NGHIÊN CỨU VÀ PHÂN TÍCH BẢO MẬT TRONG SOFWARE DEFINED NETWORKING

Nguyễn Minh Thắng[1]
[1]*Trường Đại học Kinh tế - Tài chính TP. HCM, Việt Nam, thangnm@uef.edu.vn*

Tóm tắt*: Trong thời đại công nghệ ảo hóa hiện nay, mô hình kiến trúc mạng truyền thống đã dần không còn phù hợp với nhu cầu của các doanh nghiệp, trường học. Việc chuyển giao giữa cách quản lý hệ thống mạng thủ công sang tự động hóa đã đòi hỏi một mô hình mạng mới ra đời. Sự xuất hiện của Sofware-defined networking (SDN) giúp người quản trị viên đơn giản hóa việc quản lý hệ thống mạng thông qua phần mềm Controller và thúc đẩy khả năng lập trình của mạng, do đó cho phép kích hoạt các chức năng bảo mật trong hệ thống mạng. Trong bài báo này, chúng tôi sẽ trình bày các tính năng của SDN và nghiên cứu, phân tích các khía cạnh về bảo mật trong SDN.*

Từ khóa*: Sofware defined networking (SDN), bảo mật mạng, OpenFlow.*

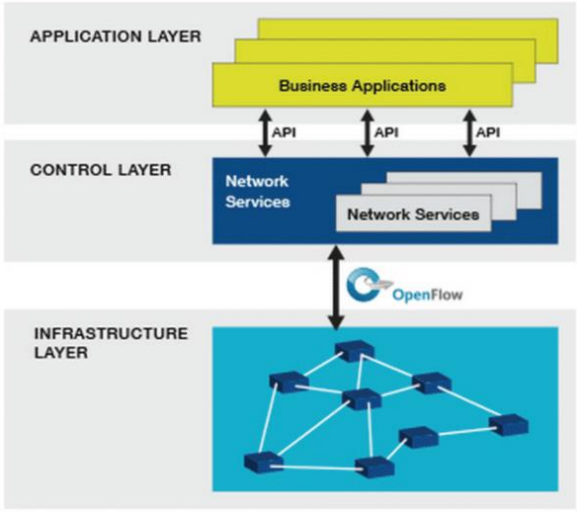
Abstract*: The traditional network architecture model is becoming no longer adequate for the demands of businesses and institutions in the present virtualization technology age. The transition from manual to automated network administration necessitated the creation of a new network model. Software-defined networking (SDN) is a networking technology that allows administrators to simplify network management by using the network's programmability and enabling security features. the network's security We will describe the features of SDN in this post, as well as study and analyze the security issues of SDN.*

Keywords*: Sofware defined networking (SDN), Network Security, OpenFlow.*

1. Giới thiệu

Hiện nay, nhu cầu sử dụng của người dùng cuối (End-User) ngày càng cao và hình thức quản trị hệ thống đã được thay đổi rất nhiều trong những năm qua. Hệ thống mạng cần phải đáp ứng việc thay đổi nhanh chóng về băng thông , định tuyến, độ trễ, bảo mật, … SDN (Sofware-Defined Networking) nổi lên là một công nghệ mới đầy hứa hẹn cho hệ thống mạng tương lai, với một bộ điều khiển trung tâm (Controller) được tách riêng với dữ liệu cho phép người quản trị dễ dàng thay đổi, cập nhật cấu hình mạng thông qua giao diện lập trình ứng dụng (APIs) [1].

SDN được coi là một trong những công nghệ quan trọng để triển khai mạng 5G, thúc đẩy sự phát triển của mạng truyền thông [2]. Với SDN, người quản trị có thể kiểm soát các luồng dữ liệu mạng và giám sát trạng thái mạng một cách dễ dàng. Ví dụ, bằng cách sử dụng SDN, người quản trị có thể dễ dàng thực hiện chức năng cân bằng tải mạng mà các kỹ thuật hiện có khó có thể thực hiện và tốn kém chi phí [3].



Hình 1. *Kiến trúc SDN*

OpenFlow là một giao thức truyền thông cho phép bộ điều khiển mạng (controller) xác định đường truyền của gói tin trong mặt phẳng chuyển tiếp giữa các thiết bị mạng như Router, Switch kể cả thiết bị vật lý và thiết bị ảo, do đó giúp di chuyển phần điều khiển mạng ra khỏi các thiết bị chuyển mạch thực tế tới phần mềm điều khiển trung tâm [3]. Theo như Hình 1, SDN sẽ tập trung vào các tính năng chính như sau:

- Phân biệt thành 3 lớp rõ ràng: lớp ứng dụng, lớp điều khiển trung tâm, lớp kiến trúc mạng thông qua các APIs.
- Cấu hình mới, thay đổi cấu hình đều thông qua khả năng lập trình.
- Tăng tính bảo mật và độ tin cậy với khả năng hiển thị và kiểm soát thông qua giao diện controller.

SDN là một kiến trúc mạng sáng tạo, hiệu quả về tính mở, tập trung quản lý và có thể lập trình được, nhưng SDN cũng có những thách thức và hạn chế riêng. Ví dụ, một bộ điều khiển tập trung logic có thể nắm được toàn bộ tình hình mạng, nhưng lại có nhiều khả năng gây ra lỗi một điểm, bị chiếm quyền điều khiển hoặc không thể hoạt động, khiến toàn bộ hệ thống mạng bị sập [2]. Do áp dụng điều khiển tập trung và sử dụng các bảng quy trình phức tạp, SDN đã trở thành mục tiêu dễ bị tấn công của các cuộc tấn công từ chối dịch vụ (DoS). Ngoài những điều trên, làm thế nào để quản lý nhiều ứng dụng trong một mặt phẳng ứng dụng để phát hiện các ứng dụng độc hại và không đáng tin cậy vẫn là một thách thức lớn trong mô hình mạng mới dựa trên SDN [4].

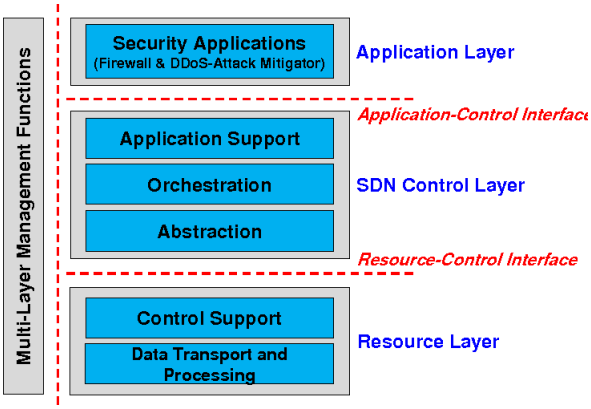
Trong bài báo này, chúng tôi sẽ trình bày mô hình kiến trúc, các đặc điểm của SDN, đồng thời phân tích tính bảo mật trong SDN. Cấu trúc bài báo như sau: Trong phần 2, chúng tôi chúng tôi giới thiệu các đặc điểm của SDN và phân tích các mối đe dọa mà nó phải đối mặt. Trong phần 3, chúng tôi mô tả các vấn đề bảo mật mà mỗi lớp và giao diện phải đối mặt, các giải pháp bảo mật hiện tại sẽ được thảo luận trong phần 4. Cuối cùng là phần kết luận và hướng nghiên cứu tương lai.

2. SDN Security Analyses

SDN là một bản nâng cấp mang tính cách mạng trên các mạng truyền thống. Kiến trúc của nó khá khác so với những kiến trúc truyền thống. Năm đặc điểm cụ thể của SDN trong Hình 2 tạo điều kiện cho kẻ tấn công có thể thực hiện ba cuộc tấn công khác nhau để xâm phạm mặt phẳng dữ liệu bao gồm Device Acttack (tấn công thiết bị), Protocol Attack (tấn công giao thức) và Side Channel Attack (tấn công kênh bên) [5].

Hình 2. *Năm đặc điểm chính liên quan đến bảo mật của SDN đặt ra các vấn đề bảo mật*

Câu hỏi đặt ra là liệu SDN có khả năng khắc phục các vấn đề bảo mật, độ tin cậy, khả năng mở rộng như đã có hoặc được thừa kế từ các mạng truyền thống hay không. Khi SDN thu hút được nhiều sự chú ý hơn, các đánh giá bảo mật và kiểm tra sẽ được thực hiện trên mô hình mới. Hayward và các cộng sự đã khảo sát những vấn đề liên quan đến bảo mật, những thách thức và những cải tiến bảo mật có được từ việc sử dụng SDN [6].



Hình 3. *Kiến trúc các dịch vụ bảo mật trên SDN*

Hình 3 là một khung mẫu cho các dịch vụ bảo mật dựa trên SDN. Như thể hiện trong hình, các ứng dụng cho các dịch vụ bảo mật (tường lửa và trình giảm thiểu tấn công DDoS) chạy thông qua tương tác với bộ điều khiển SDN [7]. Khi quản trị viên thực thi các chính sách bảo mật cho các dịch vụ bảo mật thông qua giao diện ứng dụng, bộ điều khiển SDN tạo ra các quy tắc chính sách kiểm soát

truy cập tương ứng (hoặc cấu hình mạng) để đáp ứng các chính sách bảo mật đó một cách tự chủ và nhanh chóng. Theo các quy tắc chính sách kiểm soát truy cập đã tạo, các tài nguyên mạng, chẳng hạn như bộ chuyển mạch và bộ định tuyến, thực hiện hành động để giảm thiểu các cuộc tấn công mạng, chẳng hạn như thả các gói có các mẫu đáng ngờ [8].

SDN luôn đối mặt với rất nhiều loại tấn công, chúng tôi chia ra thành năm mối đe dọa mà SDN có thể phải gặp: Spoofing, Tampering, Repudiation, Information Disclosure and Denial of Service.

3. SDN Layers' Security Issues

Theo như Hình 1, kiến trúc của SDN gồm có 3 lớp, với mỗi lớp sẽ có những mối đe dọa khác nhau mà nó phải đối mặt.

3.1. Application Layer Security (ALS)

Lớp ứng dụng tương tác trực tiếp với lớp điều khiển thông qua giao diện API. Vì không có tiêu chuẩn và thông số kỹ thuật cụ thể nên ứng dụng có thể gây ra mối đe dọa bảo mật nghiêm trọng đối với tài nguyên, dịch vụ và chức năng mạng. Mặc dù lớp ứng dụng cũng có thể phát triển các ứng dụng bảo mật để chống lại các mối đe dọa, nhưng sự không nhất quán trong môi trường phát triển và các mẫu lập trình mạng có thể dẫn đến các vấn đề không thể cưỡng lại như xung đột triển khai chính sách và khả năng tương tác [9]. Các mối đe dọa bảo mật mà lớp ứng dụng phải đối mặt như sau:

Xác thực và ủy quyền: các cơ chế xác thực bảo mật sẽ ngăn chặn các ứng dụng độc hại vì ứng dụng có quyền truy cập tài nguyên mạng và thao tác hành vi mạng, rất khó để thiết lập mối quan hệ đáng tin cậy giữa ứng dụng và bộ điều khiển. Các ứng dụng chạy trên bộ điều khiển sẽ thực thi các chức năng, do đó, một số lượng lớn các xác thực ứng dụng trong mạng có thể lập trình hiện đang là một thách thức bảo mật lớn.

Tiêm mã độc: Các ứng dụng độc hại hoặc bị hỏng có thể tạo ra các quy tắc luồng không chính xác sử dụng thông tin đăng nhập hợp pháp của người dùng để đưa vào mạng và rất khó phát hiện. Lee và cộng sự đã trình bày ba kịch bản tấn công vào lớp ứng dụng: ONOS, OpenDaylight và Floodlight [10].

Kiểm soát truy cập: Các ứng dụng độc hại có thể lợi dụng khâu kiểm soát truy cập hoặc phần mềm phát hiện xâm nhập để vượt qua và xâm nhập vào hệ thống. Ngoài ra, kiểm soát truy cập và trách nhiệm giải trình cho các ứng dụng lồng nhau cũng là một khía cạnh quan trọng.

3.2. Control Layer Secutiry (CLS)

Lớp điều khiển là xương sống của SDN, vì vậy, bảo mật lớp này là rất quan trọng. Logic của lớp điều khiển là tập trung và là nơi thực hiện các quyết định. Do đó, bộ điều khiển trở thành mục tiêu chính của Hacker, lớp điều khiển phải đối mặt với một số mối đe dọa như sau:

Các cuộc tấn công DoS/DDoS: Tấn công DoS/DDoS đã trở thành phương thức tấn công phổ biến của những kẻ tấn công, An và cộng sự đã đề xuất mô hình phân cụm siêu đồ thị dựa trên thuật toán Apriori để mô tả hiệu quả mối liên hệ giữa các nút sương mù đang bị đe dọa từ DDoS [11]. Mặc dù có nhiều giải pháp để giảm thiểu các cuộc tấn công DDoS, nhưng các mối đe dọa vẫn tồn tại, Raghunath và cộng sự đã triển khai lớp cơ chế bảo vệ trong mặt phẳng dữ liệu/lớp chuyển tiếp, lớp này loại bỏ và đưa vào danh sách đen các luồng và máy chủ độc hại, lưu lượng tấn công lớn sẽ bị ngăn chặn xâm nhập vào ngăn xếp SDN, do đó có thể tăng hiệu suất cũng như cung cấp bảo mật hơn trong SDN [12].

Bên thứ ba kiểm soát các thông tin độc hại: Lớp điều khiển thiếu kiểm soát truy cập ứng dụng hiệu quả có thể dẫn đến việc kẻ tấn công chiếm quyền điều khiển. Zhou và cộng sự đã đề xuất sử dụng bộ điều khiển dự phòng để kiểm tra thông tin xử lý của bộ điều khiển chính và bộ chuyển mạch của nó, đồng thời khi có các hành vi xử lý không nhất quán hoặc không mong muốn giữa bộ điều khiển chính với bộ điều khiển dự phòng và Switch thì nó sẽ cảnh báo thiết bị đang bị tấn công [13]. Các chương trình độc hại có thể truy cập và thay đổi tài nguyên mạng một cách bất hợp pháp và các ứng dụng có nhiều cấp độ bảo mật khác nhau phải cung cấp các quyền khác nhau.

Triển khai nhiều bộ điều khiển: nhiều bộ điều khiển có thể quản lý số lượng thiết bị chuyển mạch ngày càng tăng trong mạng đồng thời tránh được các lỗi của bộ điều khiển đơn. Tuy nhiên, Maziku và cộng sự đã chỉ ra rằng việc có các trường hợp tài nguyên tương tự trong nhiều bộ điều khiển SDN khác nhau sẽ làm tăng nguy cơ bảo mật [14].

3.3. Data Layer Security (DLS)

Lớp dữ liệu chỉ mang nhiệm vụ chuyển tiếp dữ liệu và không phân biệt luồng thông thường và luồng độc hại. Do đó, việc phát hiện tính hợp lệ và nhất quán của các quy tắc luồng trong mạng là rất quan trọng đối với sự ổn định và độ tin cậy của mạng SDN. Dưới đây là những lo ngại về bảo mật mà lớp này phải đối mặt:

Tính hợp lệ và nhất quán của các quy định về luồng: Thông qua một Switch hoặc máy chủ lưu trữ độc hại, kẻ tấn công có thể tạo ra một lượng đáng kể lưu lượng truy cập không có thật, giả mạo thông tin bảng luồng hoặc khiến bảng lưu lượng chuyển mạch bị tràn và không hoạt động chính xác.

Từ chối dịch vụ và chiếm quyền điều khiển: Vì bảng lưu lượng chuyển mạch (FlowTable) có một khoảng không gian nhất định nên các cuộc tấn công Flooding trên Switch có thể khiến không gian bảng lưu lượng của Switch trở nên bão hòa, dẫn đến từ chối dịch vụ. Hacker cũng có thể chiếm quyền kiểm soát các Switch, đánh cắp dữ liệu, tạo lưu lượng truy cập độc hại và thực hiện các cuộc tấn công từ chối dịch vụ đối với bộ điều khiển.

4. Các giải pháp bảo mật SDN

4.1 Nâng cao bảo mật SDN Controller

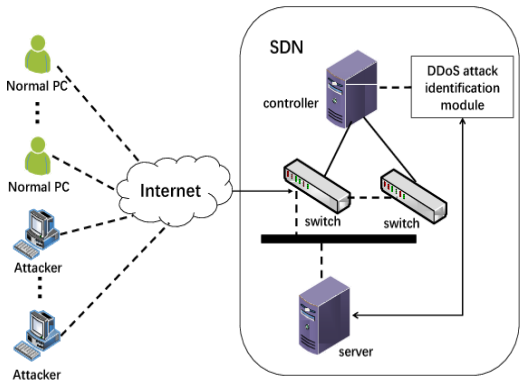
Bộ điều khiển là thiết bị cốt lõi của mặt phẳng điều khiển SDN. Nó quản lý mọi hoạt động của hệ thống mạng. Mạng SDN được đặc trưng bởi việc triển khai nhanh chóng các dịch vụ và bộ điều khiển là một thiết bị quan trọng để cung cấp các chính sách. Cải thiện tính bảo mật của bộ điều khiển là chìa khóa cho toàn bộ mạng SDN. Hiện tại, nó là lớp ứng dụng, việc truy cập bất hợp pháp hoặc gian lận nhận dạng lớp dữ liệu luôn là mối đe dọa của nó.

Abdulqadder và cộng sự đã đề xuất kiến trúc đám mây an toàn (SecSDNcloud) để có thể chống lại ba kiểu tấn công: Flow Table Overloading, Control Plane Saturation and Byzantine Attacks. Sử dụng chữ ký số để xác thực người dùng, sử dụng các giao thức định tuyến nhiều lớp hạt để cải thiện chất lượng dịch vụ và kết hợp các thuật toán di truyền với các thuật toán tìm kiếm Cuckoo cải tiến để hoàn thành việc phân công bộ điều khiển [15].

Abdou và cộng sự đã phân tích các rủi ro bảo mật của mặt phẳng điều khiển do cấu trúc của SDN mang lại và phân tích các thuộc tính mạng điển hình, các mối đe dọa bảo mật và các biện pháp bảo vệ các thuộc tính này giữa mặt phẳng điều khiển SDN và mạng truyền thống [16].

4.2 Ngăn chặn tấn công DoS/DDoS

Các cuộc tấn công DoS/DDoS hiện đang là một vấn đề lớn trong bảo mật SDN, kể tả tấn công từ bên trong lẫn bên ngoài. Hình thức tấn công chủ yếu được sử dụng là nhắm vào giao thức OpenFlow bằng cách giả mạo các gói lưu lượng truy cập giả, yêu cầu các quy tắc chuyển tiếp luồng phản hồi từ bộ điều khiển, bên cạnh đó còn có một số hình thức tấn công phổ biến khác như: ICMP, tràn ngập SYN, tràn ngập HTTP, Ping of Death và Smurf. Cuộc tấn công DoS/DDoS là hiệu quả và trực tiếp. Nó tiêu thụ tài nguyên bộ điều khiển SDN và chiếm băng thông liên kết điều khiển và không gian bảng luồng. Kết quả là, các dịch vụ không thể được thực hiện bình thường. Cách ngăn chặn tốt nhất là phát hiện và phản ứng kịp thời.



Hình 4. *Tấn công DoS/DDoS trong SDN*

De Assis và cộng sự đã so sánh ba phương pháp khác nhau: Particle Swarm Optimization (tối ưu hóa bầy hạt), Multilayer Perceptron Neural Network (mạng nơron perceptron nhiều lớp) và Discrete Wavelet Transform (biến đổi wavelet rời rạc). Sử dụng dữ liệu luồng IP và bộ điều khiển Floodight được thử nghiệm trên phần mềm giả lập Mininet, kết quả là hệ thống phòng thủ đã phát hiện và giảm thiểu được các đợt tấn công [17].

Wu và cộng sự đã đưa ra giải pháp phát hiện tấn công DoS dựa vào 3 yếu tố: sự hỗn loạn thông tin, tốc độ gói tin và tốc độ phản hồi gói tin. Các yêu cầu từ kẻ tấn công sẽ được chuyển đến bộ đệm ẩn của mặt phẳng dữ liệu, điều này giúp giảm bớt bộ đệm giao diện của mặt phẳng điều khiển và cho phép bộ điều khiển xử lý các yêu cầu bình thường một cách hiệu quả [18].

4.3 Tăng tính nhất quán Flow Rule

Vì các quy tắc luồng của SDN thường được tạo ra bởi các ứng dụng khác nhau, các quy tắc này có thể xung đột trong mặt phẳng dữ liệu và gây ra vi phạm chính sách bảo mật, tương tự như xung đột quy tắc tường lửa của mạng IP; loại bỏ xung đột quy tắc nên tạo ra một độ trễ xử lý nhỏ sao cho tất cả các quy tắc của mặt phẳng dữ liệu được xử lý một cách an toàn và chính xác trong thời gian thực [19].

Wan và cộng sự đã giới thiệu một mô hình chức năng bảo mật do phần mềm xác định thông qua một kiến trúc riêng biệt về điều khiển logic và chuyển tiếp dữ liệu. Một phương pháp phát hiện bất thường dựa trên sự kiện cho các giao thức truyền thông không công khai được đề xuất trong hệ thống điều khiển dựa trên SDN [20].

Giao tiếp giữa mặt phẳng dữ liệu và mặt phẳng điều khiển trong SDN có thể gây ra rủi ro bảo mật, chẳng hạn như các cuộc tấn công bão hòa bộ điều khiển và các cuộc tấn công tràn bộ đệm chuyển đổi. Các cuộc tấn công này có thể được bắt đầu bằng cách làm tràn ngập các gói TCP SYN đến mặt phẳng điều khiển thông qua mặt phẳng dữ liệu, Kumar và cộng sự đã đề xuất giải pháp Entropy Safety có thể phát hiện luồng dữ liệu và nằm dưới cuộc tấn công tràn ngập TCP SYN [21].

4.4 Tăng cường bảo mật ứng dụng

Lớp ứng dụng trực tiếp cấu hình bộ điều khiển thông qua giao diện giới hạn phía bắc (North-Bound). Nếu ứng dụng bị kiểm soát độc hại hoặc được cấy ghép các chương trình độc hại, nó sẽ gây ra mối đe dọa cho toàn bộ mạng SDN. Sự can thiệp lẫn nhau hoặc lỗi hoạt động giữa các ứng dụng chung cũng có thể gây ra mối đe dọa.

Varadharajan và cộng sự đã đề xuất chính sách bảo mật kiểm soát luồng thông tin giữa các miền SDN khác nhau để bảo vệ thông tin và dịch vụ SDN cho phép bảo mật chi tiết dựa trên các thuộc tính khác nhau. Các chính sách như thông số người dùng, thiết bị, vị trí và thông tin định tuyến, thuộc tính bảo mật của bộ chuyển mạch và bộ điều khiển giữa các miền khác nhau. Kết quả mô phỏng cho thấy mô hình có thể chống lại các cuộc tấn công thông thường khác nhau [22].

5. Kết luận

Bài báo đã cho thấy những ưu điểm của SDN. Việc tách các mặt phẳng chuyển tiếp và điều khiển làm cho kiến trúc mới này có những lợi thế lớn để hỗ trợ tính linh hoạt và quản lý hệ thống mạng. Tuy nhiên, song song với những ưu điểm đó thì SDN cần phải đảm bảo tính bảo mật và độ tin cậy của nó. Nâng cao tính bảo mật của lớp điều khiển là một hướng nghiên cứu quan trọng trong tương lai. Bài báo đã trình bày các mối đe dọa đến SDN và một số giải pháp để ngăn chặn các đợt tấn công. API mở cũng truyền các mối đe dọa bảo mật từ lớp ứng dụng đến lớp điều khiển và từ lớp điều khiển đến lớp dữ liệu. Các ứng dụng lớp ứng dụng cần một cơ chế kiểm tra ứng dụng hoàn chỉnh để đảm bảo quyền truy cập vào các ứng dụng an toàn và giảm tính bảo mật do các ứng dụng độc hại gây ra.

Tài liệu tham khảo

[1] Yao, Zhen. (2016). Security in Software-Defined-Networking: A Survey. 10066. 319-332. 10.1007/978-3-319-49148-6_27.

[2] Yousaf, F.Z., Bredel, M., Schaller, S., Schneider, F.: NFV and SDN—key technology enablers for 5G networks. IEEE J. Sel. Areas Commun. 35, 2468–2478 (2017).

[3] S. Shin, L. Xu, S. Hong and G. Gu, "Enhancing Network Security through Software Defined Networking (SDN)," 2016 25th International Conference on Computer Communication and Networks (ICCCN), 2016, pp. 1-9, doi: 10.1109/ICCCN.2016.7568520.

[4] M. Yue, H. Wang, L. Liu and Z. Wu (2020), "Detecting DoS Attacks Based on Multi-Features in SDN," in IEEE Access, vol. 8, pp. 104688-104700, doi: 10.1109/ACCESS.2020.2999668.

[5] Shaghaghi A., Kaafar M.A., Buyya R., Jha S. (2020) Software-Defined Network (SDN) Data Plane Security: Issues, Solutions, and Future Directions. In: Gupta B., Perez G., Agrawal D., Gupta D. (eds) Handbook of Computer Networks and Cyber Security. Springer, Cham. https://doi.org/10.1007/978-3-030-22277-2_14

[6] Scott-Hayward, Sandra & O'Callaghan, Gemma & Sezer, Sakir. (2013). SDN security: a survey. Future Networks and Services (SDN4FNS), 2013 IEEE SDN For. 1-7. 10.1109/SDN4FNS.2013.6702553.

[7] Recommendation ITU-T Y.3300, "Framework of Software-Defined Networking," ITU-T, Jun. 2014.

[8] Open Networking Foundation, "SDN Architecture," ONF, Jun. 2014.

[9] Xu, Xiaolong; Hu, Liuyun (2017). A Software Defined Security Scheme Based on SDN Environment. IEEE 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), pp. 504–512. doi:10.1109/CyberC.2017.52.

[10] Guo C., Xie D., Han Y., Guo J., Wei Z. (2020) Survey of Software-Defined Network Security Issues. Artificial Intelligence and Security. ICAIS 2020. Communications in Computer and Information Science, vol 1252. Springer. https://doi.org/10.1007/978-981-15-8083-3_45

[11] Lee, S., Yoon, C., Shin, S.: The smaller, the shrewder: a simple malicious application can kill an entire SDN environment. In: Proceedings of the 2016 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization, New Orleans, Louisiana, USA, pp. 23–28. ACM (2016).

[12] An, X., Su, J., Lü, X., Lin, F.: Hypergraph clustering model-based association analysis of DDOS attacks in fog computing intrusion detection system. EURASIP J. Wirel. Commun. Netw. 2018(1), 1–9 (2018). https://doi.org/10.1186/s13638-018-1267-2

[13] Raghunath, K., Krishnan, P.: Towards a secure SDN architecture. In: 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), pp. 1– 7 (2018)

[14] H. Zhou *et al*., "SDN-RDCD: A Real-Time and Reliable Method for Detecting Compromised SDN Devices," in *IEEE/ACM Transactions on Networking*, vol. 26, no. 5, pp. 2048-2061, Oct. 2018, doi: 10.1109/TNET.2018.2859483.

[15] Abdulqadder, I.H., Zou, D., Aziz, I.T., Yuan, B., Li, W.: SecSDN-cloud: defeating vulnerable attacks through secure software-defined networks. IEEE Access 6, 8292–8301 (2018).

[16] Abdou, A., Van Oorschot, P.C., Wan, T.: Comparative analysis of control plane security of SDN and conventional networks. IEEE Commun. Surv. Tutorials 20, 3542–3559 (2018).

[17] De Assis, M.V., Novaes, M.P., Zerbini, C.B., Carvalho, L.F., Abrãao, T., Proença, M.L.: Fast defense system against attacks in software defined networks. IEEE Access 6, 69620–69639 (2018).

[18] Wu, G., Li, Z., Yao, L.: DoS mitigation mechanism based on non-cooperative repeated game for SDN. In: 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS), Singapore, pp. 612–619. IEEE (2018).

[19] Li, Q., Chen, Y., Lee, P.P., Xu, M., Ren, K.: Security policy violations in SDN data plane. IEEE/ACM Trans. Netw. (TON) 26, 1715–1727 (2018).

[20] Wan, M., Yao, J., Jing, Y., Jin, X.: Event-based anomaly detection for non-public industrial communication protocols in SDN-based control systems. Comput. Mater. Continua 55, 447– 463 (2018).

[21] Kumar, P., Tripathi, M., Nehra, A., Conti, M., Lal, C.: SAFETY: Early detection andmitigation of TCP SYN flood utilizing entropy in SDN. IEEE Trans. Netw. Serv. Manage. 15, 1545–1559 (2018)

[22] Varadharajan, V., Karmakar, K., Tupakula, U., Hitchens, M.: A policy-based security architecture for software-defined networks. IEEE Trans. Inf. Forensics Secur. 14, 897–912 (2018)