TRƯỜNG ĐẠI HỌC BÁCH KHOA – ĐẠI HỌC ĐÀ NẴNG
KHOA ĐIỆN TỬ - VIỄN THÔNG

PHÁT HIỆN VÀ GIẢM THIỂU TẤN CÔNG DDOS BẰNG MACHINE LEARNING TRONG SDN

HỌC PHẦN: MẠNG ĐỊNH NGHĨA BẰNG PHẦN MỀM

GVHD: Tăng Anh Tuấn

Nhóm 4:

Lê Phạm Công 20KTMT1

Phan Công Danh 20KTMT1

Đà Nẵng, ngày 17 tháng 05 năm 2024

NỘI DUNG

1. Lý do chọn đề tài
2. Thiết kế hệ thống
3. Kết quả
4. Đánh giá
5. Kết luận

LÝ DO CHỌN ĐỀ TÀI

- Tấn công DDoS có thể gây ra mối đe dọa nghiêm trọng cho các dịch vụ mạng, dẫn đến tổn thất kinh tế lớn và thậm chí có thể gây ra những hậu quả thảm khốc khác.
- Việc tìm ra phương pháp phát hiện và ngăn chặn các cuộc tấn công DDoS trên nền tảng công nghệ Software Defined Network trở thành trọng yếu.

LÝ DO CHỌN ĐỀ TÀI

Phát hiện và giảm thiểu tấn công DDoS bằng Machine learning trong SDN

- Sử dụng bộ điều khiển Ryu-controller
- Trích xuất các features thông qua các Flow entry của SDN Switch
- Các loại tấn công DDoS được dùng trong đề tài: SYN, TCP và UDP
- Dùng mô hình Machine Learning để phát hiện các cuộc tấn công
- Phương pháp giảm thiểu: Chặn cổng đang nhận lưu lượng tấn công

THIẾT KẾ HỆ THỐNG

Cấu trúc hệ thống:

- **Application Plane**

  Xây dựng ứng dụng phát hiện và giảm thiểu DDoS sử dụng thuật toán Decision Tree

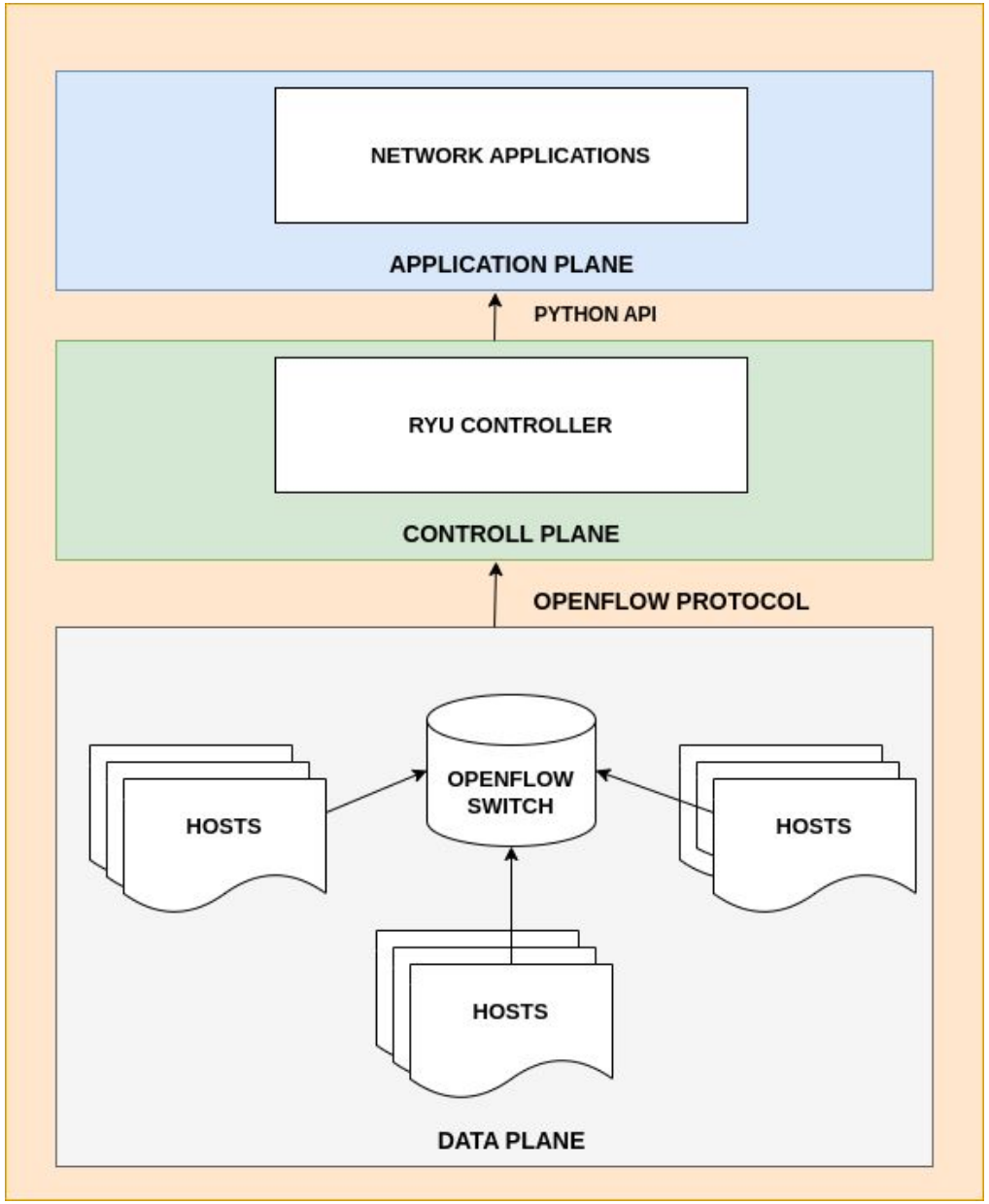
- **Controll Plane**

  Controll Plane sử dụng bộ điều khiển RYU phiên bản 4.34 để điều khiển mạng SDN

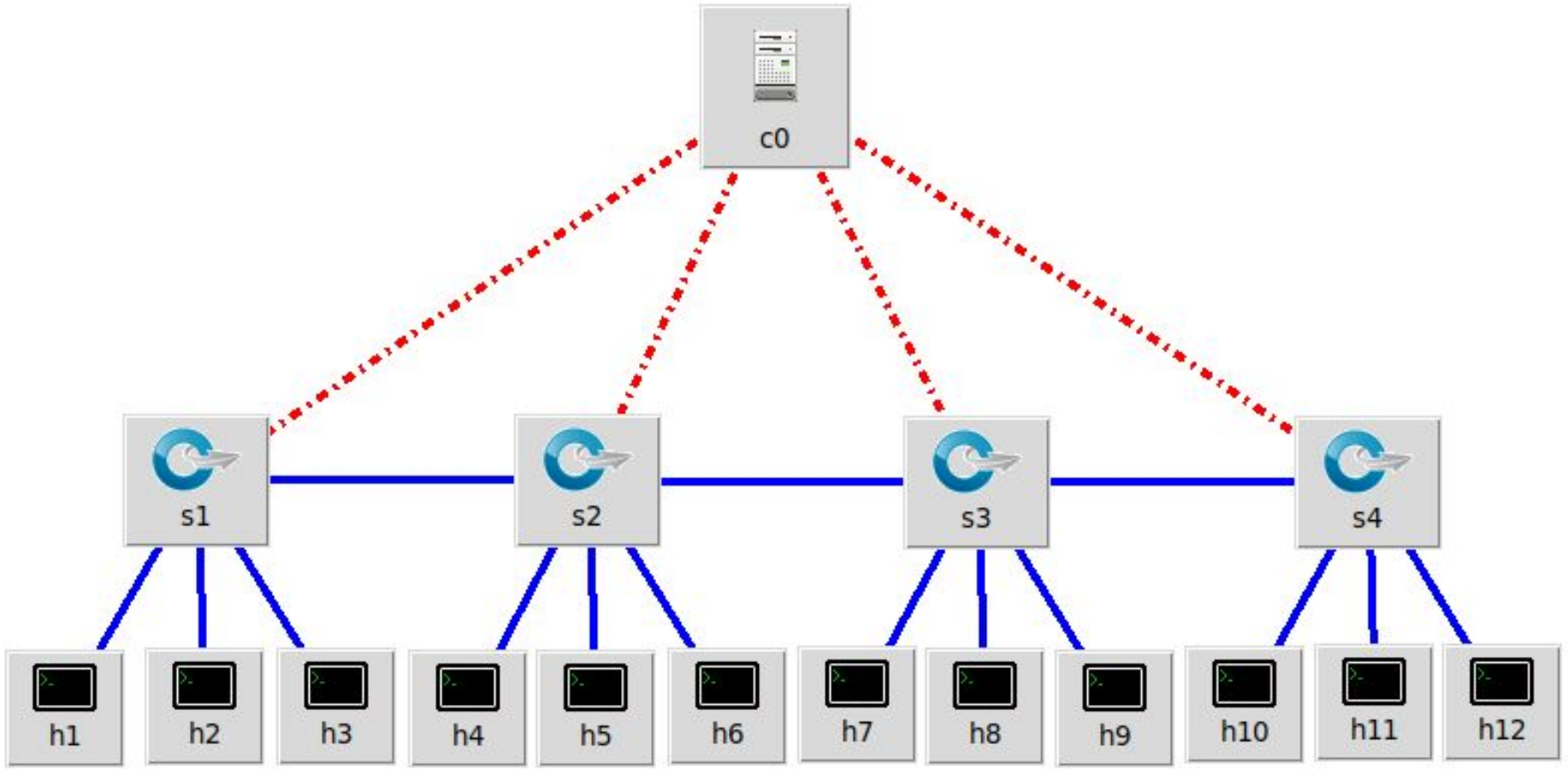
- **Data Plane**

  Sử dụng Mininet phiên bản 2.3.0 làm môi trường giả lập mạng.

  Data Plane giao tiếp với Controll Plane bằng OpenFlow Protocol phiên bản 1.3

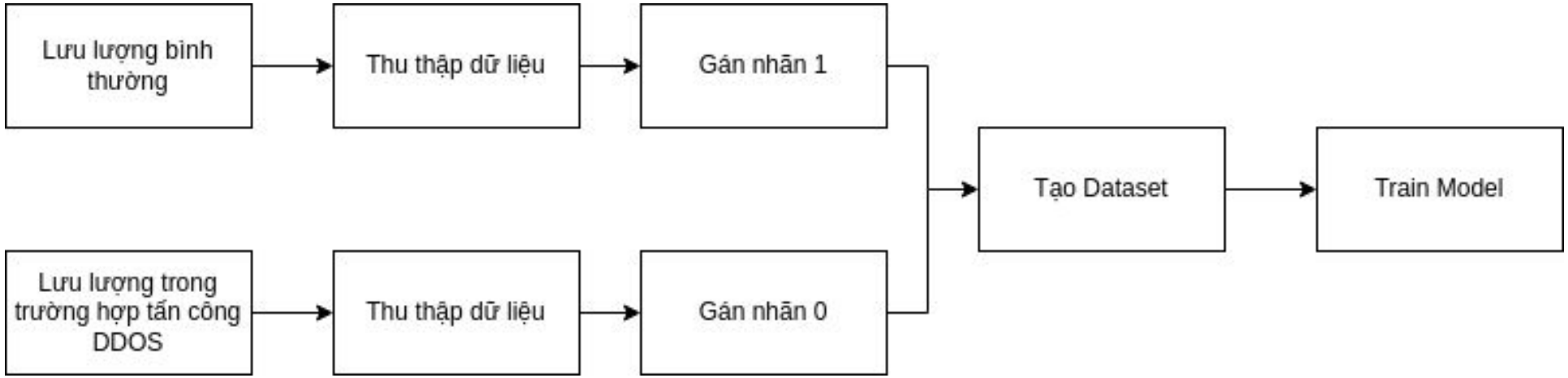


THIẾT KẾ HỆ THỐNG

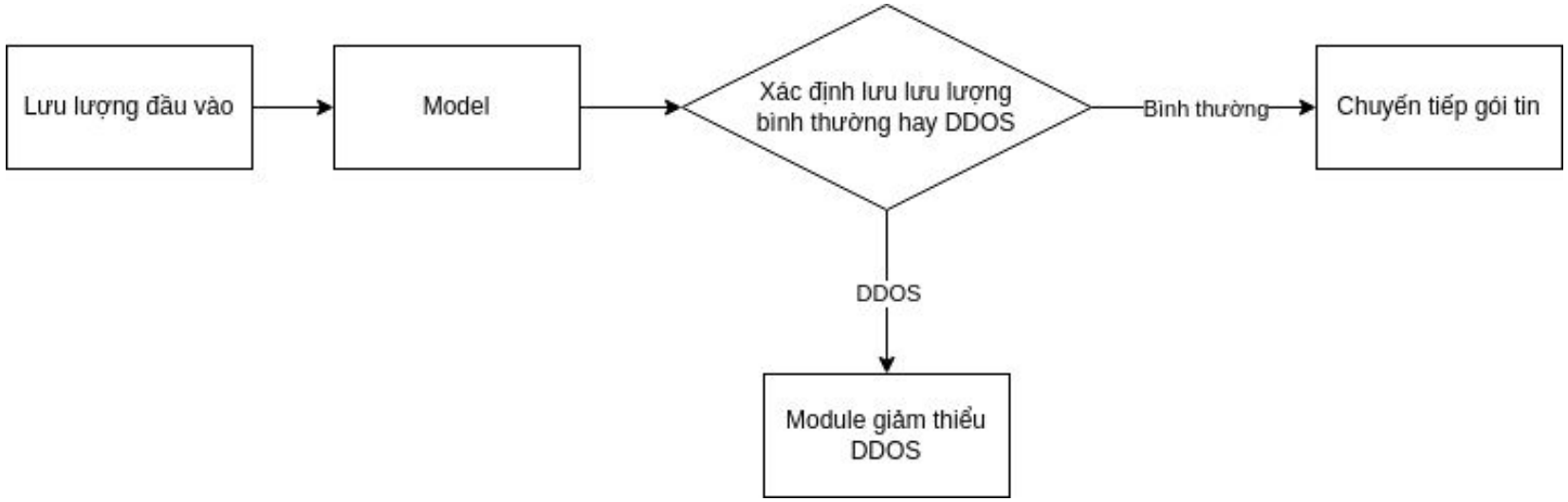


Cấu trúc mạng

THIẾT KẾ HỆ THỐNG



Sơ đồ quá trình thu thập data và đánh giá model



Sơ đồ quá trình phát hiện tấn công DDOS và giảm thiểu

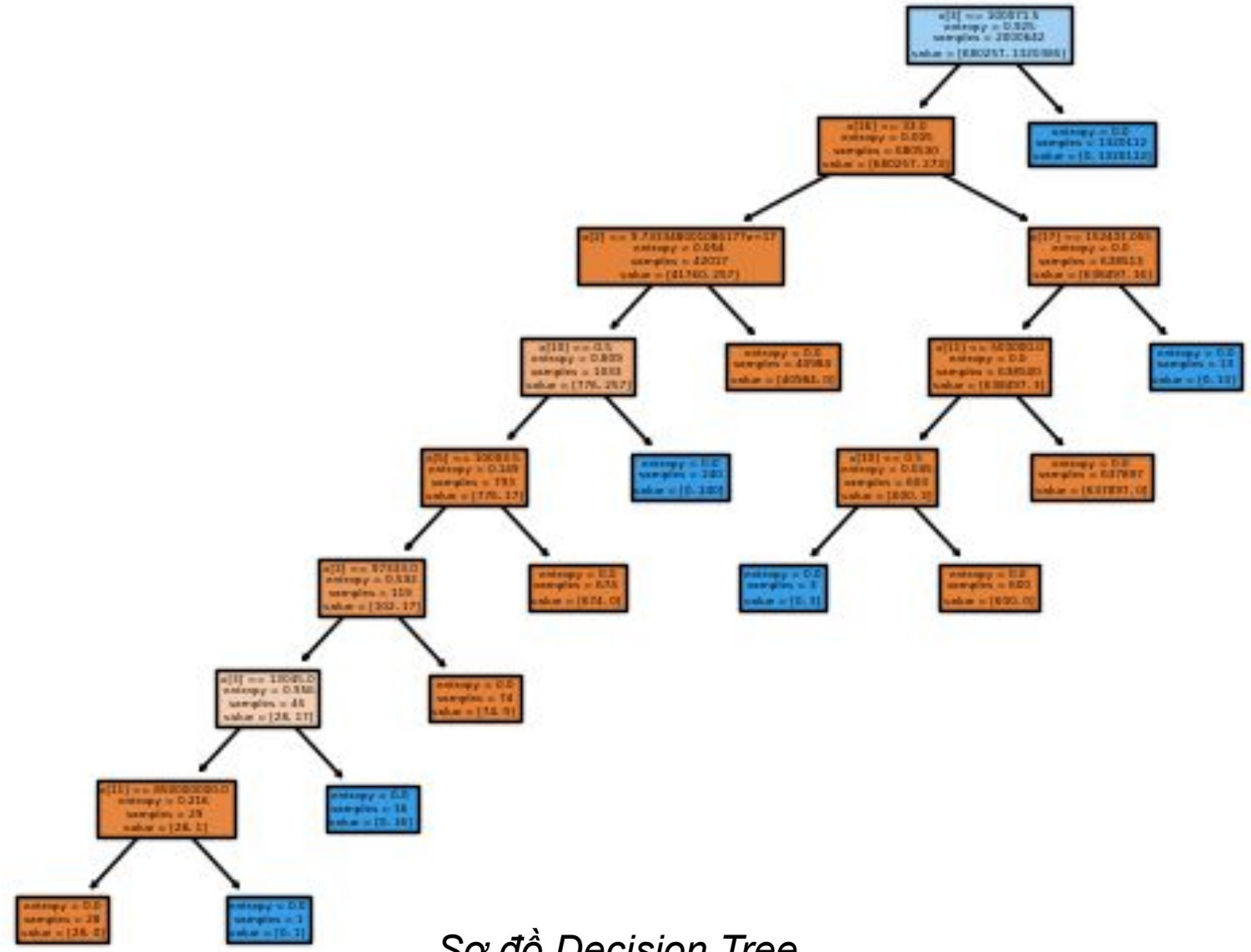
THIẾT KẾ HỆ THỐNG

DATASET	
Số lượng Feature	20 feature
Số Mẫu dữ liệu	2667523 mẫu
Các Feature được sử dụng:	flow_id, ip_src, tp_src, ip_dst, tp_dst, ip_proto, icmp_code, icmp_type, flow_duration_sec, flow_duration_nsec, idle_timeout, hard_timeout, flags, packet_count, byte_count, packet_count_per_second, packet_count_per_nsecond, byte_count_per_second, byte_count_per_nsecond, label

➔ **Dữ liệu trong trường hợp bình thường được gắn nhãn 1**

➔ **Dữ liệu trong trường hợp DDoS được gắn nhãn 0**

THIẾT KẾ HỆ THỐNG



Sơ đồ Decision Tree

THIẾT KẾ HỆ THỐNG

Node	Feature	Threshold	Value	Sample	Impurity	Children left	Children right
0	3	100071.5	[0.34, 0.66]	2000642	0.9248	1	22
1	16	33.0	[0.9996, 0.0004]	680530	0.0051	2	15
2	2	9.7333e+17	[0.9939, 0.0061]	42017	0.0538	3	14
3	10	0.5	[0.7512, 0.2488]	1033	0.8094	4	13
4	5	10003.5	[0.9786, 0.0214]	793	0.1494	5	12
5	3	97333.0	[0.8571, 0.1429]	119	0.5917	6	11
6	3	13045.0	[0.6222, 0.3778]	45	0.9565	7	10
7	11	850000000.0	[0.9655, 0.0345]	29	0.2164	8	9
15	17	152431.05	[0.9999, 0.00003]	638513	0.0004	16	21
16	11	500000.0	[0.9999, 0.00001]	638500	0.00009	17	20
17	10	0.5	[0.9950, 0.0050]	603	0.0452	18	19

Giá trị Entropy của các nút giảm khi tiến đến nút lá, cho thấy mô hình đã học được cách phân loại dữ liệu.

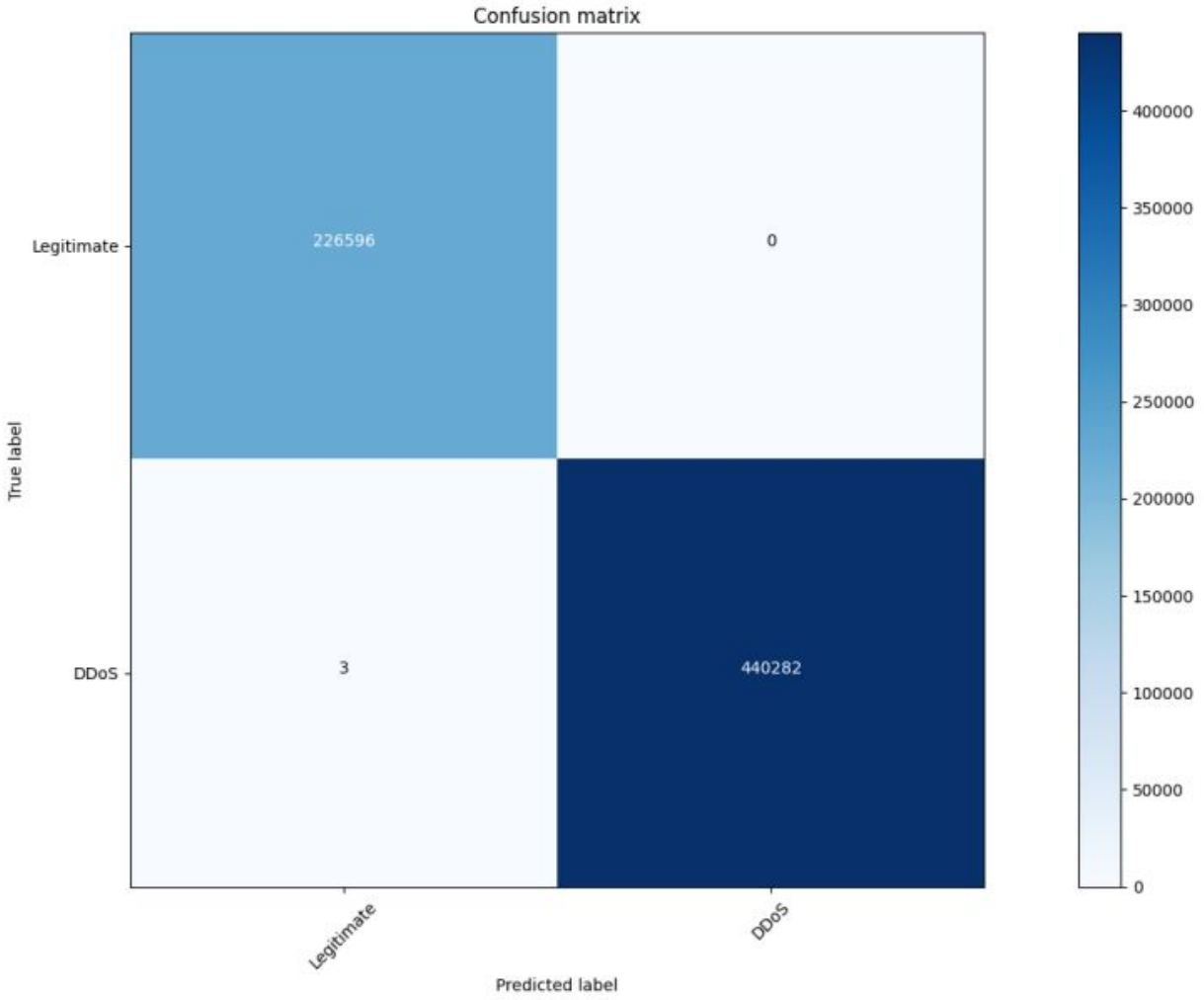
Đối với mỗi nút lá, giá trị Entropy gần như bằng 0, cho thấy rằng tại những điểm này, dữ liệu đã được phân loại một cách rất chính xác.

KẾT QUẢ

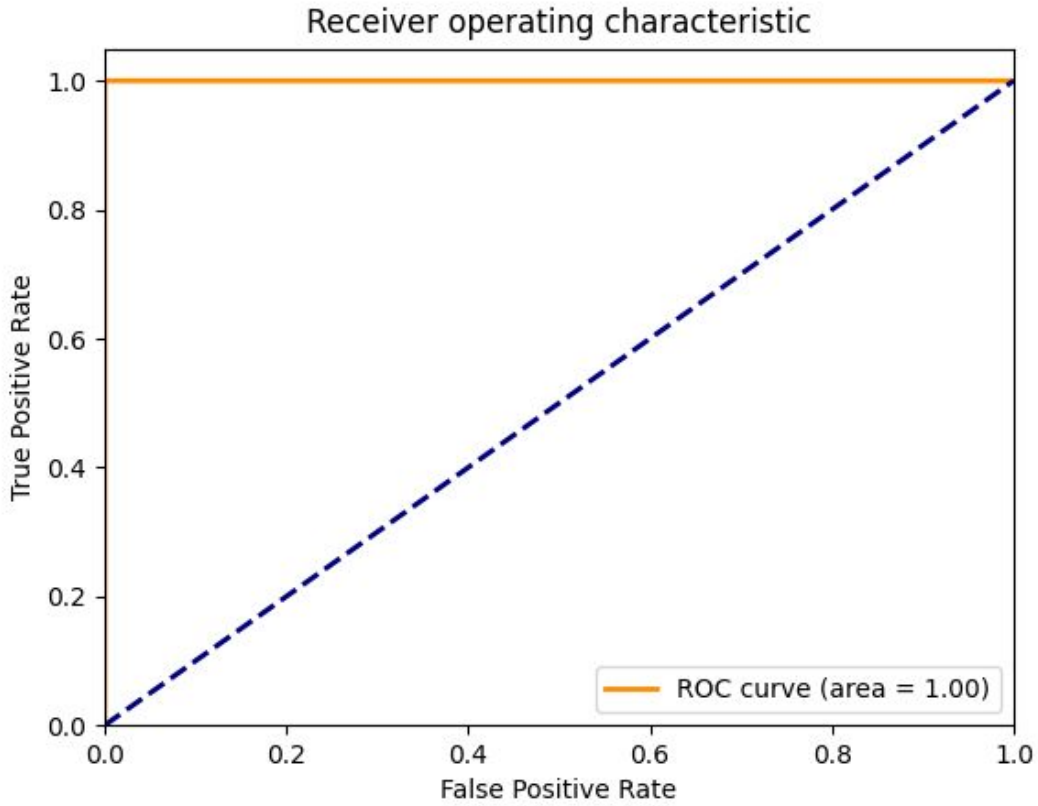
	Class 0 (DDoS)	Class 1 (Normal)	Tổng
Tập train	680257	1320385	2000642
Tập test	226596	440285	666881

Thông tin	Giá trị
Mô hình sử dụng	Decision Tree
Thời gian train	2 giây 31
Độ sâu của Decision Tree	8
Số nút lá	12
Accuracy Score	100%
Precision Score	100%
Recall Score	100%
F1 score	100%
AUC	100%

KẾT QUẢ



Confusion Matrix

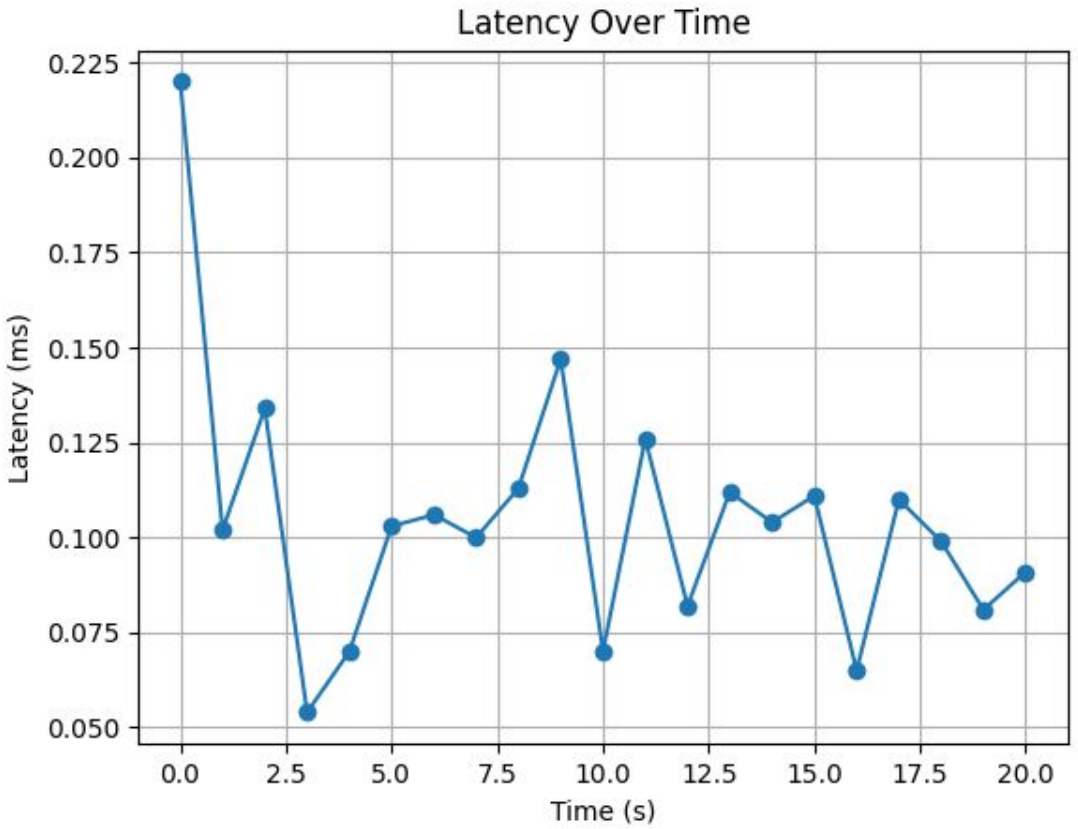


Biểu đồ ROC

KẾT QUẢ

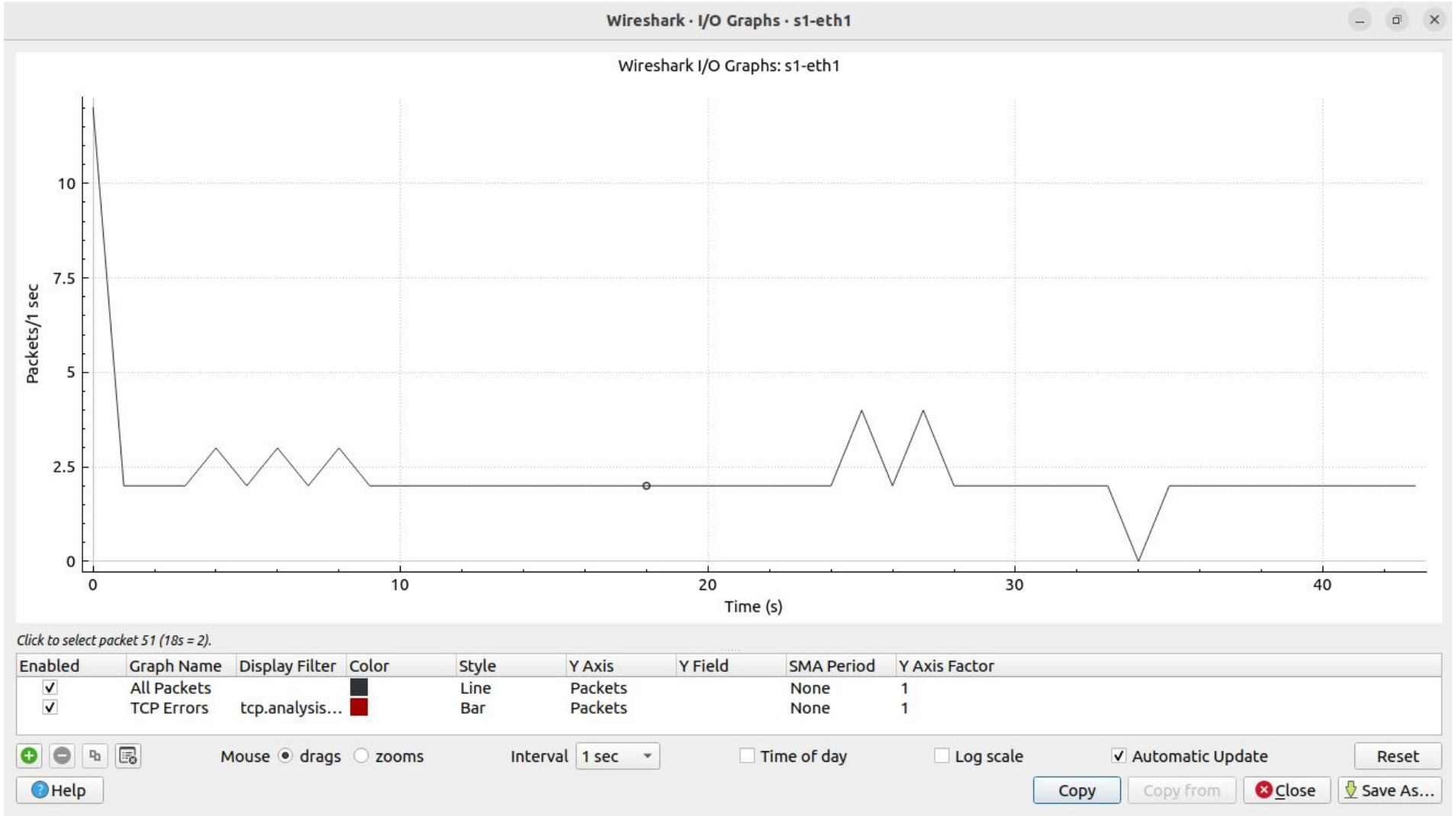
```
------------------------------------------------------------
Client connecting to 10.0.0.1, UDP port 5001
Sending 1470 byte datagrams, IPG target: 112.15 us (kalman adjust)
UDP buffer size:  208 KByte (default)
------------------------------------------------------------
[  1] local 10.0.0.2 port 37355 connected with 10.0.0.1 port 5001
[ ID] Interval       Transfer     Bandwidth
[  1] 0.0000-1.0000 sec  1.27 MBytes  10.7 Mbits/sec
[  1] 1.0000-2.0000 sec  1.13 MBytes  9.49 Mbits/sec
[  1] 2.0000-3.0000 sec  1.20 MBytes  10.0 Mbits/sec
[  1] 3.0000-4.0000 sec  1.13 MBytes  9.44 Mbits/sec
[  1] 4.0000-5.0000 sec  1.20 MBytes  10.0 Mbits/sec
[  1] 5.0000-6.0000 sec  1.13 MBytes  9.49 Mbits/sec
[  1] 6.0000-7.0000 sec  1.13 MBytes  9.49 Mbits/sec
[  1] 7.0000-8.0000 sec  1.19 MBytes  10.0 Mbits/sec
[  1] 8.0000-9.0000 sec  1.13 MBytes  9.49 Mbits/sec
[  1] 9.0000-10.0000 sec  1.20 MBytes  10.0 Mbits/sec
[  1] 0.0000-10.0420 sec  11.7 MBytes  9.78 Mbits/sec
[  1] Sent 8352 datagrams
[  1] Server Report:
[ ID] Interval       Transfer     Bandwidth        Jitter   Lost/Total Datagrams
[  1] 0.0000-10.0989 sec  11.7 MBytes  9.72 Mbits/sec   4.542 ms 0/8351 (0%)
[  1] 0.0000-10.0989 sec  1 datagrams received out-of-order
root@le-pham-cong:/home/lephamcong/Documents/SDN Final/mininet#
```

Kiểm tra băng thông của server trong mạng



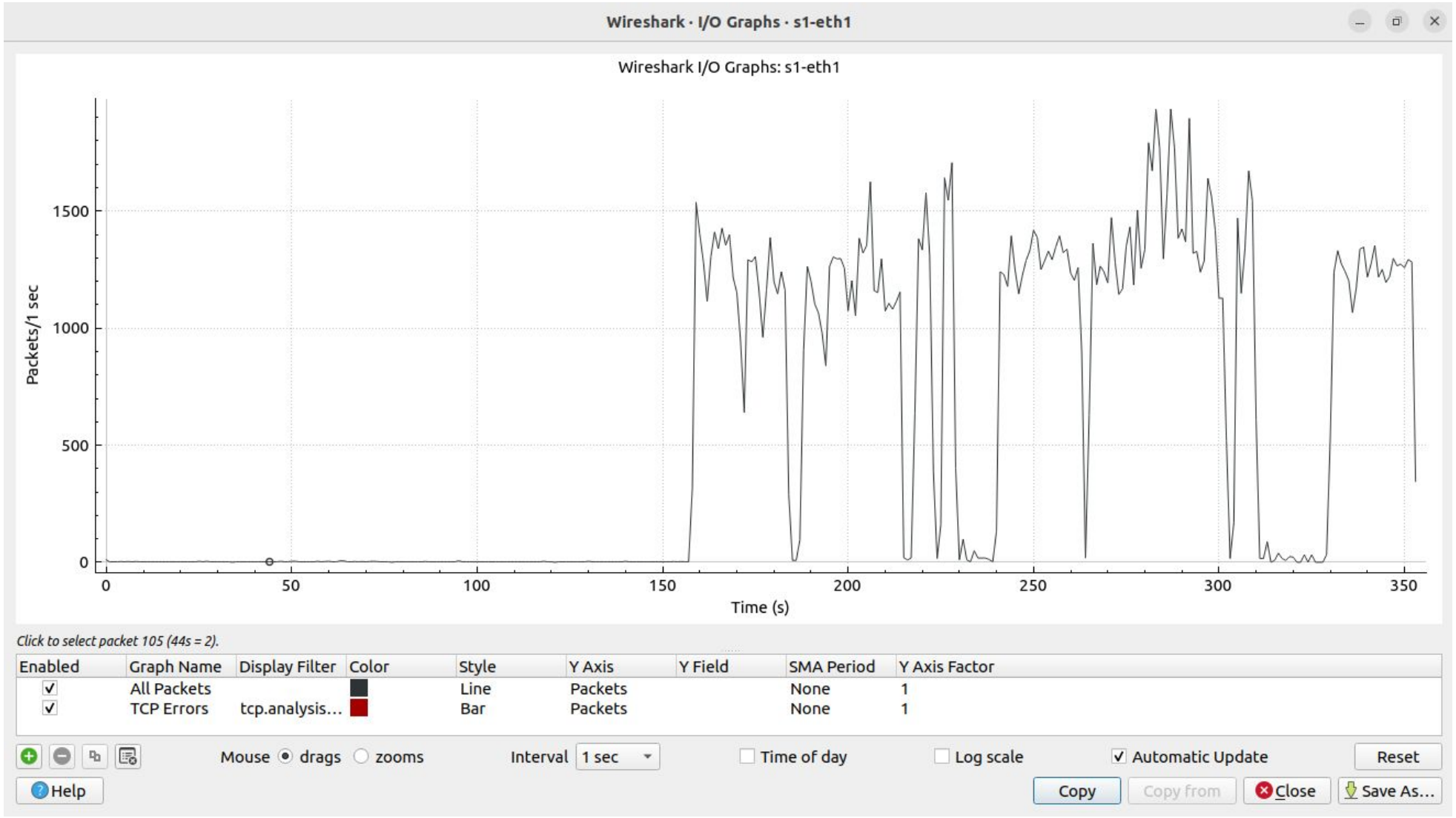
Kiểm tra độ trễ trong việc gửi và nhận gói đến server

KẾT QUẢ



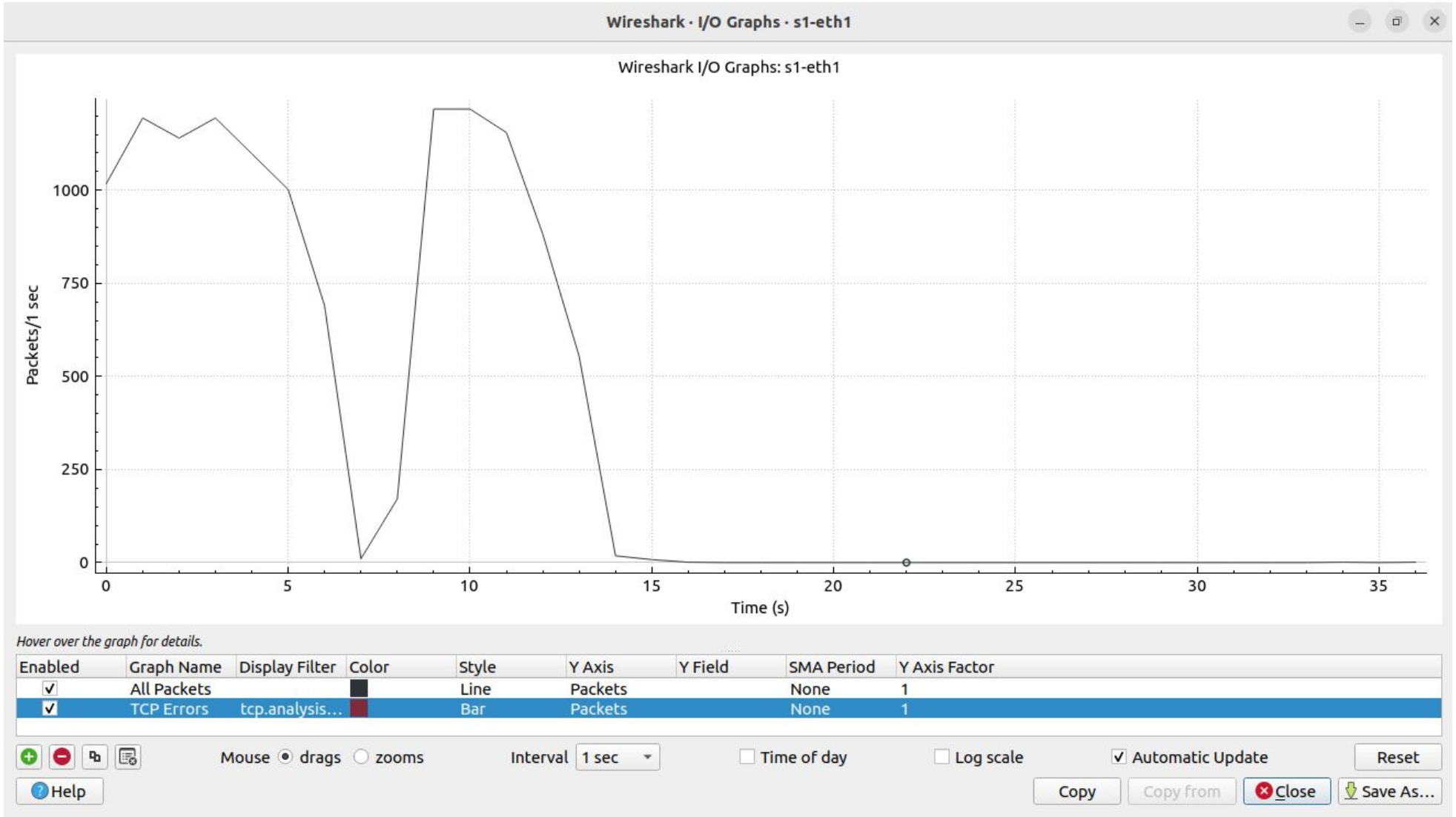
Tốc độ Packet gửi đến Server trong mạng trong trường hợp bình thường

KẾT QUẢ



Tốc độ Packet gửi đến Server trong mạng trong trường hợp DDoS

KẾT QUẢ



Tốc độ Packet gửi đến Server trong mạng khi kích hoạt module giảm thiểu sau khi phát hiện lưu lượng của một cuộc tấn công DDoS

ĐÁNH GIÁ

- Triển khai thành công mạng SDN trên nền tảng mininet, sử dụng OpenFlow v1.3, với controller là RYU.
- Giả lập thành công trường hợp tấn công DDoS, với các loại tấn công phổ biến là SYN, TCP, UDP.
- Đánh giá độ trễ: trong trường hợp normal, độ trễ đến máy chủ trong mạng khá thấp và ổn định, tỷ lệ packet bị mất rất thấp. Tuy nhiên, khi bị tấn công DDoS, server bị quá tải, dẫn đến không để truyền gửi các packet giữa client và server.
- Với mô hình Decision Tree, cho kết quả phân loại lưu lượng bình thường và tấn công có độ chính xác cao, việc mô hình hoạt động chính xác đã giúp cho việc phát hiện phát hiện DDoS đạt kết quả cao, module giảm thiểu dựa trên block port đã hoạt động tốt nhờ kết quả phát hiện chính xác.

KẾT LUẬN

Trong đề tài này đã đề xuất và triển khai giải pháp phát hiện và giảm thiểu tấn công DDoS trong mạng SDN bằng cách sử dụng mô hình machine learning dựa trên thuật toán Decision Tree.

Kết quả thử nghiệm cho thấy phương pháp đề xuất có khả năng phát hiện chính xác các trường hợp tấn công DDoS với tỷ lệ đúng cao, đồng thời giảm thiểu hiệu quả tác động của chúng đối với hệ thống mạng.

TÀI LIỆU THAM KHẢO

[1] Chirag Biradar. DDoS Attack Detection and Mitigation. https://github.com/chiragbiradar/DDoS-Attack-Detection-and-Mitigation. N/A. 34

XIN CẢM ƠN THẦY

VÀ CÁC BẠN ĐÃ LẮNG NGHE!