BLOCKCHAIN-BASED SOLUTION TO SECURITY MULTI-CONTROLLERS IN SOFTWARE-DEFINED NETWORKS AGAINST DENIAL-OF-SERVICE ATTACKS

Tran Thi Nga*, Chu Thi Ngoc Quynh
Academy of Cryptography Techniques

ARTICLE INFO

Received: 08/8/2024
Revised: 30/9/2024
Published: 30/9/2024

KEYWORDS

Software-defined Network
Multi-Controller
Blockchain
DoS Attack
ONOS

ABSTRACT

Multi-controller-based software-defined networks aid in enhancing network scalability, network availability and management ability. However, it still faces significant challenges, such as consistency between controllers, which can reduce performance and network operability against multiple attacks. Denial-of-service attacks significantly affect all the different layers of the network; hence, to address this challenge, we propose a solution using blockchain technology to ensure the security of multi-controllers against denial-of-service attacks. The paper utilizes the mininet tool and ONOS software to simulate multi-controllers for software-defined networks. Simultaneously, the paper adopts multichain to establish a private blockchain, which facilitates block creation, sending and the receiving blocks among controllers. Experimental results show that the application of a consensus mechanism on the blockchain helps detect denial-of-service attacks on controllers. From there, it helps network administrators to take timely actions to ensure the safety of multiple controllers in the network.

GIẢI PHÁP SỬ DỤNG BLOCKCHAIN ĐỂ ĐẢM BẢO AN TOÀN CHO ĐA BỘ ĐIỀU KHIỂN TRONG MẠNG ĐỊNH NGHĨA MỀM TRƯỚC TẤN CÔNG TỪ CHỐI DỊCH VỤ

Trần Thị Ngà*, Chu Thị Ngọc Quỳnh
Học viện Kỹ thuật mật mã

THÔNG TIN BÀI BÁO

Ngày nhận bài: 08/8/2024
Ngày hoàn thiện: 30/9/2024
Ngày đăng: 30/9/2024

TỪ KHÓA

Mạng định nghĩa mềm
Đa bộ điều khiển
Blockchain
Tấn công DoS
ONOS

TÓM TẮT

Mạng định nghĩa mềm dựa trên đa bộ điều khiển hỗ trợ nâng cao khả năng mở rộng mạng, tính sẵn sàng, và khả năng quản lý của mạng. Tuy nhiên, nó vẫn gặp phải những vấn đề như tính nhất quán giữa các bộ điều khiển, điều này có thể làm giảm hiệu suất và khả năng hoạt động của mạng trước một số tấn công. Tấn công từ chối dịch vụ là tấn công có ảnh hưởng tới toàn bộ các lớp khác nhau của mạng; do đó, để giải quyết vấn đề này, chúng tôi đề xuất giải pháp sử dụng công nghệ blockchain để đảm bảo an toàn cho đa bộ điều khiển trước tấn công từ chối dịch vụ. Bài báo sử dụng công cụ mininet và phần mềm ONOS để mô phỏng đa bộ điều khiển cho mạng định nghĩa mềm. Đồng thời, sử dụng multichain để tạo blockchain riêng cho phép tạo khối, gửi, nhận các khối giữa các bộ điều khiển. Kết quả thực nghiệm chỉ ra ứng dụng cơ chế đồng thuận trong blockchain giúp phát hiện được tấn công DoS vào bộ điều khiển. Từ đó, giúp người quản trị mạng có thể đưa ra những xử lý kịp thời nhằm đảm bảo an toàn cho đa bộ điều khiển trong mạng.

DOI: https://doi.org/10.34238/tnu-jst.10897

* Corresponding author. *Email: tranthinga@actvn.edu.vn*

1. Giới thiệu

Ngày nay, nhờ sự phát triển của Internet, mọi thứ đều có thể truy cập dễ dàng, mọi lúc mọi nơi. Cùng với đó, việc sử dụng rộng rãi các xu hướng công nghệ mới như điện toán đám mây, dữ liệu lớn, và kết nối vạn vật (IoT) làm cho việc vận hành và quản lý trở lên khó khăn. Do đó, mạng được định nghĩa mềm (SDN) ra đời như một mô hình mạng đầy hứa hẹn để giải quyết những vấn đề trên. Khác với mạng truyền thống, SDN tách biệt mặt phẳng điều khiển và mặt phẳng dữ liệu để đạt được kiến trúc điều khiển tập trung hợp lý, cung cấp khả năng lập trình để định cấu hình mạng. Với tư cách là người ra quyết định, bộ điều khiển SDN đóng vai trò quan trọng trong SDN. Mặc dù, các nghiên cứu trước đây đã chỉ ra rằng một bộ điều khiển duy nhất dẫn đến kém hiệu quả trong việc đảm bảo tính sẵn sàng và mở rộng mạng SDN. Để quản lý mạng quy mô lớn, đa bộ điều khiển được đề xuất nhằm giảm độ trễ phản hồi của các yêu cầu thông qua cân bằng tải và tránh tình trạng quá tải bộ điều khiển, góp phần cải thiện an toàn cho mạng SDN. Tuy nhiên, nó cũng đặt ra những thách thức mới, một trong những thách thức quan trọng của đa bộ điều khiển là tính nhất quán giữa các bộ điều khiển, bởi quá trình truyền dữ liệu các bộ điều khiển phải đưa ra quyết định dựa trên thông tin mạng nhất quán và chặt chẽ [1].

Blockchain gần đây được nhiều nhà nghiên cứu sử dụng để phát hiện hoặc ngăn chặn tấn công tiêm lỗi, tấn công xen giữa và cả tấn công DoS vào mạng SDN [2] – [7]. Nó là một sổ cái phân tán trong đó các giao dịch được ghi lại bằng một hàm băm mật mã. Một nút chứa dữ liệu, giá trị băm hiện tại và giá trị băm của khối trước đó trong khối. Một nút trong blockchain có ba nhiệm vụ cụ thể như lưu trữ lịch sử giao dịch khối, xác thực khối mới và cập nhật khối cho các nút khác để đảm bảo tất cả các nút trên blockchain có thông tin mới nhất. Với việc ứng dụng cơ chế đồng thuận trong blockchain để xác thực khối được tạo trước khi khối được cập nhật vào blockchain [8]. Lokesh cùng cộng sự đã đề xuất sử dụng blockchain để đảm bảo an toàn cho một bộ điều khiển, bài báo tập trung vào luồng điều khiển của bộ điều khiển Opendaylight [2]. Trong [3], blockchain cũng được sử dụng để đảm bảo giao tiếp giữa các bộ điều khiển SDN và các thành phần mạng khác, đồng thời phát hiện việc tiêm sai dữ liệu. Sanyal cùng cộng sự [4], đề xuất kiến trúc blockchain phân tán với lớp sương mù nằm giữa lớp điều khiển và lớp dữ liệu để phát hiện tấn công từ chối dịch vụ (DoS) trong SDN và giảm thiểu tác động của nó. Tuy nhiên, phương pháp này làm thay đổi đáng kể kiến trúc của mạng SDN và làm cho việc vận hành và quản lý trở nên phức tạp. Fernando và Wei [5], đã đề xuất một cơ sở hạ tầng bao gồm hai lớp: một lớp đa bộ điều khiển SDN và một lớp dựa trên blockchain. Các lệnh điều khiển/quản lý của các bộ điều khiển SDN được băm và ghi lại trong hợp đồng thông minh của blockchain và gửi đến bộ điều khiển SDN mục tiêu kiểm tra để xác nhận tính toàn vẹn của lệnh. Cùng ý tưởng sử dụng blockchain nhưng các tác giả trong [6], sử dụng thêm một lớp bảo mật trung gian giữa lớp điều khiển và lớp dữ liệu hoạt động như một proxy cho bộ điều khiển để phát hiện và loại bỏ lưu lượng bất thường của tấn công từ chối dịch vụ phân tán. Cũng là cơ chế phát hiện tấn công vào mặt phẳng điều khiển dựa vào blockachain nhưng Alkhamisi cùng các cộng sự lại tập chung phát hiện tấn công xen giữa và tấn công tiêm sai vào mặt phẳng điều khiển với việc sử dụng bộ điều khiển Ryu [7].

Xuất phát từ thực tế trên, bài báo đề xuất giải pháp sử dụng blockchain để đảm bảo an toàn cho kiến trúc đa bộ điều khiển SDN trước tấn công DoS. Giải pháp đề xuất tận dụng kiến trúc của các tác giả trong [3], nhưng thay đổi kịch bản thực hiện không phải thực hiện tiêm lỗi hoặc xen giữa vào bộ điều khiển từ mặt phẳng dữ liệu như các công trình trong [3], [7], mà thực hiện tấn công DoS trực tiếp vào một bộ điều khiển với giải pháp này nhóm tác giả ứng dụng cơ chế đồng thuận bằng chứng bỏ phiếu [3], [8], giúp phát hiện sớm tấn công DoS. Từ đó, giúp người quản trị mạng có thể đưa ra những xử lý kịp thời đảm bảo an toàn cho mạng. Đồng thời, giải pháp khắc phục được nhược điểm của các công trình trước đó không cần phải thay đổi cấu trúc mạng SDN làm cho mô hình mạng đa bộ điều khiển trở nên dễ kiểm soát, vận hành và đảm bảo an toàn giữa các bộ điều khiển [4] – [6], [9]. Thực nghiệm của bài báo được mô phỏng trên mininet [10], với việc sử dụng

bộ điều khiển ONOS [11]. Ngoài ra, bài báo cũng tiến hành thực hiện tấn công DoS để kiểm chứng giải pháp đề xuất.

Bài viết được bố cục theo 4 mục chính: Sau phần 1 giới thiệu, phần 2 trình bày phương pháp nghiên cứu. Ở phần 3, tác giả tiến hành thực hiện mô phỏng trên cơ sở đó đưa ra kết quả và thảo luận. Cuối cùng là kết luận và hướng phát triển.

2. Phương pháp nghiên cứu

2.1. Kiến trúc và các mối đe dọa đa bộ điều khiển của mạng SDN

Kiến trúc đa bộ điều khiển của mạng SDN bao gồm: Lớp ứng dụng, lớp điều khiển và lớp dữ liệu. Các phần sẽ liên kết với nhau thông qua giao thức hoặc các API [9]. Hình 1 mô tả kiến trúc và các điểm mục tiêu đe dọa đa bộ điều khiển của mạng SDN một cách đơn giản và đầy đủ [3].

Lớp ứng dụng

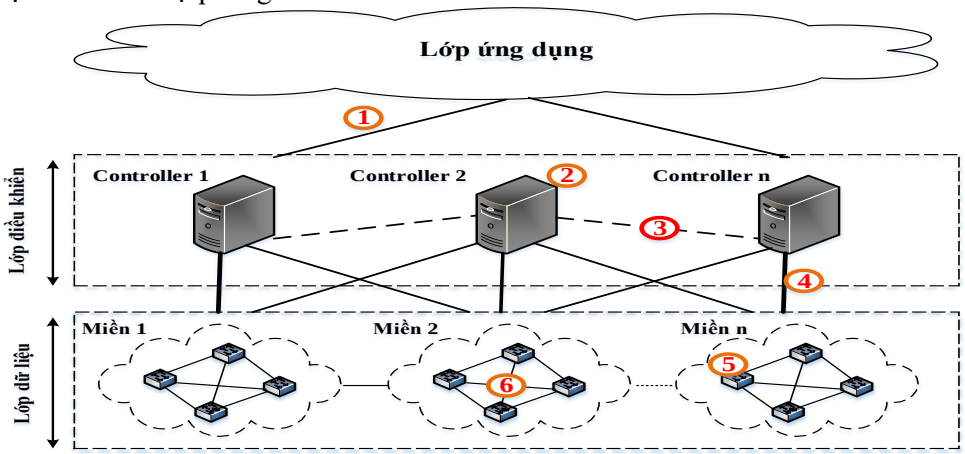
Là các ứng dụng được triển khai trên mạng, kết nối tới lớp điều khiển thông qua các API, cung cấp khả năng cho phép ứng dụng lập trình lại mạng (điều chỉnh các tham số trễ, băng thông, định tuyến…) thông qua lớp điều khiển lập trình giúp cho hệ thống mạng hoạt động tối ưu theo một yêu cầu nhất định.

Lớp điều khiển

Là nơi tập trung các bộ điều khiển (controller) thực hiện việc điều khiển và kiểm soát lưu lượng từ lớp ứng dụng và lớp cơ sở hạ tầng mạng. Các bộ điều khiển được triển khai theo phương thức phân tán. Hầu hết các bộ điều khiển của SDN hiện nay dựa trên giao thức Openflow.

Lớp dữ liệu

Lớp dữ liệu của hệ thống mạng, bao gồm các thiết bị mạng thực tế (vật lý hay ảo hóa) thực hiện việc chuyển tiếp gói tin theo sự điều khiển của lớp điều khiển. Một thiết bị mạng được hoạt động theo nhiều miền khác nhau, mỗi miền chịu sự kiểm soát của một bộ điều khiển chính và một số bộ điều khiển dự phòng.



Hình 1. *Kiến trúc và các mối đe dọa đa bộ điều khiển của mạng SDN*

Các mối đe dọa trong kiến trúc đa bộ điều khiển của mạng SDN

Có thể có nhiều mối đe dọa khác nhau trong môi trường đa bộ điều khiển SDN như: tiêm giả dữ liệu, tấn công xen giữa và tấn công DoS [3], [4], [6], [7]. Hình 1 cho thấy vị trí các mối đe dọa có thể xảy ra trong kiến trúc đa bộ điều khiển trong SDN. *Điểm 1*: Tấn công khai thác giao tiếp giữa lớp ứng dụng và lớp điều khiển. *Điểm 2*: Tấn công trực tiếp vào bộ điều khiển của mô hình đa bộ điều khiển. *Điểm 3 và 4*: Tấn công đường liên kết giữa các bộ điều khiển và giữa các thiết bị chuyển mạch. *Điểm 5*: Tấn công trực tiếp vào bộ chuyển mạch. *Điểm 6*: Tấn công đường kết nối giữa các bộ chuyển mạch.

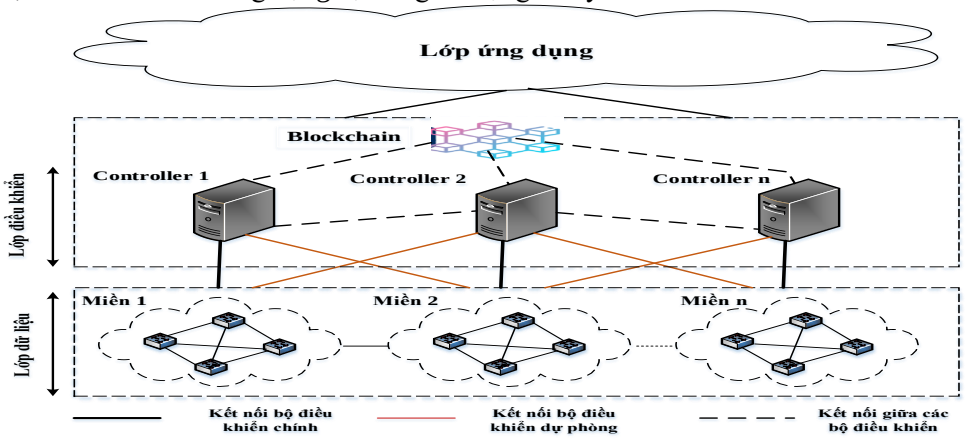
Các cuộc tấn công dù ở vị trí nào cũng có thể gây ra ảnh hưởng tới sự an toàn của đa bộ điều

khiển trong mạng SDN. Vì bộ điều khiển được coi là bộ não của mạng SDN để chuyển tiếp các thông tin trong mạng SDN [9]. Chính vì vậy, trong bài báo này tập trung vào tìm hiểu tấn công vào lớp điều khiển của SDN cụ thể là trực tiếp vào bộ điều khiển.

2.2. Giải pháp sử dụng blockchain để đảm bảo an toàn cho đa bộ điều khiển trong mạng định nghĩa mềm trước tấn công DoS

Tấn công DoS là tấn công có ảnh hưởng đến toàn bộ các lớp mạng khác nhau trong SDN. Hầu hết các tấn công này chủ yếu nhắm vào lớp điều khiển. Do đó, an toàn của bộ điều khiển đóng vai trò quan trọng trong sự thành công của SDN [7]. Trong cấu trúc đa bộ điều khiển SDN, việc duy trì chế độ xem mạng nhất quán giữa các bộ điều khiển để nâng cao độ an toàn là rất quan trọng [1], [3], [6], [7]. Để giải quyết vấn đề này, kiến trúc đa bộ điều khiển dựa trên blockchain cho SDN an toàn đã được đưa ra, kết quả nghiên cứu của họ đã khẳng định việc sử dụng blockchain đã đạt được sự thống nhất giữa các bộ điều khiển và có thể chống lại một số tấn công xen giữa, tấn công tiêm sai dữ liệu và cả tấn công DoS trong đa bộ điều khiển SDN [2] – [7].

Bài báo này nhóm tác giả trình bày ý tưởng đề xuất giải pháp đảm bảo an toàn cho đa bộ điều khiển trước tấn công DoS. Điểm khác của bài báo so với [3], là việc sử dụng công nghệ blockchain không chỉ đảm bảo tính thống nhất giữa các bộ điều khiển và chống lại tấn công tiêm sai dữ liệu vào mặt phẳng điều khiển với kiến trúc đa bộ điều khiển mà còn phát hiện được tấn công DoS vào bất kỳ bộ điều khiển nào bằng việc ứng dụng cơ chế đồng thuận trong blockchain. Đồng thời, bài báo còn giúp khẳng định với việc tích hợp blockchain vào các bộ điều khiển, giúp cho việc quản lý và mở rộng mạng linh hoạt, an toàn mà không làm thay đổi cấu trúc của mạng SDN giống như các công trình [4] – [6]. Đặc biệt, bài báo đi khai thác cơ chế an toàn của bộ điều khiển trước tấn công DoS, chứ không phải tấn công xen giữa và tấn công tiêm sai vào mặt phẳng điều khiển như các tác giả trong [7]. Ngoài ra, công cụ mà bài báo sử dụng để dựng đa controller là ONOS, còn Alkhamisi cùng cộng sự đang sử dụng là Ryu.



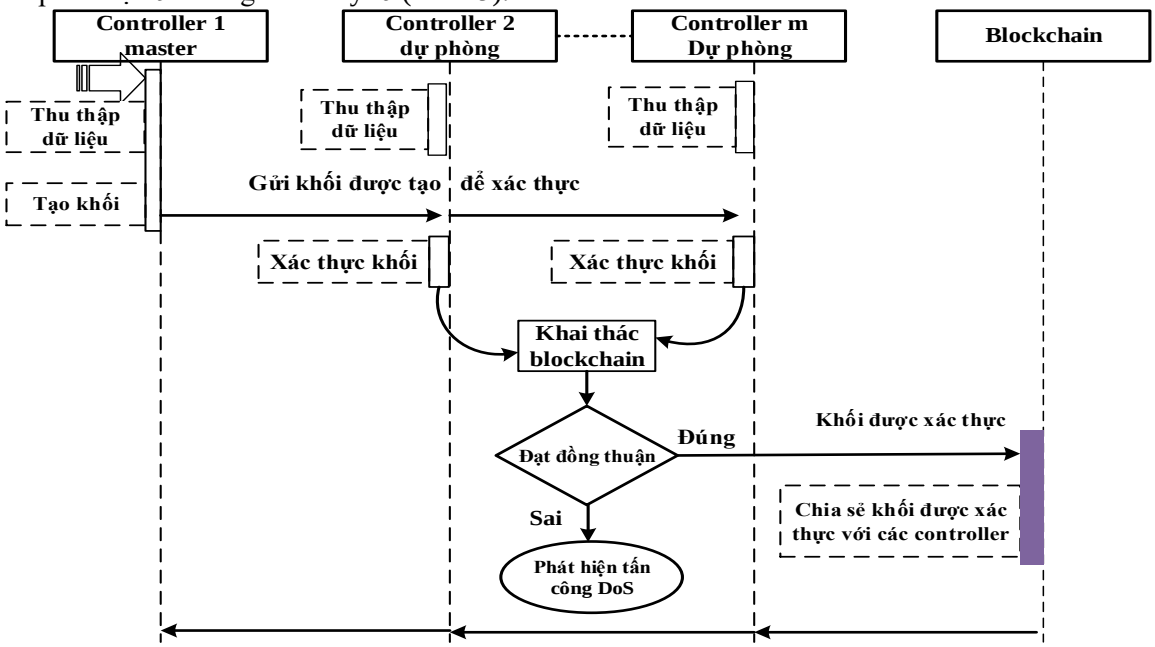
Hình 2. *Giải pháp sử dụng blockchain để đảm bảo an toàn cho đa bộ điều khiển trước tấn công DoS*

Trong mô hình đa bộ điều khiển SDN, các bộ điều khiển giao tiếp với nhau thông qua blockchain mỗi miền SDN được quản lý bởi một bộ điều khiển chính và được giám sát bởi một số bộ điều khiển dự phòng (Hình 2). Bộ điều khiển dự phòng nhận các sự kiện tương tự như bộ điều khiển chính nhưng không ảnh hưởng đến miền đó. Bộ điều khiển dự phòng có thể điều khiển miền trong trường hợp bộ điều khiển chính bị lỗi. Do đó, mỗi bộ điều khiển có thể duy trì chế độ xem của toàn mạng, các bộ điều khiển đóng vai trò là các miner trong blockchain.

Cơ chế đồng thuận

Các bộ điều khiển chính được coi là nút đáng tin cậy. Chúng có quyền đọc và ghi trên blockchain. Bộ điều khiển chính chịu trách nhiệm tạo khối mới. Việc tạo khối mới được kích hoạt bằng cách nhận các sự kiện mới gửi từ lớp dữ liệu. Khi bộ điều khiển chính nhận được thông

tin mới từ các thiết bị lớp dữ liệu trong miền của nó, nó sẽ tạo khối mới chứa đầy đủ thông tin và chia sẻ khối mới này với các bộ điều khiển dự phòng để xác thực. Các bộ điều khiển dự phòng khai thác cơ chế đồng thuận bằng chứng bỏ phiếu PoV trong blockchain [8], để xác thực khối được tạo bằng cách so sánh thông tin chứa trong khối với thông tin mà các bộ điều khiển dự phòng nhận được từ bộ chuyển mạch trong miền đó, thông qua hoạt động bỏ phiếu các miner có cùng quan điểm với nhau kết quả đưa ra cảnh báo đạt được sự đồng thuận, khi đó khối mới được cập nhật vào blockchain, đồng thời blockchain chia sẻ khối được xác thực tới các controller. Ngược lại thông qua hoạt động bỏ phiếu, chỉ cần một trong các miner có quan điểm khác với các miner còn lại kết quả đưa ra không đạt được sự đồng thuận khi đó khối mới không được xác thực và phát hiện tấn công DoS xảy ra (Hình 3).



Hình 3. *Sơ đồ luồng xử lý trong đa bộ điều khiển mạng định nghĩa mềm*

Xuất phát từ thực tế trên, bài báo tận dụng mô hình của A.Derhab cùng cộng sự [3] để phát hiện tấn công DoS không chỉ vào giao tiếp giữa các bộ điều khiển mà còn trực tiếp vào bộ điều khiển. Với kết quả xác thực khối đưa ra sau hoạt động bỏ phiếu không đạt sự đồng thuận, tức là các nội dung thông tin nhận được từ các bộ điều khiển là khác nhau. Đây cũng chính là mấu chốt để phát hiện tấn công DoS vào bất kỳ bộ điều khiển nào. Từ đây, người quản trị mạng sẽ xem xét để đưa ra những xử lý kịp thời đảm bảo an toàn cho đa bộ điều khiển trong SDN.

3. Kết quả và thảo luận

3.1. Mô phỏng thực nghiệm

3.1.1. Mô hình thực nghiệm

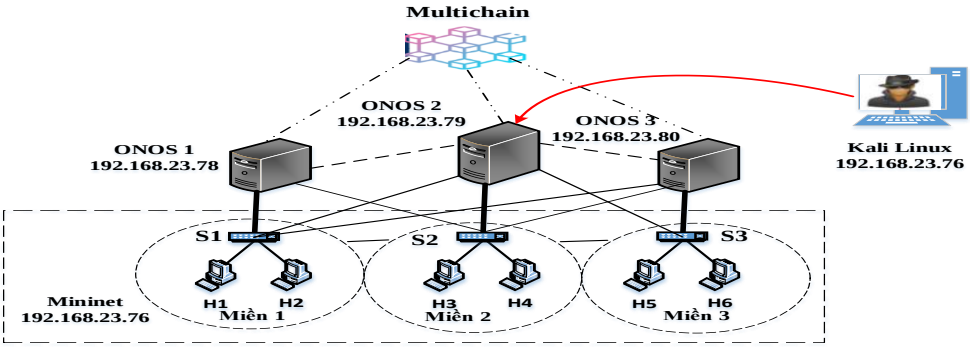
Mô hình thực nghiệm ở Hình 4 được thực hiện trên máy tính win 11 (64 bit), core i5, RAM 16G. Để xây dựng mô hình nhóm tác giả sử dụng các công cụ sau:

Mininet: Mininet là một công cụ giả lập mạng, bao gồm tập hợp các hosts đầu cuối, các switches và các liên kết trên một Linux kernel [10].

ONOS: Là phần mềm mã nguồn mở dành cho SDN controller sử dụng giao thức mở cung cấp khả năng kiểm soát tập trung, có khả năng lập trình được và theo dõi các thiết bị mạng. Giống như nhiều SDN Controllers khác, ONOS hỗ trợ OpenFlow, cũng như cung cấp các giải pháp mạng khác sẵn sàng để cài đặt khi có yêu cầu [11].

***Multichain*:** Là một nền tảng mã nguồn mở thực hiện một Blockchain riêng. Nó có thể phân quyền tới các nodes và điều khiển nodes nào được kết nối, gửi, và nhận giao dịch và node nào có thể tạo luồng và khối [12].

Đa bộ điều khiển SDN được tích hợp công nghệ Blockchain vào trong quá trình giao tiếp giữa các Controller giúp đảm bảo tính nhất quán giữa các Controller trong quá trình trao đổi thông tin giữa các bộ điều khiển. Ngoài ra, với việc ứng dụng cơ chế đồng thuận trong blockchain giúp các nhà quản trị sẽ nhận thấy những thay đổi bất thường xảy ra trong mạng. Trong thực nghiệm này, bài báo tiến hành tấn công DoS để thấy được những thay đổi của mạng trước và sau khi thực hiện tấn công. Từ đó, giúp các nhà quản trị mạng có thể đưa ra những xử lý kịp thời.



Hình 4. *Mô hình thực nghiệm*

3.1.2. Triển khai đa bộ điều khiển SDN

Trên mỗi máy ONOS Controller thiết lập các quy tắc theo sơ đồ hình 4, sử dụng code Python và các thư viện request.auth, interact, savoir, termcolor. Với kịch bản sử dụng các tham số theo Bảng 1.

Bảng 1. *Các tham số sử dụng trong mô hình thực nghiệm hình 4*

Miền 1	Miền 2	Miền 3
Controller 1 (Chính) IP: 192.168.23.78	**Controller 1 (Dự phòng)** IP: 192.168.23.78	**Controller 1 (Dự phòng)** IP: 192.168.23.78
Controller 2 (Dự phòng) IP: 192.168.23.79	**Controller 2 (Chính)** IP: 192.168.23.79	**Controller 2 (Dự phòng)** IP: 192.168.23.79
Controller 3 (Dự phòng) IP: 192.168.23.80	**Controller 3 (Dự phòng)** IP: 192.168.23.80	**Controller 3 (Chính)** IP: 192.168.23.80
S1 of:0000000000000001	**S2** of:0000000000000002	**S3** of: 0000000000000003
Host 1 IP: 10.0.0.1	**Host 3** IP: 10.0.0.3	**Host 5** IP: 10.0.0.5
Host 2 IP: 10.0.0.2	**Host 4** IP: 10.0.0.4	**Host 6** IP: 10.0.0.6

3.1.3. Triển khai blockchain trong đa bộ điều khiển SDN

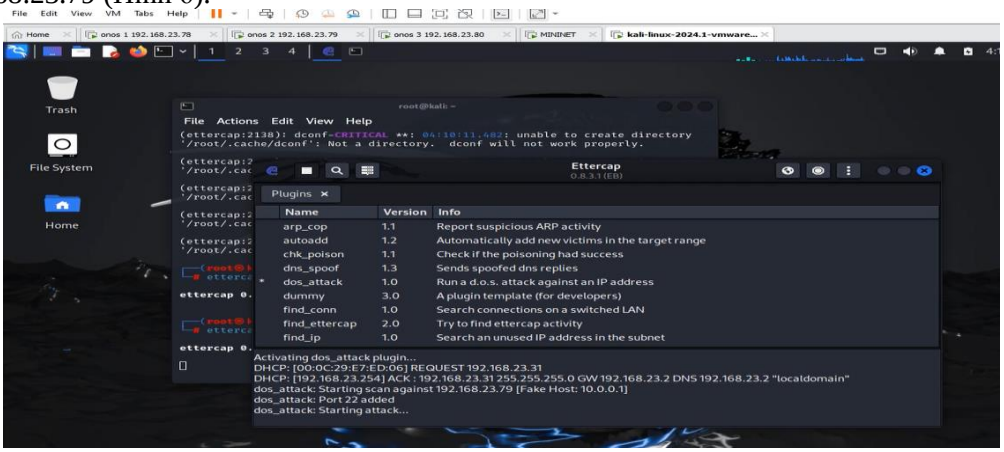
```
PENDING ADD ===> flow still panding
begining flow consensus at : 1.0054771149998487
flows consensus reached at : 0.012405273000240413
flows posted to block chain at : 0.012192940999739221
change in the flows detected at : 4063.180432687
PENDING ADD ===> flow still panding
begining flow consensus at : 1.0048602829997435
flows consensus reached at : 0.007834369000192964
flows posted to block chain at : 0.007963013999869872
change in the flows detected at : 4065.204528563
PENDING ADD ===> flow still panding
begining flow consensus at : 1.005991401999836
flows consensus reached at : 0.009431166000013036
```

Hình 5. *Kết quả khi các flow đạt được sự đồng thuận ở trạng thái bình thường*

Các máy ONOS được cài phần mềm multichain, trên máy ONOS chính sẽ khởi tạo chuỗi *sdn_chain1* và thực hiện cấp quyền đọc, ghi cho các node tham gia vào chuỗi thông qua địa chỉ *multichain chain_sdn1@192.168.23.78:7343*. Kết quả khi đó các luồng thông tin gửi tới các controller đạt được sự đồng thuận (Hình 5).

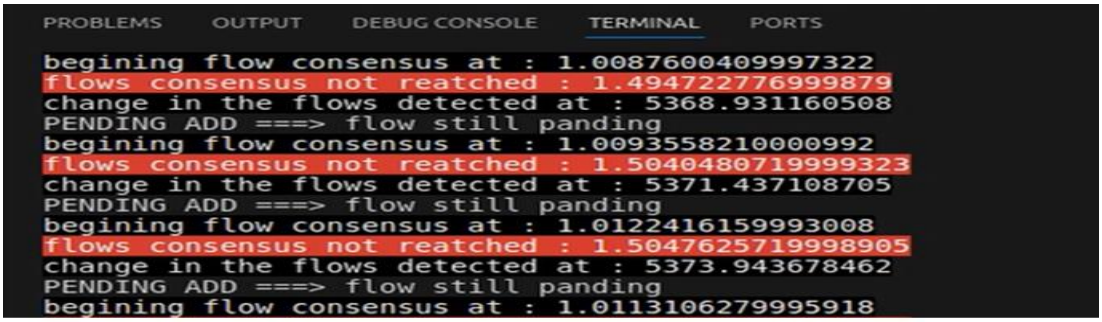
3.1.4. Tấn công DoS vào hệ thống

Tiến hành tấn công DoS với kịch bản mạo danh Host với IP:10.0.0.1 vào ONOS có địa chỉ 192.168.23.79 (Hình 6).



Hình 6. *Tấn công DoS vào ONOS controller có địa chỉ 192.168.23.79*

Khi bị tấn công DoS từ máy KaliLinux từ các quy tắc được thiết lập, các controller sẽ dựa vào cơ chế đồng thuận trong Blockchain, các controller dự phòng thu thập được các luồng thông tin không hợp lệ sẽ nhận được các cảnh báo "*flows consensus not reatched*" như Hình 7.



Hình 7. *Thông báo không đạt được sự đồng thuận khi tiến hành tấn công DoS*

3.2. Thảo luận

Sau khi đa bộ điều khiển dựa vào Blockchain hoạt động, ngoài việc có thể phát hiện luồng thông tin tiêm sai dữ liệu vào đa bộ điều khiển [3], nó còn giúp phát hiện tấn công DoS vào bất kỳ bộ điều khiển nào trong mặt phẳng điều khiển theo mô hình hình 4. Có thể thấy khi chưa có tấn công thời gian xử lý đồng thuận của thông tin trước khi bị tấn công và sau khi bị tấn công là khác nhau. Khi hệ thống hoạt động bình thường thì thời gian đồng thuận sẽ nằm trong khoảng 0,009s-0,012s (Hình 5). Sau khi tiến hành tấn công DoS vào ONOS controller dự phòng (Hình 6), nhận thấy thời gian xử lý sẽ tăng lên đến 1,494s – 1,547s. Đồng thời, đưa ra cảnh báo không đạt được sự đồng thuận (Hình 7). Việc đưa ra cảnh báo không đạt được sự đồng thuận giúp cho các nhà quản trị mạng có thể xem xét và có những xử lý phù hợp. Qua kết quả mô phỏng có thể khẳng định rằng việc sử dụng blockchain không chỉ giúp các bộ điều khiển trong mạng SDN đạt được sự thống nhất trong quản lý mạng, bởi bất kỳ thay đổi trong mạng SDN các controller đều nhận được trạng thái như nhau. Từ đó, giúp việc quản lý vận hành mạng đạt được sự thông suốt

tránh tình trạng phân cắt mạng khi có tấn công xảy ra. Đồng thời, kết quả của bài báo còn giúp các nhà nghiên cứu có cái nhìn đa chiều về cách thức tấn công và giải pháp phát hiện tấn công DoS trực tiếp vào mô hình đa bộ điều khiển trong mạng SDN.

4. Kết luận và hướng phát triển

Trong mạng SDN, công nghệ blockchain được sử dụng để đảm bảo an toàn cho các bộ điều khiển không chỉ giúp phát hiện tấn công tiêm sai dữ liệu vào mặt phẳng điều khiển mà nó còn giúp phát hiện được tấn công DoS vào bộ điều khiển. Bằng việc duy trì chế độ xem nhất quán giữa các bộ điều khiển nên khi có luồng thông tin khác nào gửi tới một trong các bộ điều khiển đều được gửi tới các bộ điều khiển còn lại. Với việc ứng dụng cơ chế đồng thuận trong blockchain giúp các bộ điều khiển có thể phát hiện bất kỳ thay đổi nào trong mạng đa bộ điều khiển SDN. Hơn nữa, theo hiểu biết của nhóm tác giả thì đây là một giải pháp hiệu quả giúp các nhà quản trị mạng có thể phát hiện tấn công DoS vào kiến trúc đa bộ điều khiển trong mạng định nghĩa mềm. Đồng thời, giải pháp này còn giúp kiến trúc mạng đa bộ điều khiển không phải thay đổi so với kiến trúc bộ điều khiển ban đầu. Hướng nghiên cứu tiếp theo, nhóm tác giả sẽ tập trung vào việc ngăn chặn tấn công DoS trong kiến trúc đa bộ điều khiển SDN.

TÀI LIỆU THAM KHẢO/ REFERENCES

[1] T. Hu, Z. Guo, P. Yi, T. Baker, and J. Lan, "Multi-controller Based Software-Defined Networking: A Survey," *in IEEE Access*, vol. 6, pp. 15980-15996, 2018.

[2] B. Lokesh and N. Rajagopalan, "A Blockchain-based security model for SDNs," *IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)*, Bangalore, India, 2020, pp. 1-6.

[3] A. Derhab, M. Guerriumi, M. Belaoued, and O. Chaikhrouhou, "BMC-SDN: Blockchain-Based Multicontroller Architecture for Secure Sofware-Defined Networks," *Wireless Communications and Mobile Computing*, vol. 2021, pp. 1-12, 2021.

[4] S. Sanyal, M. Barai, and A. Goplani, "A Novel Blockchain based Software Defined Network (SDN) Architecture to Curb the Impact of DoS/DdoS," *International Journal of Electrical, Electronics and Computers*, vol. 6, no. 5, pp. 12-24, 2021.

[5] P. Fernando and J. Wei, "Blockchain-powered software defined network-enabled networking infrastructure for cloud management," *in 2020 IEEE 17th Annual Consumer Communications & Networking Conference* (CCNC), Las Vegas, NV, USA, 2020, pp. 1-6.

[6] T. N. Cube, N. Dlodlo, and A. Terzoli, "BSD-Guard: A Collaborative Blockchain-Based Approach for Detection and Mitigation of SDN-Targeted DDoS Attacks," *Security and Communication Networks*, vol. 2022, pp. 1-16, 2022.

[7] A. Alkhamisi, I. Katib, and S. M. Buhari, "Blockchain-Based Control Plane Attack Detection Mechanisms for Multi-Controller Software-Defined Network," *Electronics*, vol. 13, no. 12, pp. 1-20, 2024.

[8] S. Fahim, S. M. K. Rahman, and S. Mahmood, "Blockchain: A Comparative Study of Consensus Algorithms PoW, PoS, PoA, PoV," *I. J. Mathematical Sciences and Computing*, vol. 9, no. 3, pp. 46-57, 2023.

[9] W. Braun and M. Menth, "Software-Defined Networking Using OpenFlow: Protocols, Applications and Architectural Design Choices," *Future Internet*, vol. 6, no. 2, pp. 302-336, 2014.

[10] K. K. Sharma and M. Sood, "Mininet as a container-based emulator for software defined networks," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 4, no. 12, pp. 681-685, 2014.

[11] P. Berde, M. Gerola, J. Hart, Y. Higuchi, M. Kobayashi, T. Koide, and G. Parulkar, "ONOS: Towards an open, distributed SDN OS," in *Proceedings of the Third Workshop on Hot Topics in Software Defined Networking*, Chicago, IL, USA, 2014, pp. 1-6.

[12] A. Ismailisufi, T. Popovic, N. Gligoric, S. Radonjic, and S. Sandi, "A Private Blockchain Implementation Using Multichain Open Source Platform," *2020 24th International Conference on Information Technology (IT)*, Zabljak, Montenegro, 2020, pp. 1-4.