PHƯƠNG PHÁP KIỂM THỬ VÀ XÁC THỰC HIỆU QUẢ CHO THIẾT BỊ AN NINH MẠNG FPGA TÍCH HỢP ANTI - DDoS VÀ SPLUNK

EFFECTIVE PERFORMANCE EVALUATION AND VALIDATION OF FPGA-BASED ANTI - DDoS AND SPLUNK INTEGRATED NETWORK SECURITY DEVICE

Nguyễn Thị Khánh Hồng[1]*, Nguyễn Trọng Tuấn[2]

[1]Trường Đại học Sư phạm Kỹ thuật - Đại học Đà Nẵng, Việt Nam
[2]Công ty TNHH Giải pháp Acronics, Việt Nam

*Tác giả liên hệ / Corresponding author: ntkhong@ute.udn.vn

(Nhận bài / Received: 09/8/2025; Sửa bài / Revised: 18/9/2025; Chấp nhận đăng / Accepted: 19/9/2025)

DOI: 10.31130/ud-jst.2025.23(9A).458

Tóm tắt - Bài báo trình bày phương pháp đánh giá hiệu năng và xác thực toàn diện cho thiết bị an ninh mạng Anti - DDoS tích hợp Splunk trên nền tảng FPGA. Một testbed 10Gbps đã được xây dựng, bao gồm các máy chủ đa dịch vụ, người dùng hợp lệ và các máy tấn công sử dụng Hping3 để tạo ra các kịch bản tấn công DDoS lớp 3/4 (tấn công đơn vector và đa vector). Quá trình đánh giá tập trung vào chất lượng dịch vụ (Web, FTP, Media, Mail, DNS), độ trễ, tỷ lệ mất gói và mức sử dụng tài nguyên máy chủ. Splunk được tích hợp để giám sát và trực quan hóa chi tiết các hoạt động tấn công. Kết quả thực nghiệm cho thấy thiết bị xử lý hiệu quả các cuộc tấn công gần mức 10Gbps, loại bỏ phần lớn lưu lượng độc hại, đảm bảo dịch vụ hoạt động ổn định với độ trễ thấp (<0,3 ms), đồng thời CPU/Bộ nhớ chỉ dao động ở mức 9-11%. Những phát hiện này khẳng định tính hiệu quả và độ tin cậy của giải pháp dựa trên FPGA trong bảo vệ mạng thời gian thực.

Từ khóa - FPGA Add-on Splunk; Anti - DDoS lớp 3/4; Kiểm thử hiệu năng mạng; Chất lượng dịch vụ (QoS); Testbed 10Gbps

Abstract - This paper presents a testing and validation methodology for an Anti - DDoS and Splunk integrated network security device based on FPGA technology. A 10Gbps testbed was constructed, consisting of multi-service servers, legitimate users, and attacking machines employing Hping3 to generate various Layer 3/4 DDoS attack scenarios, ranging from single-vector to multi-vector, both internal and external. The evaluation process focused on service quality (Web, FTP, Media, Mail, DNS), latency, packet loss, and server resource utilization under attack conditions. Splunk was integrated to monitor and provide a detailed visualization of the attack activities. Experimental results demonstrate that, the device effectively mitigates DDoS attacks with traffic rates approaching 10Gbps, filters out the majority of malicious traffic, and maintains stable service performance with low latency (below 0.3 ms) while keeping CPU/Memory usage at only 9–11%. These findings confirm the efficiency and reliability of FPGA-based solutions for real-time network protection.

Key words - FPGA Add-on Splunk; Anti - DDoS Layer 3/4; Network Performance Testing and Evaluation; Quality of Service (QoS); Testbed 10Gbps

1. Đặt vấn đề

Trong bối cảnh chuyển đổi số, an ninh mạng đóng vai trò nền tảng, ảnh hưởng trực tiếp đến sự ổn định và tăng trưởng của tổ chức, doanh nghiệp. Một trong những mối đe dọa lớn nhất là tấn công từ chối dịch vụ phân tán (DDoS), vốn ngày càng phức tạp, có quy mô rộng và tần suất cao, gây tổn thất lớn về kinh tế và uy tín [1]. Cơ chế của các cuộc tấn công này là khai thác triệt để tài nguyên máy chủ như CPU, bộ nhớ và băng thông, khiến dịch vụ bị gián đoạn hoặc ngừng hoạt động hoàn toàn. Trên thế giới, nhiều sự cố an ninh mạng diện rộng đã nhằm vào các lĩnh vực trọng yếu như năng lượng, ngân hàng, giao thông và chính phủ, trong đó các mã độc như Stuxnet hay Industroyer là minh chứng điển hình cho tính chất nguy hiểm của "chiến tranh mạng".

Tại Việt Nam, năm 2024 ghi nhận khoảng 659.000 vụ tấn công mạng [2]. Riêng sáu tháng đầu năm, có tới 211.000 cảnh báo và 20 sự cố đặc biệt nghiêm trọng [3]. Hơn 14.000 thiết bị bị ảnh hưởng bởi biến thể ransomware, với tổng cộng 83.000 máy tính nhiễm mã độc. Đồng thời, hơn 201.903 bộ dữ liệu cá nhân bị rò rỉ, chứa tới 12,3 triệu bản ghi thông tin [4].

Trong giai đoạn 2020-2025, nhiều công trình nghiên cứu đã chú trọng đến việc ứng dụng phần cứng, đặc biệt là FPGA, để tăng tốc độ xử lý và giảm thiểu độ trễ trong phát hiện tấn công DDoS [5], [6]. Bên cạnh đó, Splunk, một nền tảng SIEM (Security Information and Event Management) phổ biến, được lựa chọn để tích hợp nhằm phân tích log, giám sát và trực quan hóa dữ liệu tấn công [7].

Các hệ thống SIEM hiện nay (SolarWinds Security Event Manager, Log360, Paessler Security, Splunk Enterprise Security, IBM Qradar, Datadog Security Monitoring, …) [8] – [11] đều hỗ trợ quản lý tập trung, phát hiện bất thường, liên kết và lưu trữ log, song thường yêu cầu bản quyền định kỳ cũng như hạ tầng máy chủ mạnh để xử lý lưu lượng dữ liệu lớn [12].

Trong khi nhiều nghiên cứu tập trung vào thuật toán hoặc mô phỏng, bài báo này đặc biệt chú trọng vào kiểm thử trong môi trường thực tế (Testbed 10Gbps) với các kịch bản tấn công đa dạng, từ đó cung cấp bằng chứng thực

[1] The University of Danang - University of Technology and Education, Vietnam (Hong Nguyen Thi Khanh)
[2] Acronics Solutions Company Limited, Vietnam (Tuan Nguyen Trong)

nghiệm mạnh mẽ về hiệu quả và độ tin cậy. Sự kết hợp giữa tốc độ xử lý của FPGA và khả năng giám sát của Splunk là một điểm khác biệt có thể được so sánh với các giải pháp chỉ dùng phần mềm hoặc phần cứng chuyên dụng nhưng thiếu tính năng SIEM tích hợp chi tiết.

2. Phương pháp thực nghiệm

2.1. Thiết bị và môi trường thử nghiệm

Thiết bị Anti - DDoS 10 Gbps trên công nghệ FPGA Add-on Splunk (gọi tắt là thiết bị Anti - DDoS) được phát triển nhằm ngăn chặn các cuộc tấn công DDoS ở lớp mạng (lớp 3) và lớp vận chuyển (lớp 4), đồng thời cung cấp khả năng giám sát, phân tích log và cảnh báo thời gian thực (Hình 1). Thiết bị có thể ngăn chặn các dạng tấn công phổ biến như SYN Flood, UDP Flood, ICMP Flood, LAND Attack, IPSec IKE Flood, TCP/UDP Fragmentation. Với khả năng xử lý luồng dữ liệu 10Gbps và quản lý 100.000 kết nối đồng thời, hệ thống đảm bảo độ chính xác thống kê và duy trì tính ổn định dịch vụ.

Hình 1. *Thiết bị Anti - DDoS*

Hệ thống phần cứng của thiết bị được triển khai trên kit ZCU102 do AMD Xilinx phát triển. Đây là nền tảng mạnh được sử dụng để phát triển các ứng dụng dựa trên dòng vi mạch Zynq UltraScale+ MPSoC. Bo mạch sử dụng chip ZU9EG MPSoC, tích hợp bộ xử lý ARM Cortex-A53 bốn nhân, bộ xử lý thời gian thực ARM Cortex-R5 hai nhân, GPU Mali-400 MP2 cùng các tài nguyên logic khả trình. Kiến trúc dị thể này cho phép xây dựng các hệ thống nhúng phức tạp, đáp ứng đồng thời yêu cầu về hiệu năng, tính thời gian thực và gia tốc phần cứng.

Bộ kit hỗ trợ nhiều tùy chọn kết nối như PCIe Gen3, USB 3.0, SATA, DisplayPort và Gigabit Ethernet, dễ dàng tích hợp với các thiết bị ngoại vi và mạng. Ngoài ra, các giao diện DDR4 tốc độ cao và hệ thống quản lý nguồn tích hợp giúp nâng cao hiệu năng và độ ổn định. Kit cũng hỗ trợ các đầu nối mở rộng FMC, cho phép phát triển và mở rộng I/O theo nhu cầu.

Với cấu hình và tính năng vượt trội, nhóm nghiên cứu đã lựa chọn ZCU102 để phát triển các IP Core chuyên biệt cho thiết bị Anti-DDoS. Các khối IP core đảm nhận các chức năng chính bao gồm: AXI Ethernet 10Gb cung cấp giao diện truyền nhận dữ liệu tốc độ cao; Header Parser và Detector: trích xuất thông tin gói tin, phân loại lưu lượng, phát hiện các kiểu tấn công; Decision và Packet Generator: đưa ra chính sách xử lý (cho qua, loại bỏ, tạo gói tin phản hồi) nhằm giảm thiểu tác động tấn công; Splunk Export Module: tối ưu hóa việc xuất dữ liệu log sang Splunk thông qua Ethernet, Các thông tin về thông lượng, kiểu tấn công và kết nối tấn công được xử lý tại Detector và Decision, sau đó được sử dụng để phân tích hành vi và đưa ra cảnh báo được hiển thị trực quan hóa và phân tích thời gian thực. Các IP Core được tối ưu hóa kiến trúc (pipeline, hashing, round-robin) giúp tăng thông lượng, giảm độ trễ và giảm tải cho CPU. Nhờ đó, giải pháp FPGA Add-on Splunk vừa đạt hiệu năng cao, đồng thời cho phép nâng cấp, cập nhật các phiên bản mới một cách nhanh chóng mà không cần thay thế thiết bị mới giúp vừa tiết kiệm chi phí phần cứng và bản quyền so với giải pháp SIEM truyền thống.

Môi trường testbed được triển khai tại Trung tâm Phát triển Hạ tầng Công nghệ Thông tin Đà Nẵng với băng thông 10Gbps. Hệ thống gồm: máy chủ đa dịch vụ (Web, FTP, Media, Mail, DNS, SMB, Chat); Người dùng hợp lệ truy cập dịch vụ theo thời gian thực; Máy tấn công sử dụng Hping3, PackEth, NetScan Tools để tạo ra các lưu lượng độc hại; Thiết bị mạng (Router, Switch, SFP/SFP+ 10Gb) đảm bảo khả năng truyền dẫn. Môi trường kiểm thử được thực hiện trong điều kiện đảm bảo an toàn và kiểm soát trong suốt quá trình thực nghiệm.

2.2. Kịch bản thử nghiệm

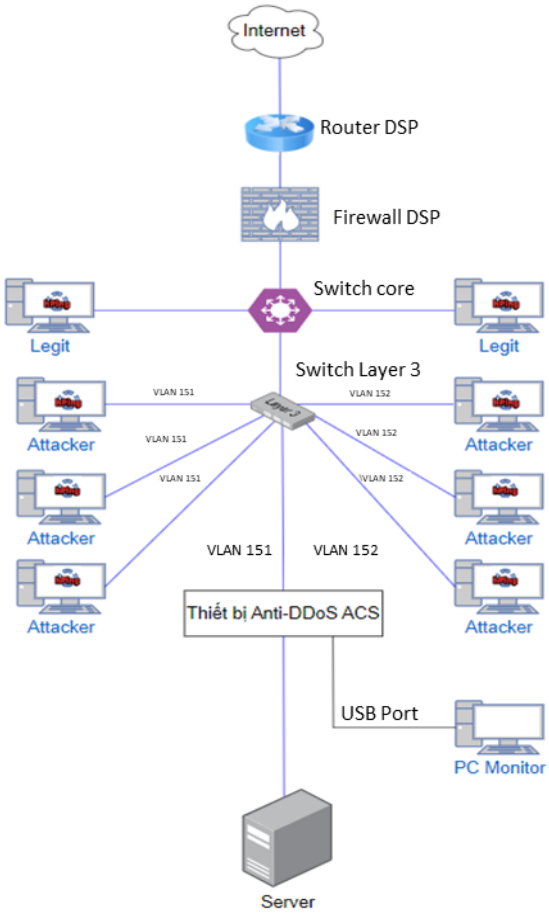
Các kịch bản kiểm thử được chia thành nhiều loại, bao gồm: (i) tấn công đơn lẻ (Single Vector): kiểm tra khả năng chống lại từng loại tấn công riêng biệt như SYN Flood, UDP Flood, ICMP Flood, LAND Attack, IPSec IKE Flood, TCP/UDP Fragmentation; (ii) tấn công đa vector (Multi-Vector): kết hợp nhiều kiểu tấn công đồng thời, ví dụ SYN Flood + LAND Attack; UDP Flood + ICMP Flood + DNS Amplification; (iii) xử lý VLAN: kiểm tra khả năng ngăn chặn gói tin tấn công chứa Single VLAN tag và Double VLAN tag. Đồng thời, quá trình thử nghiệm này thực hiện đánh giá hoạt động của môi trường trong mạng và ngoài mạng. Trong khuôn khổ bài báo này, nhóm nghiên cứu trình bày về quá trình thử nghiệm được thực hiện với mô hình tấn công bên trong mạng tại Trung tâm phát triển hạ tầng Công nghệ thông tin (IID Đà Nẵng) như mô tả ở Hình 2 gồm các thành phần sau:

- Nhóm máy người dùng hợp lệ (Legit): kết nối Internet và sử dụng các dịch vụ như kết nối Web Server, xem Youtube, xem Stream video từ Media Server, Share File FTP, Ping đến máy Server.

- Máy Server chạy các dịch vụ Web Server, Media Server, FTP Server, SMB Server, SMTP Server, Ping đến các máy End User.

- 6 máy tấn công (Attacker) sử dụng tools Hping3 tấn công UDP flood đến máy Server.

Sử dụng phần mềm PRTG để giám sát lưu lượng trên các Port của máy Server và giám sát lưu lượng trên các Port của Switch.



Hình 2. *Mô hình đánh giá chức năng chống tấn công nằm trong mạng của thiết bị Anti - DDoS 10Gb*

Các loại tấn công được sử dụng nhằm đánh giá khả năng phát hiện, ngăn chặn và duy trì chất lượng dịch vụ của thiết bị Anti - DDoS và bao gồm:

Các kịch bản được triển khai theo 3 chế độ vận hành:

- **Kịch bản 1** (No protection): hệ thống hoạt động không có thiết bị Anti - DDoS bảo vệ để ghi nhận mức thiệt hại.

- **Kịch bản 2** (Single vector): đánh giá thiết bị Anti - DDoS khi đối phó với từng loại tấn công đơn lẻ.

- **Kịch bản 3** (Multi-vector): kiểm tra khả năng chống chịu trong điều kiện bị tấn công phối hợp.

Trong từng kịch bản, người dùng hợp lệ vẫn duy trì các hoạt động thường nhật như duyệt web, xem video, chia sẻ file, gửi email nhằm phản ánh môi trường thực tế.

2.3. Tiêu chí đánh giá và các chỉ số

Quá trình kiểm thử thiết bị Anti - DDoS theo các kịch bản được nêu ở mục 2.2 tập trung vào các tiêu chí đánh giá và các chỉ số về hiệu suất và chất lượng dịch vụ như sau:

- Chất lượng dịch vụ (QoS) và tính toàn vẹn dữ liệu: Kiểm tra khả năng truy cập và sử dụng các dịch vụ (Web Server, Media Stream, ShareFile, Mail Server, Chat Server, DNS Server) cho người dùng hợp lệ trong cả điều kiện có và không có tấn công DDoS. Phân tích các thông số QoS như số lượng gói tin bị mất (Lossed Packet), sai thứ tự (Out-of-Order Packet), hỏng (Corrupt Packet), lặp lại (Duplication Packet), và độ trễ (Latency).

- Đo lường tổng thông lượng xử lý của thiết bị (khoảng 10Gbps), thông lượng tấn công và thông lượng của luồng hợp lệ và đảm bảo duy trì 100.000 kết nối.

- Tài nguyên máy Server: Giám sát việc sử dụng tài nguyên CPU và Bộ nhớ của máy Server trong suốt quá trình kiểm thử.

- Tích hợp Splunk: Kiểm tra khả năng thu thập, lập chỉ mục (Indexing), và hiển thị dữ liệu log từ thiết bị Anti - DDoS lên các Dashboard của Splunk.

Các chỉ số này phản ánh không chỉ hiệu năng ngăn chặn tấn công của thiết bị Anti-DDoS mà còn thể hiện khả năng duy trì dịch vụ ổn định cho người dùng hợp lệ.

3. Đánh giá kết quả

Khi thực hiện việc đánh giá chức năng chống tấn công trong mạng của thiết bị Anti - DDoS theo sơ đồ bố trí các thiết bị như ở Hình 2. Việc tấn công theo kịch bản được thực hiện với việc sử dụng 2 máy người dùng hợp lệ, 6 máy tấn công và máy Server sử dụng các dịch vụ như được mô tả chi tiết trong mục 2.2.

Đầu tiên, nhóm nghiên cứu thực hiện kịch bản không có thiết bị Anti - DDoS bảo vệ (No protection) cho hệ thống: ban đầu tài nguyên băng thông ở phía nhận (Receiver) tại port 10Gb trên máy Server đạt thông lượng 10Gbps, độ trễ khi thực hiện ping từ máy tính người dùng đến máy Server ở mức cao (khoảng 5ms) nhưng khi bị tấn công SYN Flood với thông lượng tấn công đến máy Server khoảng 6.5Gbps và độ trễ khi ping (từ người dùng đến máy Server) tăng lên ~10 ms. Dịch vụ xem video xuất hiện tình trạng gián đoạn, một số người dùng không thể truy cập các dịch vụ khác, CPU và bộ nhớ máy chủ rơi vào tình trạng quá tải. Điều này chứng minh tác động nghiêm trọng của tấn công DDoS đến chất lượng dịch vụ và tính sẵn sàng hệ thống.

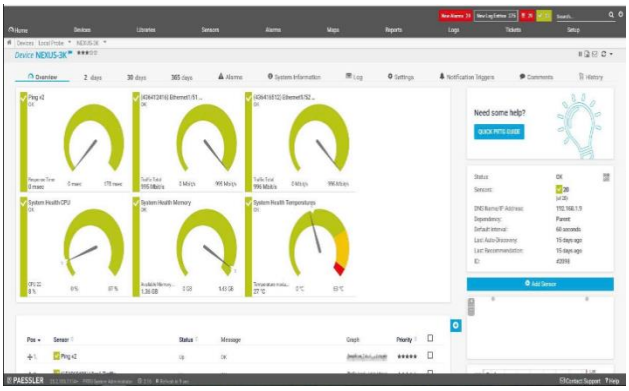
Tiếp đến, thực hiện triển khai thiết bị Anti - DDoS theo kịch bản 2 (tấn công đơn lẻ - Single Vector là thực hiện kiểm tra khả năng chống lại DDoS của từng loại tấn công riêng biệt như SYN Flood, UDP Flood, ICMP Flood, LAND Attack, IPSec IKE Flood, TCP/UDP Fragmentation). Kết quả cho thấy thiết bị Anti - DDoS đã ngăn chặn thành công nhiều dạng tấn công lớp 3/4 như SYN Flood, UDP Flood, ICMP Flood, LAND Attack, IPSec IKE Flood, cũng như các cuộc tấn công phân mảnh TCP/UDP với số liệu trung bình như sau: thông lượng tấn công đến máy Server trong khoảng (6,9 Gbps đến 9,8 Gbps); độ trễ khi thực hiện ping (từ máy tính người dùng đến máy Server) có độ trễ dưới 0,3ms. Chất lượng dịch vụ xem video được phát từ máy Server vẫn đảm bảo bình thường và tài nguyên CPU và bộ nhớ được sử dụng lần lượt là 9% và 11%

Đối với kịch bản 3: tấn công đa vector (Multi-Vector) là kết hợp nhiều kiểu tấn công đồng thời, ví dụ SYN Flood + LAND Attack; UDP Flood + ICMP Flood + DNS Amplification, thông lượng tấn công đến máy Server đạt khoảng (8,3 Gbps – 9,5 Gbps), độ trễ khi thực hiện ping (từ máy tính người dùng đến máy Server cũng ở mức dưới 0,3ms). Quá trình xem video được phát từ máy Server diễn

ra bình thường và tài nguyên CPU và bộ nhớ được sử dụng ở mức thấp lần lượt là 9% và 11%.

Dưới áp lực tấn công như ở kịch bản 2 và 3, thông lượng gần 10 Gbps, các dịch vụ Web, FTP, Mail, DNS, Media vẫn hoạt động ổn định; độ trễ trung bình duy trì dưới 0,3 ms. Mức sử dụng tài nguyên CPU và bộ nhớ trên máy chủ chỉ ở khoảng 9–11%, cho thấy khả năng xử lý hiệu quả và ít gây quá tải hệ thống.

Đặc biệt, thiết bị Anti - DDoS quản lý đồng thời 100.000 kết nối trong suốt quá trình thử nghiệm mà không ảnh hưởngđến QoS. Việc tích hợp Splunk cho phép hiển thị trực quan thông tin chi tiết về luồng tấn công (địa chỉ nguồn/đích, kiểu tấn công, thông lượng, mức tiêu thụ tài nguyên…), hỗ trợ quản trị viên giám sát và phản ứng nhanh như trong Hình 3.



Hình 3. *Màn hình giám sát Splunk – SIEM*

Bảng 1 cho thấy, khi không có biện pháp bảo vệ, hệ thống dễ bị tê liệt cả về dịch vụ lẫn tài nguyên; khi thiết bị Anti - DDoS được kích hoạt, thông lượng duy trì gần mức tối đa 10 Gbps, độ trễ giảm mạnh, gói tin mất dưới 1%, trong khi CPU/Bộ nhớ của máy chủ vẫn ổn định. Thiết bị Anti – DDoS chứng minh khả năng chống chịu trước cả tấn công đơn vector và đa vector, đồng thời bảo toàn dịch vụ cho người dùng hợp lệ. Như vậy, các kết quả kiểm thử khẳng định tính hiệu quả, ổn định và độ tin cậy của giải pháp Anti-DDoS trên nền tảng FPGA Add-on Splunk trong điều kiện thử nghiệm băng thông cao và kịch bản tấn công đa dạng.

Bảng 1. *Các chỉ số hiệu năng trong những kịch bản thử nghiệm khác nhau*

Kịch bản thử nghiệm	Thời gian kiểm tra (Phút)	Thông lượng (Gbps)	Độ trễ (ms)	Mất gói tin (%)	Tài nguyên CPU/ Bộ nhớ (%)
Kịch bản 1	120	6,5-10	5-10	3-5%	Quá tải
Kịch bản 2	120	≈9,8	<0,3	<1%	9 / 11
Kịch bản 3	120	≈9,5	<0,3	<1%	9 / 11

4. Bàn luận

Kết quả thực nghiệm cho thấy, thiết bị Anti-DDoS trên nền tảng FPGA có khả năng ngăn chặn hiệu quả các cuộc tấn công lớp 3/4 với lưu lượng gần 10 Gbps. Hệ thống duy trì hoạt động ổn định của các dịch vụ mạng quan trọng (Web, FTP, Mail, DNS, Media), độ trễ trung bình thấp (<0,3 ms), CPU/Bộ nhớ chỉ ở mức 9/11%. Đây là minh chứng rõ ràng cho tính khả thi của giải pháp trong điều kiện băng thông cao.

Bên cạnh đó, từ dữ liệu của Bảng 1 cho thấy trong kịch bản không bảo vệ, thông lượng dao động 6,5–10 Gbps và độ trễ 5–10 ms, cho thấy độ biến thiên lớn. Độ lệch chuẩn (SD) của thông lượng và độ trễ có thể ước lượng ở mức 1,0–1,5 (Gbps hoặc ms), phản ánh sự bất ổn cao. Khoảng tin cậy 95% (KTC) thì trung bình độ trễ nằm trong khoảng (6,5–8,5) ms, điều này xác nhận hệ thống dễ bị suy giảm chất lượng dịch vụ.

Ngược lại, ở hai kịch bản còn lại khi được bảo vệ bởi thiết bị Anti - DDoS, các chỉ số thể hiện như sau: thông lượng ổn định quanh 9,5–9,8 Gbps, độ trễ <0,3 ms với SD nhỏ (≈0,05 ms). Với kỳ vọng KTC 95% cho độ trễ trong khoảng (0,25–0,3) ms, chứng minh khả năng duy trì hiệu năng ổn định. Tỷ lệ mất gói dưới 1% và CPU/Bộ nhớ duy trì ở mức 9/11% cũng có độ lệch chuẩn thấp, phản ánh tính tin cậy của thiết bị.

Việc phân tích độ lệch chuẩn và khoảng tin cậy cho thấy hệ thống không bảo vệ có độ biến thiên cao, dẫn đến chất lượng dịch vụ kém ổn định. Trong khi đó, khi triển khai thiết bị Anti - DDoS, các chỉ số đều nằm trong KTC hẹp với SD thấp, chứng minh giải pháp giúp giảm biến động, duy trì dịch vụ ổn định và tăng cường độ tin cậy trong môi trường tấn công mạng.

Việc tích hợp Splunk mang lại lợi thế nổi bật: trực quan hóa dữ liệu tấn công chi tiết (địa chỉ nguồn/đích, kiểu tấn công, thông lượng, mức sử dụng tài nguyên), hỗ trợ quản trị viên phân tích, giám sát và phản ứng nhanh. Khả năng này giúp thiết bị Anti - DDoS vượt trội so với các giải pháp phần cứng Anti - DDoS thuần túy vốn thiếu công cụ SIEM tích hợp.

So sánh với các công trình liên quan: Nagy và cộng sự [5] đạt tốc độ phát hiện Top-9 tấn công DDoS trong vài mili-giây ở mức 100 Gbps; Kuka và cộng sự [6] giảm thiểu phản xạ khuếch đại ở tốc độ gần 100 Gbps; Farooq và cộng sự [13] dùng học máy cho hệ thống NIDS đạt độ chính xác > 99% và tốc độ >1000 Mpps. So với các nghiên cứu này, thiết bị Anti - DDoS của chúng tôi có thông lượng thấp hơn, nhưng nổi bật ở khả năng bảo toàn QoS và tích hợp Splunk-SIEM nhằm cung cấp góc nhìn toàn diện hơn cho quản trị hệ thống.

Tuy nhiên, nghiên cứu vẫn còn một số hạn chế. Thứ nhất, các kịch bản chủ yếu tập trung vào tấn công lớp 3/4, chưa đánh giá ở lớp 6 (lớp trình diễn) và lớp 7 (lớp ứng dụng). Việc mở rộng chức năng Anti-DDoS ở các lớp 6 và 7 sẽ giúp thiết bị Anti - DDoS xử lý các kiểu tấn công phức tạp hơn như HTTPs Attacks, Slowloris Attacks... Thứ hai, thử nghiệm được triển khai trong môi trường testbed có kiểm soát, chưa phản ánh đầy đủ tính phức tạp của hạ tầng Internet thực tế. Trong tương lai, nhóm nghiên cứu cần mở rộng thử nghiệm trên mạng diện rộng, tích hợp cơ chế logging tốc độ cao qua Ethernet, đồng thời nghiên cứu ứng dụng học máy để nhận diện sớm các mẫu tấn công mới.

5. Kết luận

Kết quả cho thấy, giải pháp chống tấn công DDoS tại lớp 3 và 4 của thiết bị Anti - DDoS có tích hợp công nghệ FPGA Add-on Splunk là hướng đi khả thi, hiệu quả và có tiềm năng ứng dụng thực tiễn, đặc biệt cho các hệ thống mạng của trung tâm xử lý dữ liệu có thông lượng lớn, số

lượng kết nối đồng thời từ 100000 kết nối trở lên và đòi hỏi quá trình giám sát mạng theo thời gian thực với chi phí đầu tư tối ưu. Mặt khác, việc lựa chọn Splunk làm nền tảng tích hợp giúp thiết bị Anti - DDoS không chỉ đạt hiệu năng cao mà còn gia tăng giá trị ứng dụng nhờ khả năng phân tích log, trực quan hóa dữ liệu và hỗ trợ quản trị an ninh mạng.

Lời cám ơn: Xin trân trọng cảm ơn Ủy ban nhân dân thành phố Đà Nẵng đã hỗ trợ kinh phí và Sở Khoa học và Công nghệ thành phố Đà Nẵng đã tạo điều kiện thuận lợi cho nhóm thực hiện nghiên cứu này trong khuôn khổ đề tài "Nghiên cứu và phát triển thiết bị giám sát an ninh, an toàn mạng có chức năng Anti-DDoS tại thành phố Đà Nẵng trên công nghệ FPGA Add-on Splunk".

TÀI LIỆU THAM KHẢO

[1] Cloudflare Inc., "*DDoS attack trends report 2023*", Cloudflare Radar, Austin, USA, Aug. 2023.

[2] Vietnamnet.vn, "Nearly half of Vietnamese organizations targeted by cyberattacks in 2024", *Vietnamnet.vn*, N/A. [Online]. Available: https://vietnamnet.vn/en/nearly-half-of-vietnamese-organizations-targeted-by-cyberattacks-in-2024-2355621.html [Accessed June 03, 2025].

[3] HPT, "The Cybersecurity Department warns Vietnamese businesses to urgently strengthen cybersecurity measures", *HPT.vn*, N/A. [Online]. Available: https://www.hpt.vn/en/news/the-cybersecurity-department-warns-vietnamese-businesses-to-urgently-strengthen-cybersecurity-measures/12632 [Accessed June 05, 2025].

[4] English.mst.gov.vn, "Information security in digital transformation", *english.mst.gov.vn,* N/A. [Online]. Available: https://english.mst.gov.vn/information-security-in-digital-transformation-197241002150001524.htm [Accessed June 05, 2025].

[5] B. Nagy, P. Orosz, T. Tóthfalusi, L. Kovács, and P. Varga, "Detecting DDoS attacks within milliseconds by using FPGA-based hardware acceleration", NOMS 2018-2018 *IEEE/IFIP Network Operations and Management Symposium*, Taipei, Taiwan, 2018, tr. 1-4, doi: 10.1109/NOMS.2018.8406299..

[6] M. Kuka, K. Vojanec, J. Kučera, and P. Benáček, "Accelerated DDoS Attacks Mitigation using Programmable Data Plane", 2019 *ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS)*, Cambridge, UK, 2019, pp. 1-3, doi: 10.1109/ANCS.2019.8901882.

[7] Splunk Inc., "*Enhancing security monitoring with Splunk",* Splunk LLC, California, USA, White Paper, 2022.

[8] INSTAGALLERYAPP "The 9 Best SIEM Tools: A Guide to Security Information and Event Management", *instagalleryapp.com*, [Online]. Available: https://instagalleryapp.com/qun-tr-mng-2/9-cong-c-siem-tt-nht-hng-dn-v-thong-tin-bo-mt-va/ [Access June 20, 2025].

[9] Intel, "*High-performance data analytics with splunk on intel hardware*", Intel, N/A, N/A, Reference Architecture Brief, 2020.

[10] Splunk>partner+, "Splunk and Cisco- Operational Intelligence Across Your Cisco Environment and Beyond", Splunk website, 2024. [Online]. Available: https://www.splunk.com/en_us/form/splunk-and-cisco-operational-intelligence.html [Access June 20, 2025].

[11] IBM Cloud Pak for Security, "Configuring a Splunk data source connection", *ibm.com/docs,* N/A. [Online]. Available: https://www.ibm.com/docs/en/cloud-paks/cp-security/1.7?topic=connectors-configuring-splunk-data-source-connection [Access June 20, 2025].

[12] Jon Papp, "Understanding Splunk Pricing & Choosing the Right Splunk License", *sp6.io/blog,* N/A. [Online]. Available: https://www.sp6.io/blog/choosing-the-right-splunk-license [Access June 20, 2025].

[13] M. A. Farooq, A. Rafique, S. A. Fahmy, and A. Arora, "High Throughput Low Latency Network Intrusion Detection on FPGAs: A Raw Packet Approach", *2025 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW)*, Milano, Italy, 2025, pp. p.183, https://dl.acm.org/doi/10.1145/3706628.3708844.