (SVM), Mô hình Markov ẩn (Hidden Markov Model - HMM), Cây quyết định (Decision Tree - J48), Advanced Support Vector Machine (SVM), Naive Bayes Logistic regression, Random Trees, Binary Bat algorithm, Random forest, và K-nearest neighbour (KNN). Rất nhiều nghiên cứu đã áp dụng các thuật toán này trong phát hiện tấn công DDoS như được tóm tắt trong Bảng 3.

Bảng 3. Một số giải phát phát hiện và giảm thiểu tấn công DDoS sử dụng học máy

STT	Tác giả năm	Phạm vi	Thuật toán/Chỉ số phát hiện	Thông số	Mặt phẳng	Nội dung chính
1	Hu và các cộng sự [15] (2017)	phát hiện Giảm nhẹ	SVM Shannon entropy (Lựa chọn tính năng)	IP nguồn Cổng nguồn IP đích, Giao thức cổng đích	Điều khiển	- Phương pháp này phát hiện và giảm thiểu tấn công tràn ngập bằng cách sử dụng phân loại entropy và SVM. - Entropy được sử dụng để xác định những thay đổi trong mạng. - Mô-đun Phát hiện DDoS thực hiện ba nhiệm vụ: thu thập thông tin, trích xuất tính năng và phát hiện tấn công - Cơ chế giảm thiểu tấn công được triển khai dựa trên danh sách trắng và cập nhật động các quy tắc chuyển tiếp.
2	Dehkordi và các cộng sự [14]	Phát hiện	BayesNet J48 Hồi quy logisticcây	Số Packet_in tin nhắn	Điều khiển	- Hệ thống này so sánh các tính năng mạng với các giá trị ngưỡng được xác định trước để phát hiện tấn công DDoS.

	(2017)		ngẫu nhiên	Tốc độ yêu cầu lưu lượng Thời lượng		- Các mô hình học máy kết hợp với tương quan để tăng độ chính xác của hệ thống hiện có.
3	Li và các cộng sự [16] (2018)	phát hiện	Thuật toán nhị phân Bat Rừng ngẫu nhiên	Bộ tính năng động	Điều khiển	- Các tác giả đã đề xuất một IDS hai giai đoạn giúp phát hiện sự bất thường trong mạng một cách thông minh bằng cách nắm bắt các luồng mạng. - Thuật toán Bat được sử dụng để chọn các tính năng từ các luồng mạng.
4	Guozi và các cộng sự [17] (2018)		φ-Entropy	Thời gian trung bình φ-entropy của IP nguồn φ-entropy của IP đích		- Trích xuất các tính năng bằng cách sử dụng năm đặc điểm từ dữ liệu được cung cấp bởi mô-đun thu thập bảng lưu lượng. - Trình phân loại KNN được sử dụng để phân loại mạng hiện tại là lưu lượng truy cập bất thường hoặc bình thường theo kết quả.
5	Deepa và các cộng sự [18] (2019)	Phát hiện	KNN SVM Naive Bayes	Thời gian khác biệt	Điều khiển	- Các tác giả đề xuất một quần thể Phương pháp phát hiện hành vi bất thường lưu lượng dữ liệu trong bộ điều khiển SDN. - Tác giả kết hợp KNN-SOM, NV-SOM và SVM-SOM và nhận thấy rằng SVM-SOM tạo ra khả năng phát hiện cao hơn tỷ lệ và độ chính xác.

4.3. Các giải pháp phát hiện DDoS sử dụng mạng Nơron nhân tạo trong SDN

Mạng Nơron nhân tạo (ANN) có khả năng tự học, tự tổ chức, khả năng chịu lỗi tốt hơn và mạnh mẽ hơn, tính song song là những ưu điểm của nó nên được nhiều nhà nghiên cứu quan tâm và sử dụng để phát hiện các cuộc tấn công DDoS. Tóm tắt các phương pháp tấn công DDoS sử dụng mạng Nơron nhân tạo được trình bày trong bảng 4.

Bảng 4. Một số giải pháp phát hiện tấn công DDoS sử dụng mạng Nơron nhân tạo

STT	Tác giả năm	Phạm vi	Thuật toán	Thông số	Mặt phẳng	Nội dung chính
1	Cui và các cộng sự [19] (2016)	Giảm thiểu Phát hiện	STORM	Số lượng gói trên mỗi luồng Số byte mỗi luồng Khoảng thời gian Tốc độ gói trên mỗi luồng Tốc độ byte trên mỗi luồng	Điều khiển	- Mô-đun kích hoạt phát hiện tấn công DDoS tăng tỷ lệ phản hồi kích hoạt sự kiện. - Kỹ thuật BPNN được sử dụng để phát hiện sự bất thường trong lưu lượng sau khi được kích hoạt bởi mô-đun kích hoạt phát hiện tấn công. - Mô-đun giảm thiểu chặn lưu lượng để giảm thiểu tác động của mô-đun đang diễn ra theo hướng của mô-đun phát hiện.
2	Xu và các cộng sự [17] (2016)	phát hiện	SOM	Số gói trên mỗi nguồn Số byte trên mỗi nguồn Số gói không đối xứng từ nguồn Số lượng byte không đối xứng từ nguồn	Điều khiển	- Quy trình phát hiện nạn nhân bằng cách sử dụng tính năng thể tích dòng chảy và tính năng không đối xứng tốc độ dòng chảy. - Sau khi phát hiện, quy trình phát hiện kẻ tấn công sử dụng bộ phân loại dựa trên SOM để xác định cuộc tấn công.
3	Cui và các cộng sự [20] (2018)	Giảm thiểu Phát hiện	BPNN	Số gói trên mỗi luồng Số luồng trên mỗi cổng Khoảng thời gian	Điều khiển	- Trích xuất hành vi tạm thời của một cuộc tấn công và mạng thần kinh lan truyền ngược được đào tạo để trích xuất mô hình tấn công. - Mô-đun phòng thủ tấn công đẩy một mục nhập luồng đến công tắc OF tương ứng, sau đó công tắc này loại bỏ tất cả các gói đến cổng cụ thể của nạn nhân.

4	Lý và các cộng sự [1] (2018)	Phát hiện Giảm nhẹ	CNN RNN LSTM	Cổng nguồn cảng đích Cổng nguồn IP đích IP nguồn	Dữ liệu	- Mạng thần kinh CNN, RNN và LSTM Các mô hình được sử dụng để phát hiện tấn công trong mạng. - Mô-đun Deep Learning DDoS Detector sử dụng mô hình deep learning đã được đào tạo để phát hiện xem các gói được nhập trong công tắc OpenFlow hiện tại có phải là gói tấn công hay không. - Gói tấn công sẽ được chuyển tiếp đến mô-đun Thống kê thông tin cho mục đích thống kê; nếu không, nó sẽ không được xử lý.
5	Nam cộng sự . [22] (2018)	Giảm thiểu Phát hiện	SOM	Entropy của IP nguồn Entropy của cổng đích Entropy của giao thức gói tin Tổng số gói tin	Điều khiển	- Mô-đun giám sát thu thập thông tin lưu lượng từ các công tắc và sau đó xử lý chuyển tiếp đến mô-đun Thuật toán. - Mô-đun thuật toán phân loại trạng thái mạng là bình thường hoặc đang bị tấn công. - Mô-đun giảm thiểu tạo ra các chính sách mới và chuyển tiếp các quyết định này tới các thiết bị chuyển mạch cũng như máy chủ.

4.4. Đánh giá các kỹ thuật giảm thiểu DDoS trong SDN

Giảm thiểu tấn công DDoS cũng là một khía cạnh quan trọng để bảo vệ tài nguyên mạng đang bị tấn công. Các nhà nghiên cứu đã sử dụng nhiều kỹ thuật như di chuyển kết nối, di chuyển gói, hạn chế băng thông luồng vào, điều chỉnh thời gian chờ và phương pháp điều khiển các giao thức truyền thông, v.v. Bài báo này đã tóm tắt các phương pháp giảm thiểu các cuộc tấn công từ chối dịch vụ phân tán, mỗi phương pháp đều có những đặc trưng riêng cần xem xét và giải quyết.

* Các giải pháp dựa trên lý thuyết thông tin sử dụng các giá trị ngưỡng được xác định trước (tùy thuộc vào hoạt động của mạng cơ sở) để phát hiện sự bất thường. Do các mạng dựa trên SDN chưa được triển khai công khai nên để xác định hành vi cơ bản chính xác của các mạng dựa trên SDN là một thách thức đối với các nhà nghiên cứu. Bên cạnh đó, việc không có sẵn các bộ dữ liệu chuẩn để thể hiện lưu lượng truy cập bình

thường và khi bị tấn công cũng là vấn đề mở cần giải quyết. Các nhà nghiên cứu đã sử dụng một số công cụ tạo lưu lượng để mô hình hóa lưu lượng thông thường tuy nhiên nó không thể phản ánh chính xác được tốc độ mạng ngày nay. Những công cụ này không thể tạo ra một tỷ lệ thích hợp của lưu lượng truy cập nền, thông thường và tấn công. Vì vậy, dự đoán chính xác về hành vi mạng cơ sở cũng là một lỗ hổng nghiên cứu trong các giải pháp hiện có.

* Các giải pháp dựa trên các kỹ thuật học máy cần bộ dữ liệu thể hiện lưu lượng truy cập bình thường để huấn luyện máy học phát hiện DDoS. Việc không có bộ dữ liệu lưu lượng truy cập bình thường thực sự của mạng SDN cũng là một thách thức đối với các kỹ thuật này. Các nhà nghiên cứu đã sử dụng các tập dữ liệu tổng hợp để huấn luyện máy học, tuy nhiên nó không đảm bảo độ chính xác như dữ liệu được thu thập trong thực tế. Bởi vậy, huấn luyện máy học một cách chính xác các hành vi bình thường là một trong những vấn đề cần phải đương đầu.

* Giải pháp phát hiện và giảm thiểu DDoS dựa trên Mạng nơron nhân tạo (ANN) cần sử dụng nhiều tham số để tính toán trạng thái hiện tại của mạng. Hầu hết các giải pháp bảo mật này được triển khai trên mặt phẳng điều khiển của kiến trúc SDN. Bộ điều khiển tập trung chịu trách nhiệm hoạch định chính sách; nó có thể phục vụ tới 20 000 yêu cầu luồng mới nếu nó đang quản lý 150 thiết bị chuyển mạch, vì vậy bộ điều khiển phải làm việc rất nhiều để xử lý lưu lượng mạng một cách hiệu quả. Tuy nhiên, chi phí tính toán bổ sung này của nhiều tham số có thể ảnh hưởng đến hiệu suất của bộ điều khiển. Vì vậy, số lượng tham số được sử dụng để phát hiện DDoS có thể giảm trong các phương pháp dựa trên ANN.

5. KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

Sự phát triển nhanh chóng của các ứng dụng và các dịch vụ trên Internet đồng thời cũng dẫn đến những mối đe doạ tiềm ẩn về vấn đề bảo mật. SDN là một cách tiếp cận mới, một trong những giải pháp mạnh mẽ và đáng tin cậy bởi khả năng linh hoạt trong việc thích ứng toàn cục đối với sự phát triển bền vững của Internet cùng với các dịch vụ của nó. SDN phân chia chức năng của các lớp một cách rõ ràng và đơn giản hoá quá trình quản lý, mang lại sự đổi mới trong bảo mật mạng. Tuy nhiên, kiến trúc SDN cũng đặt ra những thách thức không nhỏ trên khía cạnh đảm bảo an toàn an ninh mạng đối với các cuộc tấn công DDoS.

Bài báo này, cung cấp một cái nhìn tổng quan về kiến trúc phân lớp SDN cùng với những điểm mạnh của nó trong việc phát hiện và phòng thủ các cuộc tấn công DDoS. Ngoài ra, chúng tôi cũng phân tích những lỗ hổng bảo mật của kiến trúc này dẫn đến các cuộc tấn công DDoS mới. Bộ điều khiển là thành phần chịu trách nhiệm cao nhất kiến trúc SDN và là một trong những mục tiêu lớn nhất

của các cuộc tấn công. Một số khía cạnh khác nhau trong kiến trúc SDN cần được quan tâm và xử lý như không có sẵn bộ điều khiển, khả năng mở rộng, bảo mật của chuyển mạch SDN và liên kết truyền thông, sự phụ thuộc vào bộ điều khiển trung tâm, v.v. Một số phương pháp tấn công DDoS đang được sử dụng phổ biến bao gồm, các phương pháp sử dụng lý thuyết thông tin, sử dụng phương pháp học máy và sử dụng mạng trí tuệ Nơron nhân tạo.

Đã có nhiều nghiên cứu đề cập đến nội dung về phát hiện và giảm thiểu tác hại của các cuộc tấn công DDoS. Tuy nhiên, các nghiên cứu vẫn còn đang ở chế độ rời rạc, chưa hình thành được phương pháp giải quyết một cách tổng quan. Bởi vậy, chúng tôi sẽ tiếp tục nghiên cứu và xây dựng một frame-work để giảm thiểu được chi phí hoạt động của bộ điều khiển cũng như phòng chống được các cuộc tấn công DDoS trong thời gian thực.

TÀI LIỆU THAM KHẢO

1. Zhao, T., Wang, Y., Liu, J., Cheng, J., Chen, Y., & Yu, J. (2021). Robust continuous authentication using cardiac biometrics from wrist-worn wearables. IEEE Internet of Things Journal, 9(12), 9542-9556.

2. Sahoo, K. S., Puthal, D., Tiwary, M., Rodrigues, J. J., Sahoo, B., & Dash, R. (2018). An early detection of low rate DDoS attack to SDN based data center networks using information distance metrics. Future Generation Computer Systems, 89, 685-697.

3. A. Tootoonchian, Y. Ganjali (2010), "Hyperflow: A distributed control plane for openflow," in *Internet Network Management Conference on Research on Enterprise Networking*.

4. "Global number of internet users 2005-2022 (2023)," Ani Petrosyan, 23 02 2023. [Online]. Available: https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/. [Accessed 14 03 2023].

5. K.S. Sahoo and et al. (2018), "An early detection of low rate DDoS attack to SDN based data center networks using information distance metrics," in *Future Gener. Comput. Syst*.

6. S. Shin, G. Gu (2013), "Attacking software-defined networks: A first feasibility," in *Proceedings of the Second ACM SIGCOMM Workshop on Hot*.

7. S.-C. Tsai and et al. (2017), "Defending cloud computing environment against the challenge of DDoS attacks based on software defined network," in *Advances in Intelligent Information Hiding and Multimedia Signal Processing*.

8. K.S. Sahoo and et al. (2018), "Detection of high rate DDoS attack from flash events using information metrics in software defined networks," in *10th International Conference on Communication Systems*.

9. S. Khan and et al(2016), "FML: A novel orensics management layer for software defined networks," in *6th International Conference-Cloud System and Big Data Engineering*.

10. K. Kalkan,and et al. (2018), "JESS: Joint entropy-based DDoS defense

scheme in SDN," in *IEEE J. Sel. Areas Commun*.

11 N. McKeown and et al. (2008), "OpenFlow: enabling innovation in campus," in *Rev. 38*.

12. Campbell and et al. (1999), "Survey of programmable networks," *CM SIGCOMM Computer Communication Review,* vol. 29, pp. 7--23.

13. J. Boite and et al. (2017), "V. Conan, Statesec: Stateful monitoring for DDoS protection in software defined networks," in *IEEE Conference on Network Softwarization*.

14. A. D. et al. (2018), "A New DDoS Detection Method in Software Defined Network," in *IEEE Internet Things J*.

15. D. H. et al. (2017), "FADM: DDoS flooding attack detection and mitigation system in software-defined networking," in *GLOBECOM IEEE Global Communications Conference*.

16. J. L. et al. (2018), "AI-based two-stage intrusion detection for software defined IOT networks," in *IEEE Internet Things J*.

17. S. G. et al. (2018), "DDoS attacks and flash event detection based on flow characteristics in SDN," in *IEEE International Conference on Advanced Video and Signal Based Surveillance*.

18. V. D. et al. (2019), "Design of ensemble learning methods for DDoS detection in SDN environment," in *International Conference on Vision Towards Emerging Trends in Communication and Networking*.

19. Y. C. et al. (2016), "SD-Anti-DDoS: Fast and efficient DDoS defense in software-defined networks," *J. Netw. Comput. Appl.*

20. J. C. et al. (2018), "TDDAD: Time-based detection and defense scheme against DDoS attack on SDN controller," in *Australasian Conference on Information Security and Privacy*.

21. C. L. e. al. (2020), "Detection and defense of DDoS attack-based on deep learning in OpenFlow-based SDN," *Int. J. Co* CNN *mmun. Syst*.

22. T. N. et al. (2018), "Self-organizing map-based approaches in DDoS flooding detection using SDN," in *International Conference on Information Networking*.

23. N. B. et al. (2016), "Application layer DDoS attack defense framework for smart city using SDN," in *The Third International Conference on Computer Science, Computer Engineering, and Social Media*.