**Long Short-Term Memory and Fuzzy Logic for Anomaly Detection and Mitigation in Software-Defined Network Environment**

**Tóm tắt:** Mạng máy tính trở thành những cấu trúc phức tạp và năng động. Kết quả là, việc cấu hình và quản lý toàn bộ cấu trúc này là một nhiệm vụ đầy thử thách. Mạng định nghĩa phần mềm (SDN) là một mô hình mạng mới, thông qua việc trừu tượng các kế hoạch mạng, tìm cách tách rời tầng điều khiển và tầng dữ liệu, và có mục đích vượt qua những hạn chế về cấu hình cơ sở hạ tầng mạng. Như trong môi trường mạng truyền thống, môi trường SDN cũng dễ bị lỗ hổng bảo mật. Công việc này trình bày một hệ thống để phát hiện và giảm thiểu các cuộc tấn công từ chối dịch vụ phân tán (DDoS) và các vụ tấn công Portscan trong môi trường SDN (LSTM-FUZZY). Hệ thống LSTM-FUZZY được trình bày trong tác phẩm này có ba giai đoạn riêng biệt: đặc trưng, phát hiện bất thường và giảm thiểu. Hệ thống đã được thử nghiệm trong hai tình huống. Trong kịch bản đầu tiên, chúng tôi áp dụng dòng IP thu thập được từ bộ điều khiển Floodlight SDN thông qua mô phỏng trên Mininet. Mặt khác, trong kịch bản thứ hai, bộ dữ liệu CICDDoS 2019 đã được áp dụng. Kết quả thu được cho thấy hiệu quả của hệ thống để hỗ trợ quản lý mạng, phát hiện và giảm thiểu sự xuất hiện của các cuộc tấn công.

**Từ khóa:** DDoS, deep learning, fuzzy, LSTM, portscan, SDN.

I. Giới thiệu

Ngày nay, số lượng ứng dụng và dịch vụ sử dụng Internet đã tăng lên nhanh chóng. Hệ thống mạng đã trở thành cấu trúc phức tạp do một số lượng lớn các thiết bị tạo ra chúng, ví dụ, tường lửa, hệ thống phát hiện xâm nhập, cân bằng tải, thiết bị chuyển mạch, bộ định tuyến, v.v. Trong môi trường mạng truyền thống, mỗi tài sản mạng sử dụng các giao thức phức tạp và cấu hình của nó khác nhau giữa các nhà sản xuất. Với sự ra đời của Ðiện toán đám mây và sự gia tăng của các công nghệ ảo hóa, kiến trúc quản lý truyền thống của mạng không ­phù hợp cho các ứng dụng này, đặc biệt là tại các trung tâm dữ liệu hiện tại [1] Mặc dù Mạng được xác định bằng phần mềm (SDN) không được tạo ra với mục tiêu cụ thể cho các chức năng ảo hóa của mạng, nhưng nó là một kiến trúc mạng mới nổi dự kiến các mạng trong tương lai và đáp ứng nhu cầu mới của các ứng dụng hiện có [2], [3]. Ðặc điểm chính của kiến trúc SDN là sự tách biệt giữa mặt phẳng điều khiển và mặt phẳng dữ liệu, có nghĩa là mặt phẳng điều khiển được loại bỏ khỏi thiết bị mạng và tập trung trên bộ điều khiển [4], [5]. Sự tập trung của mặt phẳng điều khiển cung cấp một cái nhìn toàn cầu về mạng và cho phép quản lý các thành phần của nó thông qua một giao diện phần mềm mở và được xác định rõ [6]. Cùng với nhu cầu ngày càng tăng đối với các ứng dụng web và sự phổ biến của các thiết bị IoT (Internet of Things) mới, các vấn đề liên quan đến bảo mật xuất hiện, ví dụ, các cuộc tấn công [7], [8]. Số lượng các cuộc tấn công đã tăng lên về số lượng và sự tinh vi về cách chúng được thực hiện bởi các tác nhân độc hại, đặc biệt là Từ chối Dịch vụ Phân tán (DDoS). Mục đích của DDoS là làm cạn kiệt tài nguyên, ngay cả ở cấp độ máy chủ, nơi kẻ tấn công, thông qua nhiều lần gạ gẫm, cố gắng tước đi một số dịch vụ hoặc ở cấp độ cơ sở hạ tầng nơi kẻ tấn công bão hòa một liên kết mạng [9], [10]. Mặc dù các mạng SDN đã giới thiệu các tài nguyên lập trình và tập trung của logic điều khiển, tạo điều kiện thuận lợi cho việc quản lý, các tài nguyên này là các lỗ hổng bảo mật chính được trình bày bởi kiến trúc mạng [11], [12]. Do kiến trúc mạng SDN, người ta biết rằng việc quản lý các luồng mạng được tập trung và thực hiện bởi một bộ điều khiển, chịu các mối đe dọa bảo mật, ví dụ, các cuộc tấn công DDoS, Portscan, giả mạo IP, v.v. [10], [13]–[16]. Trong một cuộc tấn công DDoS, các dịch vụ mạng bị quá tải do số lượng lớn các yêu cầu được gửi bởi những kẻ tấn công. Bộ điều khiển là điểm trung tâm của mạng SDN và dễ bị tấn công. Bên cạnh đó, các cuộc tấn công DDoS được theo sau bởi các cuộc tấn công Portscan, nơi kẻ tấn công quét các cổng mở để thực hiện xâm nhập. Do đó, bảo mật mạng SDN vẫn chưa được xác định và cần phải phát triển các giải pháp liên quan đến việc phát hiện và giảm thiểu các cuộc tấn công. Trong vài năm qua, với sự gia tăng các mối đe dọa bảo mật và khối lượng lưu lượng truy cập khổng lồ, một số cách tiếp cận đã được đề xuất để phát hiện sự bất thường [17]–[19]. Phát hiện bất thường mạng bao gồm hai cách tiếp cận chính: Dựa trên chữ ký và dựa trên hồ sơ. Ðối với điều đầu tiên, dựa trên Chữ ký, một cơ sở dữ liệu chứa chữ ký của các loại tấn công đa dạng nhất là cần thiết và việc phát hiện một sự kiện bất thường xảy ra khi có "toán học" giữa hành vi của mạng và cuộc tấn công mẫu đã biết. Mặt khác, cách tiếp cận dựa trên hồ sơ, dựa trên dữ liệu lịch sử mạng, một dự đoán về hành vi thông thường của nó được đưa ra và một sự bất thường được phát hiện khi hành vi dự đoán và hành vi thực sự khác biệt với nhau [20]. Một trong những ưu điểm chính của loại phương pháp này là phát hiện các dị thường không xác định, vì hệ thống không yêu cầu học hành vi của nhiều cuộc tấn công hiện có. Hơn nữa, các cuộc tấn công hiện tại rất năng động và các mô hình mới xuất hiện thường xuyên [7], [17]. Do đó, các phương pháp tiếp cận dựa trên Chữ ký yêu cầu chữ ký của các cuộc tấn công được cập nhật mỗi khi một cuộc tấn công mới xuất hiện, dẫn đến một nhược điểm cho hệ thống. Nói chung, các kỹ thuật phát hiện bất thường có ý định thu nhận các mẫu lưu lượng truy cập nhạy cảm thông qua những thay đổi đột ngột về khối lượng truy cập dự kiến hoặc những thay đổi bất ngờ trong việc phân phối các đặc điểm lưu lượng truy cập mạng cụ thể, chẳng hạn như địa chỉ IP và cổng. Việc triển khai các thuật toán Học Máy cung cấp các giải pháp để phát hiện và phân loại các dị thường [21], [22]. Các thuật toán này có khả năng học các mẫu từ một tập hợp dữ liệu và đưa ra dự đoán dựa trên những dữ liệu này. Thông thường, các kỹ thuật Học máy được sử dụng trong các hệ thống phát hiện bất thường được chia thành hai cách tiếp cận: Học nông và Học sâu. Các thuật toán Học tập Nông có một số hạn chế, chẳng hạn như phần lớn phụ thuộc vào các thuộc tính được sử dụng trong quá trình đào tạo và phân tích chuyên sâu là cần thiết để nắm bắt các thuộc tính và số liệu thống kê có liên quan nhất của lưu lượng truy cập [23], [24]. Bên cạnh đó, các mô hình thường cần phải là Ðược đào tạo lại để tìm hiểu các mô hình hành vi mạng mới [25], [26]. Gần đây, các phương pháp dựa trên Deep Learning đã được áp dụng trong nhiều công việc liên quan đến hệ thống phát hiện xâm nhập, do khả năng học tập và khái quát hóa các thuộc tính được sử dụng [27]–[29]. Do đó, chúng tôi trình bày một hệ thống mô-đun để phát hiện và giảm thiểu sự bất thường được áp dụng trên môi trường mạng SDN. Hệ thống được phát triển bao gồm ba mô-đun với các chức năng được xác định rõ ràng. Mô-đun đầu tiên là mô-đun đặc trưng, sử dụng thuật toán Học sâu được gọi là Bộ nhớ ngắn hạn dài (LSTM), một kiến trúc của mạng thần kinh tái phát nhân tạo (RNN), để dự đoán hành vi bình thường của lưu lượng mạng. Mô-đun thứ hai có khả năng đáp ứng để phát hiện các sự kiện bất thường, trong đó bất đẳng thức Bienaymé- Chebyshev được áp dụng để tạo ra sự bình thường- cũ một cách động, và cùng với đó, logic Fuzzy được áp dụng để xác định sự xuất hiện của một sự bất thường trong một thời điểm nhất định của phân tích. Mô xác định sự xuất hiện của một sự bất thường trong một thời điểm nhất định của phân tích. Mô đun thứ ba của hệ thống chịu trách nhiệm giảm thiểu các dị thường được phát hiện, có ý định giảm thiểu thiệt hại do kẻ tấn công gây ra. Những đóng góp chính của công việc này là:

* Ðặc điểm lưu lượng mạng sử dụng cơ chế Deep Learning LSTM;
* Phát hiện các cuộc tấn công DDoS và Portscan bằng cách sử dụng hệ thống suy luận mờ;
* Phân tích lưu lượng mạng được thực hiện trong thời gian gần thực;
* Thử nghiệm với hai bộ dữ liệu chứa nhiều loại tấn công DDoS;
* So sánh giữa hệ thống đã phát triển và các phương pháp khác có trong tài liệu.

Phần còn lại của công việc này được tổ chức như sau: Phần II trình bày các công việc liên quan; Phần III trình bày các nguyên tắc cơ bản được sử dụng trong sự phát triển của hệ thống; Phần IV chúng tôi thảo luận về kết quả hiệu suất của hệ thống. Cuối cùng, trong Phần V, các kết luận thu được từ sự phát triển của bài báo này được trình bày.

II. CÁC CÔNG TRÌNH LIÊN QUAN

Ngày nay, các mạng SDN được sử dụng rộng rãi, tuy nhiên chúng có nhiều vấn đề liên quan đến bảo mật [4], [6], [13], [30]. Do đó, bảo mật mạng SDN vẫn không xác định và các giải pháp liên quan đến phát hiện và giảm thiểu các cuộc tấn công đã được phát triển [14].

Theo AlEroud và Alsmadi [31], khi logic chuyển tiếp gói được tập trung và phân bổ trong bộ điều khiển, các tác nhân độc hại khám phá các lỗ hổng trên bộ điều khiển, trên các liên kết giao tiếp giữa bộ điều khiển và các thiết bị chuyển tiếp và trên bộ nhớ của công tắc. Một công tắc có bộ nhớ hạn chế, khi nó bị tấn công, số lượng luồng mà các thiết bị nhận được sẽ tăng lên đáng kể, chiếm tất cả dung lượng lưu trữ từ bảng chuyển tiếp. Nhiều nghiên cứu đã được phát triển để tạo ra các cơ chế phòng thủ để cung cấp những lỗ hổng này có trong kiến trúc SDN [7], [32]. Silva và cộng sự [33] đã giới thiệu một khuôn khổ được gọi là ATLANTIC (Anomaly deTection và máy LeArNing Traffic classifI- cation cho mạng được xác định bằng phần mềm) để phát hiện, phân loại và giảm thiểu các sự kiện bất thường trong mạng SDN. Garg và Garg [34] trình bày một cơ chế thích ứng để cập nhật các chính sách một cách linh hoạt để tổng hợp các đầu vào dòng chảy và phát hiện các bất thường, để có thể giảm quá tải giám sát và các dị thường có thể được phát hiện chính xác hơn. Mousavi và St-Hilaire [35] đã áp dụng một kỹ thuật để phát hiện DDoS bằng cách sử dụng entropy. Mục tiêu chính của các tác giả là phát hiện một cuộc tấn công ở giai đoạn đầu tiên, vì việc phát hiện được thực hiện khi bắt đầu cuộc tấn công cho phép áp dụng các chính sách giảm thiểu trước khi bộ điều khiển hoàn toàn tràn ngập các gói độc hại.

Carvalho et al. [36] trình bày một hệ sinh thái mới để phát hiện và giảm thiểu các cuộc tấn công DDoS trong môi trường SDN. Hệ thống do các tác giả đề xuất bao gồm bốn giai đoạn: giai đoạn đầu tiên liên quan đến việc thu thập và lưu trữ các bản ghi luồng IP; giai đoạn thứ hai là tạo hồ sơ mạng bình thường dựa trên dữ liệu được thu thập bằng phương pháp ACODS (Tối ưu hóa thuộc địa kiến cho chữ ký số); giai đoạn thứ ba tương ứng với việc phát hiện các dị thường so sánh hành vi mạng thực với hồ sơ được tạo bằng cách sử dụng hồi quy logistic đa thức (MLR) để phát hiện các sự kiện đáng ngờ khác với hành vi dự kiến; cuối cùng, trong giai đoạn thứ tư, các chính sách giảm thiểu được áp dụng. Việc phân tích hành vi giao thông để phát hiện dị thường được thực hiện sau mỗi 30 giây. Theo kết quả được trình bày bởi các tác giả, hệ thống chứng tỏ là có hiệu quả trong việc phát hiện và giảm thiểu các giai đoạn sự kiện bất thường.

Hamamoto và cộng sự [37] đã đề xuất một hệ thống phát hiện dị thường áp dụng cho các mạng quy mô lớn. Các tác giả đã sử dụng cách tiếp cận DSNSF (Chữ ký kỹ thuật số của phân đoạn mạng bằng cách sử dụng Phân tích luồng) để tạo ra các dấu hiệu hành vi của hành vi mạng thông thường, áp dụng GA (Genetic Algo- rithm). Hơn nữa, logic Fuzzy đã được sử dụng cùng với DSNSF được tạo ra cho các hành vi bất thường trong các mạng được phân tích đó. Nó đã được sử dụng dữ liệu thực được thu thập từ Ðại học Nhà nước của Londrina bằng cách sử dụng sFlow để xác thực hệ thống được đề xuất. Ba dị thường khác nhau đã được đưa vào dữ liệu thực của mạng, sử dụng các công cụ để mô phỏng các sự kiện bất thường: DoS, DDoS và Flash Crowd. Hệ thống được đề xuất cho thấy hiệu quả, với tỷ lệ dự đoán trên 96%. Các tác phẩm khác nhau cũng áp dụng cách tiếp cận DSNSF bằng cách sử dụng các kỹ thuật khác nhau. Tuy nhiên, các đặc tính lưu lượng truy cập trên các tác phẩm này đã sử dụng cách tiếp cận phân tích dữ liệu từ hai đến bốn tuần để nhận dạng các mẫu và tạo hồ sơ thông thường trong môi trường thông thường của mạng. Hơn nữa, một hạn chế được trình bày bởi các tác phẩm này là các cuộc tấn công đã được phát hiện trong khoảng thời gian từ 1 đến 5 phút. Không giống như các tác phẩm này, mô hình được đề xuất trong bài báo này thực hiện dự đoán về hành vi giao thông bình thường bằng cách áp dụng cửa sổ trượt và phát hiện các sự kiện bất thường mỗi giây.

Với sự gia tăng của các ứng dụng nhận dạng hình ảnh, xử lý ngôn ngữ tự nhiên, tin sinh học, các mô hình Học sâu có vai trò cơ bản trong việc giải quyết các loại vấn đề này. Do khả năng khổng lồ của nó để trích xuất kiến thức trên quy mô lớn từ dữ liệu phức tạp, có được lợi thế về kết quả của nó nếu chúng ta so sánh chúng với các kỹ thuật Học máy truyền thống [18], [21]. Trong An ninh mạng, các mô hình Học sâu đang được áp dụng trong nhiều lĩnh vực khác nhau, ví dụ như phát hiện xâm nhập [38], phát hiện phần mềm độc hại, phát hiện thư rác [39], phát hiện tấn công DDoS [40], v.v.

Li và cộng sự. [41] đã đề xuất một cơ chế Máy học có giám sát để bảo vệ và phát hiện các cuộc tấn công DDoS trong môi trường mạng SDN dựa trên học sâu. Mô hình được trình bày bởi các tác giả bao gồm các lớp sau: lớp đầu vào, lớp đệ quy chuyển tiếp, lớp đệ quy ngược, lớp ẩn được kết nối đầy đủ và lớp đầu ra. Khi xây dựng mô hình, nó đã được sử dụng Mạng thần kinh tái phát (RNN), Bộ nhớ ngắn hạn dài (LSTM) và Mạng thần kinh tích chập (CNN). Theo kết quả thu được từ mô hình này sau khi phát hiện, bộ điều khiển SDN tạo ra các chính sách loại bỏ và gửi chúng đến các công tắc. Ðối với việc dẫn dắt thử nghiệm, tập dữ liệu ISCX đã được sử dụng để đào tạo mô hình phát hiện và xác minh kiến trúc phòng thủ thông qua các cuộc tấn công DDoS trong thời gian thực. Theo kết quả được trình bày, phương pháp phòng thủ được trình bày đã thu được tỷ lệ chính xác là 98%. Tuy nhiên, việc học có giám sát để phát hiện các cuộc tấn công mạng là một nhược điểm, bởi vì cách những kẻ tấn công thực hiện các cuộc tấn công liên tục được cập nhật.

Tuan A Tang và cộng sự. [42] đã sử dụng Deep Learning để phát hiện các luồng bất thường trong mạng SDN. Các tác giả đã đề xuất một Mạng thần kinh sâu (DNN) cho một hệ thống phát hiện những kẻ xâm nhập và mô hình đã được đào tạo bằng cách sử dụng tập dữ liệu NSL-KDD. Tập dữ liệu được tạo thành từ 41 thuộc tính. Tuy nhiên, chỉ có một tập hợp con gồm 6 thuộc tính được sử dụng. Thông qua các thí nghiệm, mô hình được đề xuất chỉ thu được độ chính xác là 75,75%. Số lượng thuộc tính thấp ảnh hưởng đến độ chính xác thấp. Dey và Rahman [43] trình bày một phương pháp phát hiện dị thường dựa trên các luồng trên bộ điều khiển OpenFlow sử dụng DNN. Mô hình được đề xuất đã kết hợp hai cách tiếp cận Gated Recurrent Unit và Long Short Term Mem- ory (GRU-LSTM) để xây dựng hệ thống phát hiện xâm nhập. Hai phương pháp lựa chọn tính năng đã được sử dụng cho mỗi sự bất thường được phân tích để cải thiện hiệu suất của mô hình, NOVA F-Test và Recursive Feature Elimination. Ðối với quá trình thử nghiệm, tập dữ liệu NSL-KDD cũng đã được sử dụng. Các kết quả thử nghiệm cho thấy độ chính xác là 87%. Shone và cộng sự. [38] đã đề xuất một mô hình tập hợp DL mới cho NIDS, kết hợp học tập sâu và nông. Mô hình kết hợp Bộ mã hóa tự động sâu không đối xứng và Rừng ngẫu nhiên. Dữ liệu được sử dụng cho bài kiểm tra đến từ bộ dữ liệu KDD CUP 99 và NSL-KDD. Kết quả cho thấy độ chính xác 97,85%.

Mặc dù vậy, nhiều tác phẩm có sẵn trong tài liệu [17], [21], [25], [26], [28] để phát hiện các cuộc tấn công DDoS chỉ đánh giá một vài loại tấn công DDoS. Không giống như những công việc này, một trong những đóng góp chính được trình bày bởi hệ thống được đề xuất trong bài báo này là phát hiện 12 loại tấn công DDoS (ví dụ: NTP, DNS, LDAP, MSSQL, NetBIOS, SNMP, SSDP, UDP, UDP-Lag, WebD-DoS (ARME), SYN và TFTP). Ngoài ra, hệ thống được đề xuất có khả năng học hành vi bình thường của mạng, đây là một lợi thế để phát hiện các cuộc tấn công zero-day.

A diagram of a system

Description automatically generated

Hình 1: Kiến trúc hệ thống được đề xuất sử dụng LSTM và logic mờ để phát hiện và giảm thiểu bất thường.

III. HỆ THỐNG ÐƯỢC ÐỀ XUẤT

Hệ thống được đề xuất trong bài báo này có mục tiêu chính là đặc tính lưu lượng mạng, phát hiện và giảm thiểu các cuộc tấn công DDoS và Portscan trong môi trường mạng do Phần mềm xác định. Hệ thống được sử dụng làm nguyên tắc cho khái niệm Chữ ký số của các phân đoạn mạng (DSNS) do Proença giới thiệu [20]. Khái niệm này áp dụng một kỹ thuật hiệu quả để tạo ra một mô hình đặc trưng cho hồ sơ mạng bằng cách sử dụng dữ liệu lịch sử. Ðặc tính được đề xuất bởi Proença và cộng sự đã được lý tưởng hóa cho môi trường mạng truyền thống và sử dụng cơ sở lịch sử từ các tuần lưu lượng truy cập trước có chứa các đối tượng MIB (Cơ sở thông tin quản lý) từ giao thức quản lý SNMP (Simple Network Management Proto- col). Mặt khác, đặc tính được đề xuất trong bài báo này sử dụng các thuộc tính luồng IP được thu thập từ bộ điều khiển SDN và dự đoán về chữ ký mạng được thực hiện Bằng cách sử dụng một cửa sổ trượt của giao thông. Do đó, hệ thống được đề xuất loại bỏ việc sử dụng cơ sở dữ liệu để tạo ra chữ ký. Có thể nhận ra hành vi từ hồ sơ thông thường của mạng khác với dự kiến và giúp ích trong phương pháp phát hiện giai đoạn bất thường được trình bày trong công việc này.

Hệ thống phát hiện và giảm thiểu các dị thường được đề xuất trong công việc này được chia thành ba giai đoạn:

1. Dự đoán hành vi bình thường của lưu lượng truy cập mạng và định nghĩa các ngưỡng bình thường;
2. Ứng dụng của Fuzzylogic để xác định xem có bất thường hay không, sử dụng làm tham số lưu lượng dự đoán và các ngưỡng được xác định ở giai đoạn cuối cùng;
3. Áp dụng các chính sách giảm thiểu với ý định thực hiện các biện pháp đối phó với các cuộc tấn công được phát hiện, đảm bảo hoạt động của mạng.

Hình 1 minh họa sơ đồ sơ đồ cho hoạt động của hệ thống phát hiện và giảm thiểu sự bất thường được đề xuất trong bài báo này. Hệ thống được phát triển trên mặt phẳng ứng dụng. Giai đoạn đầu tiên là đặc tính lưu lượng, trong đó các thuộc tính

A diagram of a diagram

Description automatically generated

Hình 2: Cấu trúc tế bào LSTM.

luồng được xử lý trước để dự đoán lưu lượng mạng và các dấu hiệu hành vi bình thường cùng với các ngưỡng tiêu chuẩn. Giai đoạn tiếp theo là mô-đun phát hiện bất thường, trong đó hệ thống suy luận mờ quyết định động để xác định sự xuất hiện của các sự kiện bất thường. Khi có sự bất thường, các IP và cổng nằm trong khoảng phân tích được coi là đáng ngờ. Giai đoạn thứ ba chịu trách nhiệm áp dụng các chính sách giảm thiểu và nhận các luồng đáng ngờ đầu vào được xác định ở giai đoạn cuối. Trong tập hợp các luồng này, mô-đun giảm thiểu áp dụng biện pháp đối phó thích hợp nhất để giảm thiểu tác động của một cuộc tấn công.

A. BỘ NHỚ NGẮN HẠN DÀI ÐỂ DỰ BÁO LƯU LƯỢNG MẠNG

1) BỘ NHỚ NGẮN HẠN DÀI

Trong phần phụ này, một số khái niệm về LSTM sẽ được giới thiệu ngắn gọn để hỗ trợ sự hiểu biết về mô-đun đặc trưng được đề xuất trong công việc này. Ðược giới thiệu bởi Hochre- iter và Schmidhuber [44], LSTM một kiến trúc đặc biệt của các mạng lưới thần kinh nhân tạo tái phát, với khả năng học các phụ thuộc lâu dài. Cấu trúc của một tế bào LSTM được minh họa trong Hình. 2. Như đã quan sát, tại mỗi thời điểm, ô được điều khiển bởi các cổng khác nhau có thể duy trì hoặc đặt lại giá trị theo trạng thái của cổng. Ba cổng được áp dụng trên ô, cổng quên (ft), cổng đầu vào (nó) và cổng đầu ra (ot). Hơn nữa, có một cổng điều chế lối vào được gọi là giá trị ứng cử viên. Các cổng có thể được mô tả như sau:

it = σ(Wx,ixt + Wii,hht−1 + bi) (1)

ft = σ(Wf,ixt +Wf,h ht−1 +bf) (2)

ot = σ(Wo,i xt + Wo,h ht−1 + bo) (3)

c′t = tanh(Wc’,i xt + Wc’,h ht−1 + bc’ ) (4)

Trong đó W có nghĩa là ma trận có trọng lượng synap, b có nghĩa là vectơ thiên vị, xt là đầu vào thực tế, c′t là một vectơ có mới Các ứng cử viên được thêm vào trạng thái thực tế của tế bào, ht−1 là đầu ra trước đó của LSTM trong thời gian tức thời t −1, σ (·) và tanh(·) là các hàm kích hoạt tương ứng, Sigmoid và Tangent Hyperbolic. Bước đầu tiên trên LSTM là quyết định bao nhiêu giá trị bộ nhớ trước đó sẽ bị xóa khỏi trạng thái của ô. Quyết định này được đưa ra bởi cổng quên. Giai đoạn tiếp theo là xác định bao nhiêu thông tin mới sẽ được lưu trữ, được tạo ra bởi cổng đầu vào. Tiếp theo, trạng thái của ô được sử dụng và xác định với biểu thức sau:

ct = ft ⊙ ct−1 + it ⊙ c′t (5)

trong đó ⊙ biểu thị tích nguyên tố. Ðầu ra LSTM Ht được định nghĩa bởi:

ht = ot ⊙ tanh(ct) (6)

2) GIAI ÐOẠN DỰ BÁO LƯU LƯỢNG MẠNG

Dự đoán lưu lượng truy cập nhằm mục đích tạo ra dấu hiệu hành vi bình thường của mạng, điều này rất cần thiết cho việc quản lý và bảo mật mạng. Ðặc điểm mạng làm cho quyết định quản lý liên quan đến các vấn đề có thể xảy ra đáng tin cậy và an toàn hơn. Ðể có được dự đoán gần với hành vi thực là một bước quan trọng hướng tới việc phát hiện lưu lượng truy cập bất thường, vì chữ ký được tạo ra phân định giới hạn bình thường của mẫu lưu lượng truy cập tại một thời điểm nhất định trên phân đoạn mạng được quan sát.

Các đặc tính của chữ ký được tạo ra từ dữ liệu IP Flow được thu thập từ các công tắc làm việc mạng SDN bởi bộ điều khiển sử dụng một nguyên mẫu OpenFlow. Trong số các thuộc tính được thu thập bởi bộ điều khiển, các thuộc tính sau đã được chọn: bit/s, gói/s, địa chỉ IP nguồn, địa chỉ IP đích, cổng nguồn và đích. Các thuộc tính luồng này đã được phân tích và sử dụng cho các tác phẩm trước đây trong đặc tính lưu lượng mạng của tốc độ cao và trình bày kết quả tốt để mô tả và hiểu rõ hơn hành vi mạng [45], [46]. Kích thước byte và gói là các thuộc tính định lượng, có nghĩa là các thuộc tính khối lượng có khả năng cung cấp thông tin liên quan đến lượng thông tin được vận chuyển trên mạng. Những thứ khác là các thuộc tính danh nghĩa và cung cấp thông tin định tính có nghĩa là các thuộc tính này cho phép hiểu thiết bị nào đang giao tiếp với nhau và dịch vụ nào đang được chúng truy cập. Việc sử dụng các thuộc tính này là cơ bản để xác định các cuộc tấn công có thể xảy ra và không thể sử dụng mô-đun giảm thiểu để giảm thiểu thiệt hại do một cuộc tấn công gây ra.

Các thuộc tính IP và cổng là dữ liệu danh nghĩa và để thực hiện phân tích định lượng, cần phải chuyển đổi các thuộc tính này thông qua phép tính entropy. Vì vậy, Entropy Shannon (3) đã được sử dụng trong công việc này [47], nó cho phép trích xuất thông tin từ nồng độ và dự đoán các thuộc tính dòng chảy này. Cuối cùng, với tập thuộc tính luồngx= {x1, x2, . . . ,xN} Ở đâuxTôiđại diện cho sự xuất hiện của mẫuTôi vào khoảng thời gian. Entropy H đến X được định nghĩa trong phương trình (7)

H(x) =− , (7)

S = ∑i=1N là tổng của tất cả các lần xuất hiện trong biểu đồ. Có thể xác định các cuộc tấn công bằng cách sử dụng entropy để mô tả lưu lượng truy cập. Ví dụ: trong khi xảy ra cuộc tấn công DDoS, địa chỉ IP của nạn nhân và entropy cổng đích sẽ tập trung; sự phân tán entropy của cổng nguồn do nhiều kẻ tấn công sử dụng các cổng nguồn ngẫu nhiên.

Sau khi đảm bảo rằng tất cả các thuộc tính luồng được thu thập đều được trình bày theo cách định lượng, quá trình tạo chữ ký lưu lượng sẽ bắt đầu. Vấn đề dự đoán lưu lượng mạng bằng LSTM có thể được định nghĩa theo mô hình sau. Hãy xem xét vào thời điểm hiện tạit, tập dữ liệu X= (x1, x2, . . . ,xd), trong đó mỗix Tôilà một vectơ thuộc tính luồng được định nghĩa là:

* x1: bit/s
* x2: bit/giây
* x3: entropy IP nguồn
* x4: entropy IP đích
* x5: entropy cổng nguồn
* x6: Entropy cổng đích

Mạng nơ-ron trí nhớ ngắn hạn dài được thiết kế để xử lý theo trình tự nhờ khả năng duy trì trí nhớ dài hạn. Trong những năm gần đây, LSTM được sử dụng rộng rãi trong dự đoán chuỗi thời gian và đã được chứng minh là vượt trội so với các thuật toán toán học truyền thống [48]–[50]. Ngoài ra, LSTM là một kỹ thuật mạnh mẽ có thể thể hiện mối quan hệ giữa các sự kiện hiện tại và trước đó, đồng thời nâng cao khả năng dự báo lưu lượng mạng.

Trong cách tiếp cận công việc này, LSTM đã được áp dụng để giải quyết vấn đề dự đoán chuỗi thời gian một biến. Bằng cách này, LSTM dự đoán dấu hiệu của hành vi mạng bình thường. LSTM được áp dụng cho từng thuộc tính luồng được xác định trước đó, có nghĩa là mỗi LSTM sẽ chịu trách nhiệm dự đoán dấu hiệu hành vi bình thường cho từng thuộc tínhx Tôi. Mô hình LSTM sẽ học một hàm ánh xạ một chuỗi cácN quan sát đầu vào trước đó thành quan sát đầu ra [51]. Ví dụ, tạitngay lập tức, với một chuỗi đầu vào củaNcác quan sát trong quá khứ bao gồm các vectơ bitx1= {xt-n …, xt-3xt-2, xt-1}, tạo ra kết quả y1= {yt} đại diện cho dự đoán hành vi đối với thuộc tính bit luồng. Quả sung.3minh họa mô hình LSTM cho chữ ký số (LSTM-DS) được đề xuất trong bài báo này.

A diagram of a server

Description automatically generated

Hình 3: Mô hình đề xuất dự báo lưu lượng sử dụng 6 LSTM.

Mặc dù sử dụng 6 mạng LSTM, mỗi mạng cho mỗi thuộc tính luồng, quá trình huấn luyện mạng là một tác vụ ngoại tuyến. Chi phí tính toán cho việc đào tạo cao. Tuy nhiên, nó không quan trọng đối với ứng dụng của nó [52]. Vì vậy, trong giai đoạn vận hành với mạng LSTM đã được huấn luyện, quá trình dự đoán lưu lượng được thực hiện ngay lập tức. Thuật toán1minh họa quá trình hoạt động của mô-đun LSTM-DS.

Lưu lượng truy cập dự đoán sẽ không giống với lưu lượng truy cập thực tế. Tuy nhiên, cần phải xác định

Yêu cầu: X= (x1,x2, . . . ,xd)

Đảm bảo: y= (y1,y2, . . . ,yd)

1:y1= LSTM-bit(x1)

2:y2= Gói LSTM(x2)

3:y3= LSTM SrcIPEntropy(x3)

4:y4= LSTM DstIPEntropy(x4)

5:y5= LSTM SrcPortEntropy(x5)

6:y6= LSTM DstPortEntropy(x6)

7:y7= (y1,y2,y3,y4,y5,y6)

8: trả lại y =0

ngưỡng giữa lưu lượng dự đoán và lưu lượng thực. Bất đẳng thức Bienaymé-Chebyshev được sử dụng để xác định ngưỡng này giữa giá trị dự đoán và giá trị thực. Bất đẳng thức Bienaymé Chebyshev xác định giới hạn phần trăm dữ liệu nằm ở số k của khoảng độ lệch chuẩn xung quanh giá trị trung bình. Bất đẳng thức có thể được áp dụng để phát hiện các giá trị ngoại lệ [53] khi chưa biết phân bố dữ liệu. Phương trình cho bất đẳng thức Bienaymé-Chebyshev được biểu diễn trong phương trình (số 8):

P( | X − µ | ≥ k σ ) ≤ , (8)

Ở đâu X là một biến ngẫu nhiên, µlà ý nghĩa, k >0 là tham số độ lệch vàσlà độ lệch chuẩn. Xác định tham sốk=4.47 trong phương trình (số 8), xác suất thu được sẽ bằng 0,05, đây là điểm giới hạn thông thường có ý nghĩa thống kê để xác minh sự khác biệt của một giả thuyết liên quan đến dữ liệu được quan sát [54].

B. FUZZY LOGIC ĐỂ PHÁT HIỆN SỰ BẤT THƯỜNG

1) LÝ THUYẾT FUZZY LOGIC

Trong logic cổ điển, một mệnh đề chỉ có thể lấy giá trị là đúng hoặc sai. Mặt khác, lý thuyết tập mờ đã đưa ra một khái niệm mới, nghĩa là các giới từ có thể nhận các giá trị từ 0 đến 1. Khái niệm này được gọi là mức độ thành viên. Được giới thiệu bởi Zadeh vào năm 1965 [55], lý thuyết tập mờ cung cấp một công cụ toán học có khả năng hỗ trợ việc đưa ra quyết định một môi trường với các biến số không chính xác, sự không chắc chắn và thông tin không đầy đủ.

Một tập Fuzzy có thể được định nghĩa là (S,f) nơi mà S tập hợp bất kỳ và f đại diện cho chức năng thành viên. Mọi phần tử x thuộc về đến S, các f(x) giá trị xác định mức độ thành viên của x trong bộ (S,f). Các x phần tử được coi là không bao gồm uf(x) = 0, bao gồm toàn bộ uf(x) = 0 và thành viên mờ uf(x) = 1.Một ví dụ về chức năng thành viên là Gaussiana, được định nghĩa là:

f(x) = (9)

trong đó m là trung bình và σ là độ lệch chuẩn của tập S.

Theo Wu và Banzhaf [56], logic Fuzzy được sử dụng để phát hiện sự bất thường trong các mạng vì hai lý do chính. Thứ nhất, các vấn đề phát hiện bất thường liên quan đến vô số thuộc tính số được thu thập và dẫn xuất thống kê, có thể gây ra lỗi phát hiện. Thứ hai, các mô hình tạo ra một hồ sơ bình thường của hành vi mạng cần phải xác định ngưỡng giữa các hành vi bình thường và bất thường. Tuy nhiên, khoảng thời gian này không được xác định rõ và những thay đổi nhỏ về hành vi giao thông có thể gây ra báo động sai. Xem xét những yếu tố này, logic Fuzzy đã được sử dụng trong công việc này để giúp với việc ra quyết định để phát hiện sự bất thường.

2) GIAI ĐOẠN PHÁT HIỆN BẤT THƯỜNG

Mô hình được đề xuất để phát hiện sự bất thường trong tác phẩm này sử dụng giao thông quá khứ, mô hình được dự đoán bởi LSTM và logic Fuzzy. Bước đầu tiên là "fuzzification" các nguồn cho từng thuộc tính dòng chảy đang được phân tích, áp dụng chức năng thành viên. Chức năng thành viên được áp dụng trong tác phẩm này là một sự sửa đổi của chức năng Gaussian thành viên, được định nghĩa là:

f(yt)j = (10)

trong đó xt là lưu lượng thực tế, yt là dự đoán lưu lượng của LSTM và σ ̈t là ngưỡng tạo ra bởi sự bất bình đẳng của Bienaymé- Chebyshev từ thuộc tính lưu lượng j.   
Eq. 10 xác định mức độ thành viên của bộ giao thông tiêu chuẩn. Do đó, để phát hiện một sự bất thường chúng ta sẽ áp dụng bổ sung của nó, được định nghĩa là:

fj = 1 - fi

Kết quả fi’ đại diện cho điểm bất thường của thuộc tính dòng chảy j. Điểm bất thường được sử dụng để phân loại hành vi giao thông cho một phân tích dữ liệu tức thời. Quá trình "defuzzification" quyết định giao thông là "normal", "Portscan" hoặc "DDoS", được mô tả trong các quy tắc sau đây:

Các giá trị cho điểm γ và ζ được xác định là 1.2362 và 3.3821, tương ứng. Những giá trị này được đánh giá theo độ chính xác và được nêu chi tiết ở phần IV-C. Hình 4 minh họa điểm số bất thường của tất cả các thuộc tính dòng chảy trong một ngày phân tích lưu lượng mạng, trong đó chứa một khoảng thời gian tấn công DDoS và Portscan được mô tả trong các qui tắc sau:

Rule 1: IF THEN “normal” (12)

Rule 2: IF AND

THEN “Portscan” (13)

Rule 3: IF THEN “DDoS” (14)

Các giá trị cho γ và ζ điểm số được xác định lần lượt là 1,2362 và 3,3821. Các giá trị này được đánh giá theo độ chính xác và được trình bày chi tiết ở Phần IV-C . Hình 4 minh họa điểm bất thường của tất cả các thuộc tính luồng trong một ngày phân tích lưu lượng mạng, trong đó có giai đoạn tấn công DDoS và Portscan. Mặt khác, hình 5 minh họa tổng số điểm bất thường của tất cả sáu thuộc tính dòng chảy. Với điểm số bất thường được tính toán, hệ thống có thể phát hiện một cuộc tấn công dựa trên các quy tắc được xác định trong (12), (13), và (14).

C. GIAI ĐOẠN GIẢM THIỂU

Việc phát hiện và xác định sự bất thường là những giai đoạn thiết yếu đảm bảo hoạt động và các dịch vụ có sẵn trong các hệ thống mạng. Sau khi phát hiện một sự kiện bất thường, một cơ chế phải được sử dụng để giảm thiểu tác động gây ra bởi sự kiện đó. Quá trình thông thường để xác định tác động của các cuộc tấn công là bằng cách giảm thiểu, áp dụng các chính sách tự động mà không cần sự can thiệp của con người, và nhằm đảm bảo khả năng phục hồi và hoạt động của mạng lưới. Do đó, hệ thống được đề xuất bao gồm một mô-đun chịu trách nhiệm xác định dòng chảy bất thường và các chính sách giảm thiểu được thực hiện.

Chính sách giảm thiểu được cấu trúc bằng cách sử dụng mô hình Sự kiện - Điều kiện - Hành động (ECA), được coi là phù hợp cho việc quản lý năng động các chính sách. Trong mô hình này, Sự kiện đề cập đến một sự bất thường cụ thể và được liên kết với một tập hợp các quy tắc. Các quy tắc này được mô tả là một tập hợp các điều kiện tương ứng với bối cảnh trong đó sự bất thường xảy ra. Cuối cùng, Hành động này là một biện pháp đối phó được thực hiện liên quan đến các dòng chảy được xác định là độc hại [57].

Phương pháp chính được sử dụng trong các ứng dụng giảm thiểu tấn công trên môi trường SDN là để sửa đổi đầu vào bảng dòng chảy của bộ chuyển đổi hoặc để thêm một đầu vào dòng chảy mới. Sau khi phát hiện một cuộc tấn công, một số đặc điểm phải được xác định, ví dụ như IP nguồn, IP đích, số cổng nguồn, số cảng đích, và loại giao thức. Những đặc điểm này giúp xác định kẻ tấn công và là cơ bản để thực hiện các biện pháp đối phó để giảm thiểu thiệt hại mà một cuộc tấn công gây ra. Một mục mới trên bảng dòng chảy có thể được cài đặt dựa trên một hoặc nhiều đặc điểm này, báo hiệu rằng các gói thuộc về dòng chảy là từ kẻ tấn công. Ngoài ra, các hành động được thực hiện có thể là loại bỏ các gói này, tắc nghẽn giao thông bất thường và/hoặc chuyển hướng bánh mì [58].

Dựa trên các khái niệm đã trình bày, mô-đun giảm nhẹ của hệ thống được thực hiện bằng hai chính sách nhằm giảm thiểu các bất thường được phát hiện. Sau khi cảnh báo của mô-đun phát hiện tắt, mô-đun giảm thiểu sẽ hành động. Bước đầu tiên là xác định các luồng nghi ngờ trong khoảng thời gian phân tích. Việc xác định các tảng băng bị nghi ngờ được thực hiện dựa trên phân tích địa chỉ IP và các cổng tạo ra khoảng thời gian bất thường. Những địa chỉ di chuyển tới địa chỉ IP nhận được nhiều luồng nhất được coi là nghi phạm.

A group of blue and white graphs

Description automatically generated

Hình 4: Điểm bất thường trên mỗi thuộc tính luồng.

A graph with green lines

Description automatically generated

Hình 5: Tổng điểm bất thường theo sáu thuộc tính luồng.

Bằng cách xác định các luồng đáng ngờ, trong trường hợp Sự kiện do mô-đun phát hiện khởi chạy là một cuộc tấn công DDoS, việc loại bỏ các luồng sẽ được thực hiện dựa trên các địa chỉ IP nguồn xuất hiện thường xuyên hơn trên các luồng bị nghi ngờ và đồng thời có cùng một địa chỉ IP. cảng đích. Khi Sự kiện được khởi chạy là một cuộc tấn công Portscan, quá trình xác định cuộc tấn công được thực hiện bằng địa chỉ IP gốc có nhiều cổng đích nhất. IP này được coi là IP tấn công và tất cả các luồng của nó sẽ bị loại bỏ.

**Quá trình giảm thiểu được thể hiện trong Thuật toán 2 .**

**Thuật toán 2** Quy trình giảm thiểu tấn công

**Yêu cầu:** Luồng nghi ngờ

**Đảm bảo:** Loại bỏ các gói bất thường

1: **If** DDoS tấn công **then**

2: Xác định địa chỉ IP đích nhận được nhiều luồng nhất

3: Xác định trong các luồng đó địa chỉ IP của kẻ tấn công có cùng cổng đích

4: **If** IPs và cổng nằm trong *Danh sách an toàn* **then**

5: Chuyển tiếp gói tin

6: **Else**

7: Thả gói tin

8: **If** Portscan tấn công **then**

9: Xác định địa chỉ IP đã nhận được nhiều luồng nhất

10: Xác định trong các luồng đó IP gốc nào có nhiều cổng đích nhất

11: **If** cổng điện tử IP nằm trong *Danh sách an toàn* **then**

12: Chuyển tiếp gói tin

13: **Else**

14: Thả gói tin

Có những điểm bất thường không phải do phần mềm độc hại gây ra, nhưng có biểu hiện tương tự như một cuộc tấn công. Ví dụ: hiện tượng bùng nổ truy cập bất thường có cùng đặc điểm với một cuộc tấn công DDoS, tuy nhiên, chúng là các yêu cầu hợp pháp từ người dùng thực. Trong các nghiên cứu của Giotis et al. [58] và Assis et al. [46] , các tác giả đề xuất triển khai một cơ chế duy trì danh sách các thuộc tính luồng IP của người dùng hợp pháp trong một thời gian xác định là 5 phút. Theo cách tương tự, chúng tôi cũng triển khai một cơ chế gọi là Danh sách An toàn (Safe List) lưu giữ danh sách các địa chỉ IP và cổng. Do đó, danh sách này được xác minh trước khi bắt đầu quá trình giảm thiểu tấn công.

## IV. KẾT QUẢ VÀ THẢO LUẬN

Hệ thống được triển khai bằng ngôn ngữ Python và các thư viện phát triển ứng dụng Deep Learning Keras và TensorFlow. Các thử nghiệm được thực hiện trong môi trường với cấu hình: Intel Core i5 2.21 GHz, RAM 8 GB và hệ điều hành Windows 10. Sử dụng các thông số mặc định, bao gồm: dropout = 0.2, hàm mất là MSE (Mean-Square Error), tỷ lệ học (learning rate) = 0.001, và bộ tối ưu hóa (optimizer) được đặt thành Adam theo đề xuất trong tài liệu [59], là một thuật toán tối ưu hóa tỷ lệ học thích ứng để huấn luyện mạng nơ-ron sâu.

Để chứng minh hiệu quả và tính năng của hệ thống đề xuất, chúng tôi đã áp dụng các thử nghiệm từ các kịch bản khác nhau. Môi trường thử nghiệm được sử dụng trong kịch bản 1 là một cấu trúc mạng với 120 máy chủ và các cuộc tấn công được thực hiện vào các khoảng thời gian trong ngày. Trong kịch bản 2, chúng tôi sử dụng các luồng IP được mô phỏng từ một tập dữ liệu công khai có tên CICDDoS 2019 [60] từ Viện An ninh mạng Canada. Cơ sở dữ liệu này chứa các loại tấn công DDoS khác nhau và hồ sơ lưu lượng thực tế.

**A. Kịch bản**

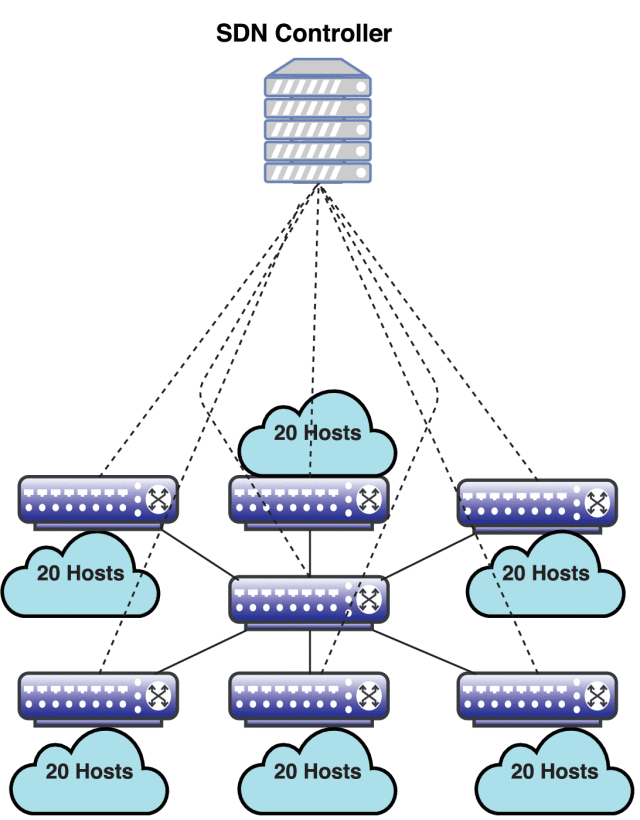
Hệ thống phân tích hành vi lưu lượng mỗi giây. Do đó, các luồng mạng phải được thu thập trong khoảng thời gian này. Để thực hiện phân tích này, trong kịch bản 1, việc mô phỏng hành vi mạng bằng trình mô phỏng mạng SDN Mininet [61] là cần thiết. Công cụ này cho phép tạo các mạng ảo thực tế bao gồm bộ điều khiển, máy chủ, liên kết và switch trên một máy ảo duy nhất. Mininet sử dụng ảo hóa nhẹ để tạo các cấu trúc mã nguồn mở tùy chỉnh và được ứng dụng rộng rãi trong lĩnh vực này để thực hiện nghiên cứu và phát triển các giải pháp cho môi trường SDN. Các thí nghiệm sử dụng một công cụ tên là Scapy [62] để đưa lưu lượng vào mạng được mô phỏng nhằm đảm bảo kịch bản mô phỏng gần nhất với môi trường SDN thực tế, với lưu lượng dữ liệu cao chạy qua mạng.

Hơn nữa, để triển khai cơ chế phát hiện và giảm thiểu bất thường, chúng tôi đã sử dụng bộ điều khiển SDN Floodlight. Đây là một bộ điều khiển dựa trên Java được phát triển bởi BigSwich, hỗ trợ đa dạng các switch OpenFlow, ảo hoặc vật lý, và có thể xử lý các mạng hỗn hợp, OpenFlow và không OpenFlow. Các thuộc tính luồng được sử dụng bao gồm: bit/giây, gói/giây, entropy IP nguồn, entropy IP đích, entropy cổng nguồn và entropy cổng đích.

Hình 6 minh họa cấu trúc được mô phỏng trong kịch bản 1. Kịch bản đầu tiên được hình thành bởi một cấu trúc trong đó các thành phần của nó được phân bố theo dạng hình sao. Cấu trúc này được tạo thành từ các switch trung tâm, trong đó có sáu switch được kết nối. Mỗi mạng con chứa 20 máy chủ, tổng cộng 120 máy chủ. Hai ngày 24 giờ đã được mô phỏng, mỗi ngày chứa 86.400 mẫu. Ngày mô phỏng đầu tiên chỉ chứa các mẫu hành vi bình thường của mạng. Ngày này được sử dụng trong giai đoạn huấn luyện LSTM, vì một phương pháp huấn luyện bán giám sát đã được sử dụng trong quá trình huấn luyện của nó. Ngày mô phỏng thứ hai được sử dụng để đánh giá hiệu suất hoạt động của hệ thống trong việc phát hiện và giảm thiểu tấn công. Cùng với việc mô phỏng, hai cuộc tấn công đã được thực hiện với cường độ và thời gian khác nhau. Đó là một cuộc tấn công DDoS và một cuộc tấn công quét cổng (Portscan). Thông tin liên quan đến các thông số được sử dụng trong các cuộc tấn công được hiển thị chi tiết trong BẢNG 1. Bộ dữ liệu này có sẵn trực tuyến.

Bảng 1: Thông tin về các tham số của các cuộc tấn công trong Kịch bản 1

|  |  |
| --- | --- |
| Loại tấn công | Tham số tấn công |
| DDoS | Attackers:16  Attacking Ips: 10.0.0.80 – 10.0.0.85  Victim IP address: 10.0.0.50 |
| Portscan | Attacking Ips: 10.0.0.10  Victim IP address: 10.0.0.24  Ports: 1 – 20000  Thời gian chờ giữa các gói: 0.15 |



Hình 6: Cấu trúc liên kết mạng 1 được mô phỏng trên Mininet.

Trong kịch bản 2, chúng tôi sử dụng bộ dữ liệu công khai CICDDoS 2019 [60]. Bộ dữ liệu này được chia thành hai ngày, một ngày để huấn luyện và một ngày để thử nghiệm. Bộ dữ liệu huấn luyện bao gồm 12 loại tấn công DDoS khác nhau, bao gồm NTP, DNS, LDAP, MSSQL, NetBIOS, SNMP, SSDP, UDP, UDP-Lag, WebDDoS (ARME), SYN và TFTP. Ngày thứ hai, ngày thử nghiệm, chứa 6 loại tấn công DDoS, bao gồm NetBios, LDAP, MSSQL, UDP, UDP-Lag và SYN. Các thuộc tính của luồng được sử dụng giống như trong kịch bản 1.

**B. Số liệu và Kiểm tra**

Các thử nghiệm được áp dụng nhằm mục đích xác minh tính hiệu quả của hệ thống đề xuất, liên quan đến các mô-đun tạo ra nó, phát hiện và giảm thiểu. Hiệu suất của mô-đun đề xuất được phân tích bằng các số liệu thống kê sau [63]: độ chính xác (precision), độ thu hồi (recall), tỷ lệ dương giả (false-positive rate).

1. Độ chính xác: Cho biết tỷ lệ phần trăm các khoảng thời gian được phân loại là bất thường, thực sự là bất thường.
2. Độ thu hồi: Đo lường mức độ hiệu quả của mô hình trong việc xác định các khoảng thời gian bất thường so với tất cả các khoảng thời gian.
3. Tỷ lệ dương giả (false-positive rate): Thể hiện lỗi phân loại, lưu lượng được xác định là bất thường, nhưng thực tế lưu lượng đó là bình thường.

Các số liệu này có thể được tính toán dễ dàng bằng các phương trình sau:

Độ chính xác = (15)

Độ thu hồi = (16)

FPR = (17)

Trong đó, TP, TN, FP, FN lần lượt là dương thật, âm thật, dương giả và âm giả. Độ chính xác là một số liệu được áp dụng rộng rãi trong các công trình phát hiện bất thường. Tuy nhiên, nó có thể dẫn đến kết quả thiên lệch khi bộ dữ liệu không cân bằng, giống như trường hợp của dữ liệu được áp dụng trong công trình này. Bộ dữ liệu chứa nhiều mẫu bình thường hơn mẫu bất thường, và hệ thống có thể phân loại tất cả các mẫu chính xác là bình thường và phân loại sai các mẫu bất thường, dẫn đến kết quả thiên lệch. Số liệu Độ chính xác có thể được sử dụng để giải quyết kết quả thiên lệch này và nhấn mạnh việc phân loại chính xác các mẫu bất thường.

Đặc tính Hoạt động của Người nhận (ROC) [63] có thể là sự kết hợp của tỷ lệ TP và FP, cung cấp phân tích trực quan về khả năng phát hiện hành vi bất thường của hệ thống. Tuy nhiên, để lượng hóa hiệu quả tốt hơn giữa nhiều bộ phân loại, chúng tôi phân tích diện tích dưới đường cong (AUC) của đường cong ROC. Bộ phân loại có giá trị AUC cao nhất có khả năng phân loại mẫu tốt nhất. Do đó, AUC được áp dụng để đánh giá phương pháp đề xuất với các mô hình khác có sẵn trong tài liệu.

Hiệu quả của mô-đun giảm thiểu được đánh giá thông qua việc áp dụng một bài kiểm tra thống kê gọi là Bài kiểm định McNemar, cũng thông qua tỷ lệ gói bị mất. Bài kiểm định McNemar là một bài kiểm tra không tham số và được thực hiện trên các mẫu ghép đôi và dữ liệu danh nghĩa. Nó được áp dụng cho bảng tần số 2 × 2 với dấu vết nhị phân, nghĩa là hai hành vi (ví dụ: bất thường và bình thường) với mục đích xác minh xem tần số cận có bằng nhau hay không [64]. Bảng 2 minh họa một ví dụ chung về bảng tần số 2 × 2 thể hiện kết quả của hai bài kiểm tra trên một mẫu *n* cá nhân.

Bảng 2: Bảng dự phòng (2 x 2)

|  |  |  |  |
| --- | --- | --- | --- |
|  | Positive test 2 | Negative test 2 | Sum row |
| Positive test | a | b | a+b |
| Negative test | c | d | c+d |
| Sum column | a+c | b+d | n |

Giả thuyết Null cho rằng xác suất của mỗi kết quả là bằng nhau, có nghĩa là không có sự thay đổi trong các tần số cận và pa + pb = pa + pc e pc + pd = pb + pd , trong đó pa, pb, pc, pd biểu thị xác suất lý thuyết của các lần xuất hiện trên các ô có nhãn tương ứng. Giả thuyết Null và giả thuyết đối lập lần lượt được trình bày như sau:

H0 : pb = pc

H1 : pb ≠ pc

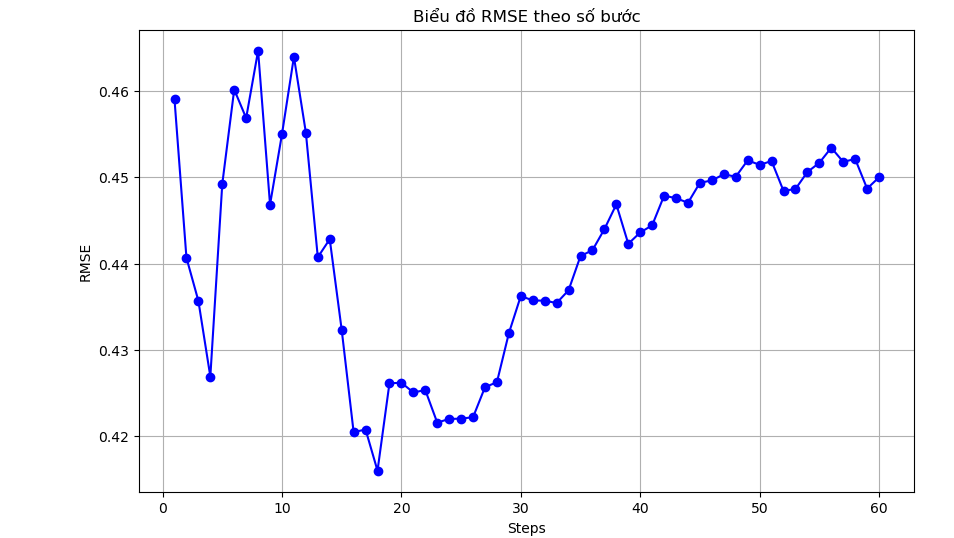
Công thức kiểm tra MacNemar bắt nguồn từ phương trình chi bình phương:

X2 = (18)

có phân phối chi bình phương với bậc tự do [số mức tự do của bảng tần số - 1]. Nếu kết quả đáng kể, điều đó có nghĩa là Pb ≠ Pc cho thấy các tần số cận khác biệt đáng kể với nhau, thì giả thuyết null bị bác bỏ.

**C. Đánh giá các thông số**

Mục này đánh giá kết quả của các thông số được sử dụng trong quá trình phát triển hệ thống đề xuất. Thông số đầu tiên được phân tích là kích thước bước thời gian được mạng LSTM sử dụng trong giai đoạn dự đoán lưu lượng. Các giá trị được sử dụng để kiểm tra bao gồm từ 2 đến 30 mẫu lưu lượng thu thập trước đó. Chỉ số RMSE được sử dụng để xác định kích thước bước thời gian tốt nhất. Biểu đồ trong Hình 7 minh họa các giá trị RMSE thu được cho mỗi giá trị được đánh giá. Kích thước bước thời gian cho kết quả tốt nhất là 5, với giá trị RMSE là 0,0445.



Hình 7: Kích thước bước thời gian được sử dụng để dự báo lưu lượng LSTM.

Bước tiếp theo là xác định số lượng đơn vị ẩn. Quá trình đánh giá thông số này sử dụng các giá trị từ 5 đến 100 đơn vị, và RMSE được tính toán cho mỗi giá trị. Số lượng đơn vị cho kết quả tốt nhất là 50, sau đó không có cải thiện đáng kể nào. Hình 8 minh họa đồ thị với kết quả đạt được cho mỗi giá trị đơn vị và giá trị RMSE tương ứng.

A graph with orange dots

Description automatically generated

Hình 8: Số lượng đơn vị được sử dụng để dự báo lưu lượng LSTM.

Đồ họa trong Hình 9 và Hình 10 minh họa quá trình đánh giá γ và ζ nhằm tìm ra tổng điểm bất thường phù hợp nhất. Các giá trị này được xác định bằng cách thay đổi γ và ζ tính toán độ chính xác tương ứng của chúng. Giá trị γ cuối cùng được xác định bằng công thức argmax( accuracyγ) và giá trị ζ được xác định bằng công thức argmax(accuracyζ) . Điểm số cho γ và ζ được xác định lần lượt là 1,2362 và 3,3821.

A graph with a line

Description automatically generated

Hình 9: Đánh giá độ chính xác của Gamma

A graph with a line and points

Description automatically generated

Hình 10: Đánh giá độ chính xác cho Zeta

**D. Kịch bản đánh giá 1**

Để xác thực thêm hiệu quả của hệ thống, chúng tôi đã so sánh hệ thống của mình với bốn phương pháp phát hiện bất thường khác, được áp dụng để phát hiện điểm bất thường trong mạng SDN. Phương pháp đầu tiên là k-Nearest Neighbor (kNN) [65] , một bộ phân loại có giám sát với chi phí tính toán thấp, được sử dụng để phát hiện các phần mềm độc hại trong trung tâm dữ liệu. Phương pháp thứ hai là Multi-layer Perceptron (MLP) [66] , một mạng nơ-ron nhân tạo được áp dụng trong việc phát hiện các cuộc tấn công DDoS. Một phương pháp khác dựa trên Support Vector Machine (SVM) [67] để phát hiện các cuộc tấn công ngập lụt (flooding attack). Chúng tôi cũng so sánh nó với LSTM-2 [68], sử dụng Học sâu (DL) để phát hiện các cuộc tấn công DDoS trong môi trường SDN. Cuối cùng, phương pháp gần đây xuất hiện trong tài liệu có tên Particle Swarm Optimization Digital Signature (PSO-DS) [46]. Phương pháp heuristic sử dụng kỹ thuật học không giám sát để phát hiện các cuộc tấn công DDoS và quét cổng trên mạng SDN.

Để cải thiện việc so sánh giữa các phương pháp, trên các phương pháp có giám sát (kNN, SVM, MLP và LSTM-2), chúng tôi đã sử dụng một bộ dữ liệu để huấn luyện, đại diện cho một ngày thu thập dữ liệu lưu lượng mạng. Ngày này bao gồm lưu lượng thông thường và các cuộc tấn công DDoS và quét cổng. Thông tin về số lượng mẫu cho các lớp được minh họa trong Bảng 3.

Bảng 3: Thông tin về các mẫu cho lớp

A black numbers on a white background

Description automatically generated

Phân tích chi tiết được minh họa trong Hình 11, nơi chúng tôi trình bày kết quả các số liệu của các phương pháp so sánh. Hệ thống LSTM-FUZZY cho thấy tỷ lệ dương giả thấp, đạt 0,25%. Phương pháp so sánh LSTM-2 cho thấy tỷ lệ dương giả cao nhất, lên tới 1,53%. Mặt khác, các phương pháp SVM và kNN không cho thấy tỷ lệ dương giả. Xét về các số liệu thu hồi và độ chính xác, tất cả các phương pháp đều cho thấy giá trị trên 98%. Không có phương pháp nào đạt hiệu suất tốt hơn trên tất cả các số liệu được đánh giá.

A graph with multiple colored lines

Description automatically generated with medium confidence

Hình 11: Kết quả phát hiện trong kịch bản đầu tiên giữa LSTM-FUZZY và các phương pháp khác.

Hình 12 thể hiện đường cong ROC cho mỗi phương pháp so sánh, giúp trực quan hóa khả năng phát hiện bất thường của chúng. Thông qua đường cong ROC, có thể xác định phương pháp nào có khả năng phù hợp nhất để phát hiện sự bất thường. Bằng cách phân tích các kết quả thu được, rõ ràng phương pháp LSTM-FUZZY thu được kết quả tốt nhất so với các phương pháp khác. LSTM-FUZZY đưa ra giá trị AUC là 99,87%, ngụ ý rằng phương pháp này cho tỷ lệ dương thật cao hơn với tỷ lệ dương giả thấp nhất.

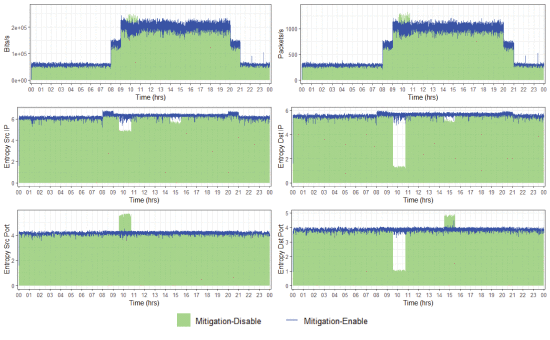
A graph of a number of lines

Description automatically generated with medium confidence

Hình 12: Đường cong ROC của các phương pháp so sánh kịch bản 1.

1. **Giảm thiểu**

Dựa trên các cảnh báo được tạo ra bởi quá trình phân loại của LSTM-FUZZY, các chính sách giảm thiểu tấn công đã được áp dụng. Hình 13 thể hiện các thuộc tính lưu lượng: màu xanh lá cây là lưu lượng không áp dụng giảm thiểu, màu xanh dương là lưu lượng sau khi giảm thiểu. Tấn công DdoS trong khoảng thời gian từ 9:45:00 đến 10:35:00, chúng ta có báo cáo tấn công DDoS. Trong giai đoạn này, lưu lượng gói và bit tăng khi mô-đun giảm thiểu bị tắt. Khi kích hoạt mô-đun, lưu lượng giảm về mức bình thường do loại bỏ các gói bất thường. Giai đoạn tấn công Portscan từ 14:30 đến 15:30 gây ra những thay đổi nhỏ về hành vi lưu lượng. Khi áp dụng giảm thiểu, các thuộc tính bị ảnh hưởng cũng trở lại bình thường.



Hình 13: Biểu đồ hiển thị lưu lượng truy cập không được giảm thiểu và lưu lượng truy cập được giảm thiểu trong các khoảng thời gian có điểm bất thường trong kịch bản 1.

Trong kịch bản này, chúng ta cũng đã áp dụng kiểm định McNemar và tỷ lệ gói bị loại bỏ để phân tích hiệu quả của quy trình giảm thiểu tấn công. Mức ý nghĩa cho kiểm định McNemar là α = 5%. BẢNG 4 cung cấp thông tin về phân loại lưu lượng thành bất thường và bình thường trước và sau khi thực hiện giảm thiểu. Bằng cách áp dụng kiểm định vào thông tin trong bảng, giá trị p thu được là dưới 2.2 × , nhỏ hơn giá trị α. Do đó, giả thuyết null trong trường hợp này cũng bị bác bỏ. Điều này cho thấy thực sự có sự khác biệt giữa các tần số, nghĩa là quy trình giảm thiểu đã hiệu quả trong việc giảm thiểu tác động của mối đe dọa. Ngoài ra, tỷ lệ các gói bất thường bị hệ thống loại bỏ là 99,88%. Kết quả này cho thấy hầu hết các gói tin bất thường đều bị loại bỏ.

Bảng 4: Bảng dự phòng để đánh giá quá trình giảm thiểu trong Kịch bản 1

|  |  |  |
| --- | --- | --- |
|  | Bình thường(sau) | Bất thường(trước) |
| Bình thường(trước) | 78323 | 86 |
| Bất thường(sau) | 7728 | 262 |

**E. Kịch bản đánh giá 2**

Kịch bản này nhằm đánh giá mô-đun phát hiện của hệ thống bằng cách áp dụng các loại tấn công DDoS khác nhau. Như đã đề cập trước đó, bộ dữ liệu CICDDoS 2019 [60] do Viện An ninh mạng Canada phát triển gồm hai ngày (huấn luyện và kiểm thử). Ngày huấn luyện bao gồm 12 loại tấn công DDoS, và ngày kiểm thử chứa sáu loại tấn công DDoS.

Hệ thống được đề xuất trong công trình này phân tích lưu lượng mạng mỗi 1 giây. Do đó, cần thực hiện xử lý sơ bộ bộ dữ liệu CICDDoS 2019 để tóm tắt các luồng thành các nhóm theo khoảng thời gian một giây dựa trên dấu thời gian của chúng. Sau khi nhóm, chúng tôi nhận thấy rằng tất cả các khoảng thời gian chỉ được tạo bởi các mẫu bất thường. Để giải quyết vấn đề này, chúng tôi đã tách các luồng theo bất thường và bình thường trước khi xử lý thành các khoảng thời gian 1 giây.

Tuy nhiên, kích thước của các mẫu luồng chứa các tấn công DDoS vượt trội so với dữ liệu bình thường do đặc điểm của các cuộc tấn công. Điều này không ảnh hưởng đến LSTM-FUZZY, vì trong giai đoạn huấn luyện, phương pháp chỉ sử dụng các mẫu bình thường để đặc trưng cho lưu lượng mạng, nhưng nó có thể dẫn đến quá khớp đối với các phương pháp SVM, kNN, MLP và LSTM-2 sử dụng phương pháp có giám sát trong quá trình huấn luyện.

Để duy trì đặc tính và tính đại diện của dữ liệu được áp dụng trong quá trình huấn luyện, giải pháp được áp dụng để giải quyết vấn đề này là lấy mẫu các luồng ngẫu nhiên cho từng loại tấn công. Thông qua các thử nghiệm thực nghiệm, đối với mỗi loại tấn công, chúng tôi đã chọn tỷ lệ gấp 5 lần các luồng bình thường. Bộ huấn luyện bị giảm nhưng vẫn duy trì đủ số lượng mẫu cho quá trình huấn luyện.

Giống như kịch bản đầu tiên, hiệu quả của LSTM-FUZZY được so sánh với các phương pháp cổ điển, kNN, SVM, MLP, LSTM-2 và PSO-DS. Hình 15 minh họa kết quả của các số liệu thu được cho từng phương pháp. Về số liệu thu hồi (recall), rõ ràng là LSTM-FUZZY đạt được hiệu suất vượt trội so với các phương pháp so sánh khác, đạt giá trị 93,13% cho số liệu này, tiếp theo là LSTM-2, PSO-DS, kNN, MLP và SVM, đạt mức tương ứng là 90,53%, 89,66%, 89,27%, 87,92% và 87,92%.

A graph of a function

Description automatically generated with medium confidence

Hình 14: Đường cong ROC của các phương pháp so sánh kịch bản 2.

A graph with multiple colors

Description automatically generated with medium confidence

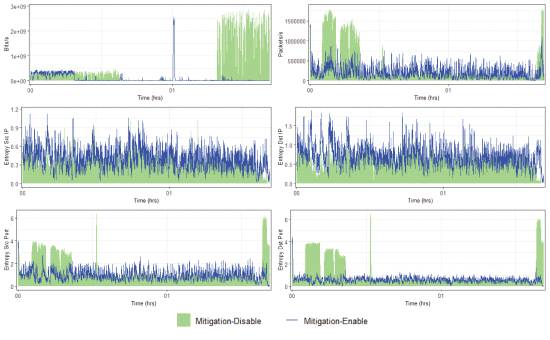
Hình 15: Kết quả phát hiện trong kịch bản thứ hai giữa LSTM-FUZZY và các phương pháp khác.

Mức độ chính xác (precision) là số liệu tiếp theo được đánh giá. Một lần nữa, LSTM-FUZZY đạt được kết quả tốt nhất với tỷ lệ 97,89%. Các phương pháp còn lại xếp theo thứ tự giảm dần là SVM, LSTM-2, MLP, kNN và PSO-DS, với tỷ lệ lần lượt là 97,74%, 96,61%, 94,98%, 89,27% và 81,19%. Xét về tỷ lệ dương giả (false-positive rate), LSTM-FUZZY và SVM có tỷ lệ bằng nhau là 2,2%, có thể coi là kết quả tốt. Các phương pháp còn lại là MLP, LSTM-2, kNN và PSO-DS lần lượt có tỷ lệ 5,52%, 9,98%, 11,53% và 20,76%. Hệ thống đề xuất cho thấy kết quả vượt trội so với các phương pháp so sánh khác, ngoại trừ SVM đạt kết quả tương đương. Tuy nhiên, khi sử dụng đường cong ROC, sự cải thiện giữa các phương pháp so sánh được quan sát rõ ràng hơn. Mặc dù kết quả tương đồng, hiệu suất của hệ thống đề xuất là một cải tiến đáng kể, vì các mạng máy tính hiện đại hoạt động với các đường truyền có tốc độ cao. Trong một ngày hoạt động của mạng, một tỷ lệ nhỏ các cuộc tấn công không được phát hiện có thể gây thiệt hại cho hoạt động của nó. Ví dụ, vào tháng 10 năm 2016, một cuộc tấn công DDoS với 100 nghìn điểm cuối độc hại đã vượt qua băng thông 1,2 Tbps [69]. Giống như kết quả đã trình bày trong kịch bản đầu tiên, phương pháp LSTM-FUZZY cũng đạt hiệu quả trung bình tốt hơn các phương pháp so sánh khác trong kịch bản thứ hai, đạt được kết quả kiểm thử hứa hẹn, khiến nó trở thành một kỹ thuật hiệu quả trong việc phát hiện các loại tấn công DDoS khác nhau.

Cũng giống như trong kịch bản trước, đường cong ROC được sử dụng để xác định phương pháp nào thể hiện hiệu suất tốt nhất trong việc phát hiện tấn công. Hình 14 thể hiện phân tích trực quan của đường cong ROC. Thông qua AUC, chúng ta có thể thấy rằng LSTM-FUZZY là phương pháp đạt được sự cân bằng tốt nhất giữa tỷ lệ dương thật (true-positive rate) và tỷ lệ dương giả (false-positive rate), đạt giá trị 96,22%. Các phương pháp tiếp theo là SVM, MLP, kNN, LSTM-2 và PSO-DS với các giá trị lần lượt là 94,93%, 91,28%, 86,53%, 82,01% và 80,63%.

1. **Giảm thiểu**

Trong kịch bản này, chúng tôi đã đánh giá hiệu quả giảm thiểu các cuộc tấn công DDoS từ bộ dữ liệu CICDDoS 2019. Hình 16 minh họa hành vi lưu lượng của ngày kiểm thử có báo cáo tấn công DDoS khi mô-đun giảm thiểu bị tắt và so sánh hành vi của nó khi giảm thiểu được kích hoạt. Lưu lượng được tạo ra mà không áp dụng chính sách giảm thiểu được biểu thị bằng vùng màu xanh lá cây, và đường màu xanh lam cho thấy lưu lượng sau khi áp dụng giảm thiểu tấn công DDoS. Xét về mặt trực quan, chúng ta có thể thấy khi các cuộc tấn công được giảm thiểu, các giá trị thuộc tính được phân tích sẽ trở lại hành vi mong đợi của nó.



Hình 16: Phân tích lưu lượng truy cập bằng cách tắt và bật mô-đun giảm thiểu vào ngày thử nghiệm từ bộ dữ liệu CICDDoS 2019.

Kiểm định MacNemar được áp dụng với mức ý nghĩa α = 5 % và giả thuyết null cho rằng các tần số cận bằng nhau. Sau khi áp dụng kiểm định vào BẢNG 5 , giá trị p thu được là 2.2 × , nhỏ hơn giá trị α. Do đó, giả thuyết null bị bác bỏ, cho thấy thực sự có sự khác biệt giữa các tần số biên, nghĩa là quy trình giảm thiểu đã hiệu quả.Hơn nữa, tỷ lệ các gói bất thường bị loại bỏ là 99,20%, cho thấy hầu hết các gói bất thường đã được giảm thiểu.

Bảng 5: Bảng dự phòng áp dụng để đánh giá mức độ giảm thiểu trong Kịch bản 2

|  |  |  |
| --- | --- | --- |
|  | Normal(after) | Anomalous(after) |
| Normal(before) | 4811 | 136 |
| Anomalous(before) | 2175 | 68 |

## V. KẾT LUẬN

Trong nghiên cứu này, chúng tôi trình bày một hệ thống mô-đun để tự động phát hiện và giảm thiểu các bất thường trong mạng SDN. Hệ thống gồm ba mô-đun hoạt động tự động, giúp việc giám sát, phát hiện và giảm thiểu tấn công dễ dàng hơn. Trong mô-đun đầu tiên, chịu trách nhiệm mô tả đặc tính lưu lượng, chúng tôi đã phát triển một phương pháp mới để dự đoán hành vi bình thường của mạng bằng cách áp dụng bộ nhớ dài hạn ngắn (LSTM) bán giám sát với luồng IP. Ở phần thứ hai, chúng tôi đề xuất cơ chế nhận dạng tấn công thông qua bất đẳng thức Bienaymé-Chebyshev kết hợp với logic mờ. Cuối cùng, trong mô-đun thứ ba, chúng tôi đã áp dụng các chính sách giảm thiểu tự động hóa để hạn chế thiệt hại do các cuộc tấn công gây ra và duy trì hoạt động của mạng.

Để đánh giá hệ thống, chúng tôi đã sử dụng hai kịch bản với những đặc điểm riêng biệt. Trong kịch bản đầu tiên, chúng tôi đã sử dụng dữ liệu SDN được mô phỏng bằng công cụ Mininet và bộ điều khiển Floodlight, bao gồm các khoảng thời gian có tấn công DDoS và Portscan. Trong kịch bản thứ hai, chúng tôi đã sử dụng tập dữ liệu công khai có tên CICDDoS 2019. Tập dữ liệu này bao gồm 12 loại tấn công DDoS khác nhau. Để đánh giá mô-đun phát hiện, chúng tôi đã so sánh LSTM-FUZZY với các phương pháp khác hiện có trong tài liệu, bao gồm SVM, kNN, MLP, LSTM-2 và PSO-DS. Trong cả hai kịch bản, chúng tôi đã so sánh hiệu suất của phương pháp đề xuất với các phương pháp khác. Dựa trên kết quả thu được, LSTM-FUZZY cho thấy hiệu suất vượt trội so với các phương pháp khác, đạt được tỷ lệ dương giả thấp và tỷ lệ chính xác, thu hồi và AUC cao.

Trong kịch bản đầu tiên, chúng tôi đã áp dụng các chính sách giảm thiểu dựa trên loại tấn công được mô-đun phát hiện xác định. Trong mô-đun này, chúng tôi đã xác định các luồng nghi ngờ dựa trên phân tích địa chỉ IP và cổng tạo nên khoảng thời gian bất thường. Loại bỏ các luồng này. Qua kiểm định McNemar và giảm tốc độ gói tin bất thường, cho thấy mô-đun này đạt được hiệu suất khả quan, giảm thiểu ảnh hưởng của các cuộc tấn công.

Khả năng học hỏi của LSTM để trích xuất các mẫu ngắn hạn và dài hạn cho phép ứng dụng dự đoán hành vi bình thường của lưu lượng mạng. Mô-đun đã tạo ra các dự đoán phù hợp gần với hành vi lưu lượng thực tế, và có thể áp dụng chúng trong giai đoạn phát hiện. Các đặc tính của Logic mờ cho phép phát hiện bất thường theo cách không giám sát, ngụ ý rằng hệ thống không cần dữ liệu được gán nhãn. Ưu điểm của việc sử dụng kỹ thuật này là làm cho việc vận hành hệ thống dễ dàng hơn và loại bỏ nhu cầu sử dụng tập dữ liệu được gán nhãn, điều này đòi hỏi nhiều công việc và có thể chứa đầy lỗi của con người. Hơn nữa, Logic mờ hoạt động trong việc phát hiện các cuộc tấn công DDoS khác nhau với tỷ lệ dương giả mạo thấp, cho phép hệ thống hoạt động trong môi trường SDN hiện tại với độ chính xác cao để phát hiện và giảm thiểu những cảnh báo sai.

Kết quả thu được cho thấy các module tạo nên hệ thống đề xuất đều hoạt động hiệu quả, đáp ứng được mục tiêu được giao cho từng module. Việc thực hiện các hoạt động do hệ thống thực hiện là tự động, nghĩa là quá trình giám sát, xác định các sự kiện bất lợi và các biện pháp ứng phó được thực hiện mà không cần sự can thiệp của con người. Việc giám sát và quản lý mạng là một hoạt động phức tạp. Việc hệ thống tự động giúp giảm tải công việc cho quản trị viên, đảm bảo mạng vận hành trơn tru và hiệu quả. Do đó, hệ thống được phát triển trong nghiên cứu này có thể được áp dụng để cộng tác và tạo điều kiện thuận lợi cho các thủ tục quản lý cũng như đảm bảo tính sẵn có của các dịch vụ được cung cấp.

Kiến trúc module của hệ thống cho phép duy trì và điều chỉnh các kỹ thuật khác để mô tả lưu lượng truy cập, phát hiện và giảm thiểu sự bất thường trong môi trường SDN. Đặc điểm này cho phép hệ thống thích nghi khi động lực mạng thay đổi và xuất hiện các nhu cầu bảo mật mới. Do đó, công việc trong tương lai có thể khám phá các lỗ hổng khác và kết hợp các chính sách giảm thiểu để đáp ứng các nhu cầu bảo mật mới có thể xuất hiện trong môi trường mạng SDN. Một điểm khác có thể được mở rộng là khám phá nhiều thử nghiệm hơn trong các tình huống khác với các loại cấu trúc liên kết và tấn công khác nhau.

## TÀI LIỆU THAM KHẢO