ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

KIỀU MINH VIỆT

CHỐNG TẤN CÔNG TỪ CHỐI DỊCH VỤ TỐC ĐỘ THẤP VÀO GIAO THỨC TCP BẰNG CÁC CẢI TIẾN CƠ CHẾ QUẢN LÝ HÀNG ĐỢI TÍCH CỰC

Chuyên ngành: Mạng máy tính và truyền thông số liệu
Mã số: 9480102.01

TÓM TẮT LUẬN ÁN TIẾN SĨ
MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG DỮ LIỆU

HÀ NỘI – 2022

Công trình được hoàn thành tại:

Trường Đại học Công nghệ - Đại học Quốc gia Hà Nội

Tập thể hướng dẫn khoa học:

1. GS. TS. Nguyễn Thanh Thủy

2. TS. Nguyễn Đại Thọ

Phản biện 1: .....

.....

Phản biện 2: .....

.....

Phản biện 3: .....

.....

Luận án sẽ được bảo vệ trước Hội đồng cấp Đại học Quốc gia chấm luận án tiến sĩ họp tại Đại học Công nghệ - Đại học Quốc gia Hà Nội vào hồi ..... giờ, ngày ..... tháng ..... năm .....

Có thể tìm thấy luận án tại:

1. Thư viện Quốc gia Việt Nam.
2. Trung tâm Thông tin - Thư viện, Đại học Quốc gia Hà Nội.

Mở đầu

1 Bối cảnh nghiên cứu và lý do chọn đề tài

Tấn công từ chối dịch vụ phân tán tốc độ thấp vào giao thức TCP (*TCP-targeted low-rate distributed denial-of-service attack – LDDoS*) là một loại tấn công từ chối dịch vụ phân tán mới, được giới thiệu lần đầu tiên bởi A. Kuzmanovic và E. Knightly vào năm 2003. So với các tấn công DDoS truyền thống, tấn công LDDoS khó bị phát hiện hơn do tốc độ gửi gói tin tấn công trung bình của nó tương đối thấp do hành vi gửi gói tin tấn công theo từng đợt cách đều nhau, mỗi đợt với một tốc độ cao nhưng diễn ra trong một khoảng thời gian ngắn. Mặc dù vậy, các tấn công này vẫn có thể bóp nghẹt thông lượng của các kết nối TCP bởi vì các kết nối này liên tục rơi vào trạng thái chờ phát lại gói tin (timeout) do ảnh hưởng gây ra bởi các đợt bùng nổ gói tin định kỳ của cuộc tấn công.

Các cơ chế hiện có để phát hiện và chống tấn công DDoS truyền thống thường dựa trên đo lường thống kê có thể không áp dụng được đối với các tấn công LDDoS, biến chúng trở thành thách thức mới trong mạng Internet hiện nay. Nó cho thấy sự cần thiết của việc nghiên cứu các giải pháp, cơ chế để chống lại loại hình tấn công mới này. Bên cạnh đó, việc lựa chọn đề tài nghiên cứu cải tiến cơ chế quản lý hàng đợi tích cực nhằm hỗ trợ router chống các tấn công LDDoS là một việc làm hợp lý bởi vì ngày càng nhiều ý kiến cho rằng các thiết bị router thay vì duy nhất chỉ thực hiện một nhiệm vụ là trung chuyển gói tin từ nguồn đến đích thì cần phải tham gia nhiều hơn vào việc phát hiện và điều chỉnh các nguồn dữ liệu gửi quá nhiều gói tin vào mạng hơn mức chia sẻ công bằng hoặc thậm chí với một mục đích xấu là gây ra hiện tượng từ chối dịch vụ cho các nguồn dữ liệu bình thường đang tham gia truyền dữ liệu qua mạng.

2 Các vấn đề còn tồn tại

Có rất nhiều cơ chế và giải pháp đã được đề xuất để chống tấn công LDDoS và một số mô hình phân tích để ước lượng thông lượng TCP trong điều kiện có tấn công xảy ra. Hiệu quả của một số cơ chế và giải pháp chống tấn công LDDoS chưa được làm rõ và tăng cường. Bên cạnh đó, các mô hình phân tích với mục đích chính là đánh giá hiệu quả tấn công dưới dạng thông lượng TCP dựa trên các tham số đã biết của cuộc tấn công và của môi trường mạng, tuy nhiên các mô hình này lại chưa đáp ứng được yêu cầu về tính chính xác hoặc nếu có thì lại gặp phải nhược điểm không xem xét tất cả các trường hợp có thể xảy ra, chẳng hạn như mô hình của Luo chưa xem xét các trường hợp mà kích thước cửa sổ tắc nghẽn của các kết nối TCP bị giảm một nửa một hoặc nhiều lần trước khi timeout.

3 Mục tiêu nghiên cứu

Xuất phát từ các vấn đề còn tồn tại nêu trên, luận án này hướng đến hai mục tiêu chính:

1. Đề xuất và xây dựng một phương pháp mới để ước lượng thông lượng TCP khi có tấn công xảy ra. Phương pháp mới phải đạt được độ chính xác cao và khắc phục được nhược điểm của các mô hình đã có.

2. Nghiên cứu nâng cao hiệu quả chống tấn công LDDoS của một cơ chế hỗ trợ router cụ thể gọi là tiếp cận dựa trên độ đo CPR (*Congestion Participation Rate*).

4 Đối tượng, phạm vi và phương pháp nghiên cứu

a) Đối tượng nghiên cứu

Đối tượng nghiên cứu của luận án là: (1) hành vi và thông lượng của các kết nối TCP trong điều kiện có tấn công LDDoS xảy ra (2) các thuật toán quản lý hàng đợi tích cực tại router, trong đó tập trung chủ yếu vào tiếp cận dựa trên độ đo CPR để chống tấn công LDDoS.

b) Phạm vi nghiên cứu

Nghiên cứu được thực hiện hoàn toàn trong môi trường mô phỏng sử dụng phần mềm mô phỏng mạng *NS-2*. Luận án chưa thực hiện nghiên cứu trong môi trường mạng thực Internet.

c) Phương pháp nghiên cứu

Phương pháp nghiên cứu được sử dụng trong luận án là mô hình hóa và thử nghiệm đánh giá kết quả. Đầu tiên, luận án mô hình hóa các bài toán dưới dạng mô hình toán học. Sau đó, các kết quả lý thuyết được kiểm chứng thông qua mô phỏng. Hiệu năng của tiếp cận dựa trên độ đo CPR và các cải tiến cũng được đánh giá và so sánh thông qua mô phỏng.

Chương 1

Giới thiệu

1.1 Tấn công từ chối dịch vụ phân tán DDoS và DDoS tốc độ thấp

Ngày nay các tấn công từ chối dịch vụ phân tán (*distributed denial-of-service attacks – DDoS attacks*) vẫn là mối đe dọa chính đối với mạng Internet. Các tấn công DDoS truyền thống thường sử dụng cách tiếp cận "đao to, búa lớn" trong đó kẻ tấn công có thể tuyển lựa lên đến vài trăm nghìn máy tính tham gia và điều khiển chúng gửi một số lượng rất lớn các gói tin tới một mục tiêu trên mạng có thể là một máy tính, một router hay một switch. Tuy nhiên các tấn công này rất dễ bị phát hiện do bản chất tốc độ cao, gây ra bất thường về mặt thống kê đối với các bộ giám sát mạng, vì thế hiệu quả của chúng thường bị giảm bớt.

Tuy nhiên, các tấn công LDDoS vừa có thể bóp nghẹt thông lượng TCP tổng cộng đồng thời vẫn có thể che dấu hành vi của chúng bằng cách giảm tốc độ tấn công trung bình xuống một mức thấp làm cho các bộ giám sát mạng không thể phân biệt được đâu là dòng gói tin tấn công và đâu là dòng gói tin TCP thông thường. Các tấn công LDDoS phát các gói tin tấn công vào mạng theo từng đợt bùng nổ gói tin cách đều nhau nhằm khai thác cơ chế chờ phát lại gói tin được quy định trong giao thức TCP (*TCP's timeout mechanism*).

1.2 Chống tấn công DDoS tốc độ thấp

Các cơ chế chống tấn công LDDoS có thể được chia ra thành hai loại: (1) các cơ chế đầu cuối (*end point*) và (2) các cơ chế hỗ trợ router. Các máy tính cuối có thể ngẫu nhiên hóa giá trị RTO để nó không còn phụ thuộc vào $minRTO$ như trước nữa, hoặc có thể ngẫu nhiên hóa giá trị của $minRTO$, hoặc sử dụng giá trị $minRTO = 0.2$ giây (như trong hệ điều hành Linux) thay vì 1 giây như ban đầu. Đối với các cơ chế hỗ trợ router, có thể kể đến là các thuật toán quản lý hàng đợi tích cực, chẳng hạn RED (*Random Early Detection*). Tuy nhiên RED không thể chống tấn công LDDoS hiệu quả. Tuy nhiên, nó có thể được tích hợp thêm với một độ đo gọi là CPR (*Congestion Participation Rate – CPR*) để chống tấn công LDDoS hiệu quả hơn.

1.3 Mô hình phân tích của tấn công DDoS tốc độ thấp

Hiện nay đang tồn tại 2 mô hình phân tích chính cho các tấn công LDDoS, đó là mô hình của Kuzmanovic và mô hình của Luo.

1.4 Những đóng góp chính của luận án

Luận án này có một số đóng góp chính cho lĩnh vực phòng chống tấn công DDoS tốc độ thấp nói riêng và tấn công DDoS nói chung như sau:

1. Đề xuất một phương pháp mới để tính thông lượng TCP khi có tấn công LDDoS xảy ra, nghiên cứu được thực hiện với một mô hình mạng đơn giản bao gồm từ một đến nhiều dòng TCP có thời gian trễ truyền bằng nhau và đều đi qua một liên kết nghẽn cổ chai. Kết quả mô phỏng cho thấy phương pháp đề xuất có độ chính xác khá cao trong các kịch bản được xem xét trong đó TCP không sử dụng báo nhận trễ và nó có thể xác định được khoảng giá trị mà thông lượng TCP nhiều khả năng rơi vào trong các trường hợp TCP sử dụng báo nhận trễ.
2. Đề xuất cơ chế thay đổi ngưỡng CPR theo thời gian trong tiếp cận dựa trên độ đo CPR. Kết quả mô phỏng cho thấy tiếp cận dựa trên độ đo CPR có tương thích ngưỡng có thể bảo vệ thông lượng TCP khá tốt khi có tấn công xảy ra đồng thời đảm bảo chia sẻ băng thông công bằng cho các kết nối TCP mới trong điều kiện bình thường.
3. Đề xuất một độ đo mới CIR (*Congestion Interval Rate*) để thay thế cho độ đo cũ CPR. Các kết quả mô phỏng cho thấy tiếp cận dựa trên độ đo CIR có thể bảo vệ thông lượng TCP tốt hơn so với tiếp cận ban đầu khi có tấn công xảy ra.

1.5 Cấu trúc của luận án

Luận án gồm 6 chương:

- Chương 1 giới thiệu chung về tấn công LDDoS, các giải pháp chính trong chống tấn công LDDoS, các mô hình phân tích đã có của tấn công, những đóng góp chính của luận án, và bao gồm cả phần trình bày này về cấu trúc của luận án.
- Chương 2 cung cấp các thông tin liên quan và mô hình lưu lượng của tấn công LDDoS.
- Chương 3 trình bày phương pháp mới ước lượng thông lượng TCP trong điều kiện có tấn công LDDoS.
- Chương 4 phân tích tiếp cận dựa trên độ đo CPR, đề xuất cơ chế thay đổi ngưỡng CPR theo thời gian.
- Chương 5 thảo luận và làm rõ các vấn đề hiện tại của tiếp cận dựa trên độ đo CPR và đề xuất độ đo CIR mới để bảo vệ thông lượng TCP tốt hơn trong điều kiện có tấn công LDDoS xảy ra.
- Chương 6 kết luận về luận án, những công việc đã làm được và những hướng nghiên cứu tiếp theo trong tương lai.

Chương 2

Tấn công từ chối dịch vụ phân tán DDoS tốc độ thấp

2.1 Khái niệm tấn công từ chối dịch vụ DoS

Tấn công từ chối dịch vụ (*denial-of-service attack – DoS attack*) là một hành động nhằm ngăn chặn hoặc làm suy yếu việc sử dụng hợp pháp mạng cũng như các hệ thống máy tính, các ứng dụng bằng cách làm cạn kiệt các tài nguyên như là các bộ xử lý trung tâm (*central processing units – CPU*), băng thông (*bandwidth*), bộ nhớ trong (*memory*), không gian đĩa cứng (*disk space*).

2.2 Nguồn gốc của tấn công DDoS

Nguồn gốc của tấn công DDoS nằm ở kiến trúc chức năng của mạng Internet, nó được xây dựng dựa trên 2 nền tảng: dịch vụ nỗ lực tối đa và mô hình đầu cuối tới đầu cuối. Các router trong mạng Internet chỉ có trách nhiệm trung chuyển gói tin từ nguồn tới đích, thực hiện nhiệm vụ lưu trữ và đẩy gói tin đi. Tất cả các công việc khác, nổi bật trong đó là điều khiển tắc nghẽn, được dành cho các máy tính cuối.

Nếu một máy tính trở nên độc hại bằng cách liên tục gửi gói tin vào mạng với một tốc độ cao hoặc chỉ đơn giản là không sử dụng cơ chế điều khiển tắc nghẽn, nó sẽ làm tổn thương các máy tính khác đang giao tiếp bởi vì một vài tài nguyên như là băng thông mạng, các chu kỳ của bộ xử lý trên router hay trên máy tính cuối, hoặc dung lượng bộ nhớ bị cạn kiệt. Trong khi đó, mạng trung gian vẫn truyền các gói tin tới đích một cách thụ động và không làm gì để ngăn chặn lưu lượng mạng từ máy tính độc hại này. Hiện tượng nổi tiếng này được gọi là tấn công từ chối dịch vụ (*denial-of-service attack – DoS attack*). Nếu có nhiều máy tính tham gia vào tấn công thì nó được gọi là tấn công từ chối dịch vụ phân tán (*distributed denial-of-service attack – DDoS attack*).

2.3 Các khó khăn và thách thức chính trong việc chống tấn công DDoS

Các hệ thống chống tấn công DDoS phải:

1. Có khả năng phân loại gói tin.
2. Có thể điều khiển được phần lớn lưu lượng tấn công.

Hai yêu cầu này thường khó đạt được nếu là hệ thống một điểm, chẳng hạn các cơ chế hỗ trợ router. Để phân loại gói tin, router cần phải có một bộ nhớ lớn để lưu trữ thông tin của các dòng gói tin đi qua nó, tuy nhiên do nhiều nguyên nhân khác nhau, bộ nhớ trong tại router rất hạn chế. Các hệ thống một

điểm thường phải hy sinh mục tiêu đầu tiên, đó là phân biệt lưu lượng, để đạt được mục tiêu thứ hai, điều khiển một lượng lớn lưu lượng tấn công. Khi đó nó phải sử dụng các kỹ thuật như Bloom filter để lưu trữ thông tin của một số lượng rất lớn các dòng gói tin trong điều kiện bộ nhớ hạn chế, nhưng điều này lại làm suy yếu tính chọn lọc của hệ thống bởi vì luôn có khả năng thông tin của hai dòng gói tin khác nhau bị trộn lẫn và trở nên nhập nhằng do chúng được lưu trữ tại cùng một vị trí trong bộ nhớ.

Các hệ thống một điểm có thể được đặt tại 3 vị trí khác nhau: ở gần nạn nhân, tại mạng trung gian hoặc tại mạng nguồn nơi xuất phát của các lưu lượng tấn công. Các hệ thống chống tấn công DDoS phân tán kết hợp cả ba hệ thống chống tấn công DDoS một điểm nói trên.

Các tấn công DDoS khó bị phát hiện và loại bỏ là do: (1) Giả mạo địa chỉ nguồn (2) Số lượng máy tính tấn công lớn (3) Sự giống nhau giữa lưu lượng tấn công và lưu lượng thông thường.

2.4 Sơ lược lịch sử hình thành mạng Internet và cơ chế điều khiển tắc nghẽn của giao thức TCP

Mạng Internet, ban đầu gọi là ARPANET (*Advanced Research Projects Agency Network*), ra đời năm 1969 với 4 nút mạng, đó là mạng chuyển mạch gói và triển khai bộ giao thức TCP/IP. ARPANET được tài trợ bởi Cơ quan dự án nghiên cứu nâng cao (*ARPA*) thuộc Bộ quốc phòng Mỹ (*United States Department of Defense*). Phương thức chuyển mạch gói triển khai trong mạng ARPANET dựa trên các khái niệm và thiết kế của Leonard Kleinrock, Paul Baran, Donald Davies, và Lawrence Roberts. Các giao thức giao tiếp TCP/IP của ARPANET được phát triển bởi Robert Kahn và Vint Cerf, tích hợp với các khái niệm từ dự án CYCLADES của người Pháp dưới sự chỉ đạo của Louis Pouzin.

Cơ chế điều khiển truyền dữ liệu của giao thức TCP dựa trên khái niệm cửa sổ (*window*). Mỗi kết nối TCP duy trì một biến gọi là kích thước cửa sổ W xác định số lượng gói tin lớn nhất được phép gửi đi mà chưa có báo nhận. Khi số lượng gói tin đã gửi đi và chưa có báo nhận bằng W, nguồn TCP phải chờ một gói tin báo nhận trở về trước khi nó có thể gửi đi một gói tin mới. Một gói tin báo nhận (*acknowledgement packet – ACK packet*) được tạo ra bởi máy đích mỗi khi nó nhận được một gói tin với dữ liệu mới từ nguồn TCP gửi đến, sau đó gói tin báo nhận sẽ được gửi về nguồn (gói tin này có thể bị làm trễ để giảm một nửa số lượng gói tin báo nhận hoặc để chờ dữ liệu từ máy đích gửi đến máy nguồn nếu là giao tiếp 2 chiều).

TCP phát hiện mất gói tin thông qua 2 cơ chế:

- Khi nguồn TCP nhận được 3 gói tin báo nhận trùng lắp.
- Một khoảng thời gian định trước, ký hiệu là RTO đã hết nhưng nguồn TCP vẫn chưa nhận được báo nhận của một gói tin mà nó đã gửi đi trước đó đồng thời nó cũng nhận được ít hơn 3 báo nhận trùng lắp.

Khi hiện tượng mất gói tin hiếm khi xảy ra TCP sử dụng chính sách tăng theo cấp số cộng và giảm theo cấp số nhân *AIMD* (*additive increase multiplicative decrease*) cho phép các kết nối TCP tương thích tốc độ truyền của chúng với các điều kiện mạng hiện tại như là băng thông, trạng thái tắc nghẽn, và ngược lại khi mất gói tin xảy ra thường xuyên, TCP sử dụng cơ chế phát lại gói tin do timeout.

RTO: Thời gian chờ phát lại gói tin

RTT: Thời gian đi về của gói tin

RTTVAR: Biến thiên thời gian đi về của gói tin

SRTT: Thời gian đi về của gói tin đã làm trơn

G: Mức độ chi tiết của đồng hồ (thường $\leq$ 100 mili giây)

Tính toán giá trị RTO hiện tại dựa trên những công thức sau đây:

Ban đầu:

$$RTO = 1 \text{ giây.} \tag{2.1}$$

Khi đo được giá trị RTT đầu tiên, ký hiệu là R, phía máy gửi đặt:

$$SRTT = R, \tag{2.2}$$

$$RTTVAR = R/2, \tag{2.3}$$

$$RTO = max(minRTO, SRTT + max(G, 4 \times RTTVAR)), \tag{2.4}$$

trong đó $minRTO = 1$ giây. Khi đo được giá trị RTT tiếp theo, ký hiệu là R', phía máy gửi đặt:

$$RTTVAR = (1 - \beta) \times RTTVAR + \beta \times |SRTT - R'|, \tag{2.5}$$

$$SRTT = (1 - \alpha) \times SRTT + \alpha \times R', \tag{2.6}$$

trong đó $\alpha = 1/8$ and $\beta = 1/4$,

$$RTO = max(minRTO, SRTT + max(G, 4 \times RTTVAR)). \tag{2.7}$$

Thông thường chúng ta có $minRTO > SRTT + max(G, 4 \times RTTVAR)$, dẫn đến $RTO =$

$minRTO = 1$ giây theo các công thức 2.4, 2.7 ở trên. Hơn nữa, khi hiện tượng timeout xảy ra, và giả sử rằng giá trị RTO hiện tại là 1 giây, TCP giảm cửa sổ tắc nghẽn của nó xuống một gói tin, RTO được gấp đôi thành 2 giây, và gói tin bị mất được gửi lại. Sau 2 giây, nếu gói tin đó vẫn chưa được báo nhận thì RTO được đặt giá trị là 4 giây và cứ như vậy. Các giá trị RTO có thể bị giới hạn bởi một cận trên ít nhất là 60 giây. Dãy các lần nhân đôi giá trị của RTO, được biết đến như là thuật toán lùi thời gian phát lại gói tin theo hàm số mũ, ban đầu được hình thành để giúp giao thức TCP phản ứng lại với hiện tượng tắc nghẽn mạng nghiêm trọng khi mà các gói tin bị mất thường xuyên, nhưng bây giờ đã trở thành mục tiêu của các tấn công LDDoS.

2.5 Mô hình tấn công DDoS tốc độ thấp

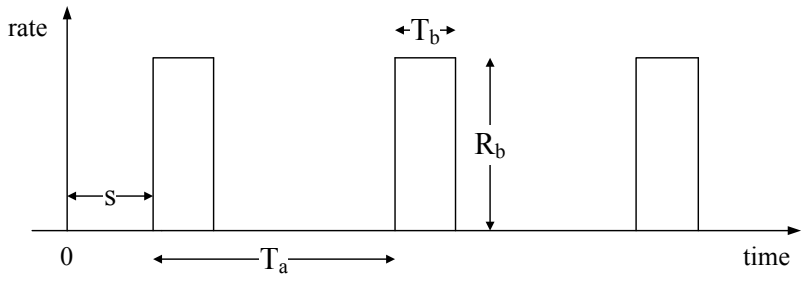
Một kết nối hay còn gọi là một dòng dữ liệu thường được định nghĩa bởi bộ 5 thành phần (địa chỉ IP nguồn, cổng nguồn, địa chỉ IP đích, cổng đích, giao thức). Mỗi dòng tấn công LDDoS có thêm các tham số khác là T_a, T_b, R_b, và s (xem Hình 2.1), trong đó:

(1) T_a là chu kỳ của các đợt bùng nổ gói tin tấn công.

(2) T_b là chiều dài của mỗi đợt bùng nổ gói tin tấn công.

(3) R_b là tốc độ của mỗi đợt bùng nổ gói tin tấn công.

(4) s là thời điểm bắt đầu tấn công.



Hình 2.1: Một dòng tấn công DDoS tốc độ thấp.

Khi một tấn công LDDoS bao gồm nhiều dòng tấn công, nó có thể được mô tả bởi bộ 4 thành phần (n, g, m, σ) với n là số lượng dòng tấn công, g là số lượng nhóm tấn công, m là số lượng dòng tấn công trong mỗi nhóm, và σ là hiệu thời gian bắt đầu của 2 nhóm tấn công liên tiếp với giả sử rằng tất cả các dòng tấn công trong cùng một nhóm đều bắt đầu tấn công tại cùng một thời điểm (giá trị s là như nhau).

Chương 3

Thông lượng TCP trong điều kiện có tấn công DDoS tốc độ thấp

3.1 Giới thiệu

Chương này đề xuất một phương pháp mới để ước lượng thông lượng TCP trong điều kiện có tấn công LDDoS xảy ra. Để đơn giản, các dòng TCP ở đây được giả sử có cùng thời gian trễ truyền và cùng đi qua một liên kết nghẽn cổ chai (do đó chúng được gọi là đồng nhất).

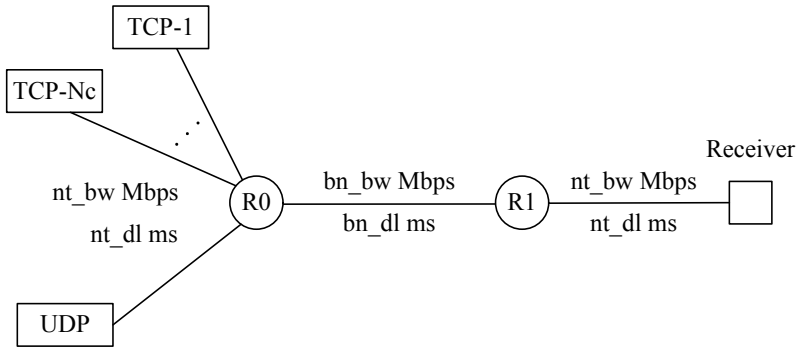
Phương pháp ước lượng của chúng tôi bao gồm hai giai đoạn. Giai đoạn đầu tiến hành xác định hình dạng của tiến trình kích thước cửa sổ của mỗi dòng TCP dựa trên các tham số tấn công đã biết và trong một môi trường mạng cụ thể. Điều này là khả thi vì nhiều nghiên cứu đã chỉ ra rằng các dòng TCP đồng nhất cùng đi qua một liên kết nghẽn cổ chai sẽ đồng bộ với nhau, các tiến trình kích thước cửa sổ của chúng gần như trùng khít với nhau. Giai đoạn thứ hai sẽ tính thông lượng của mỗi dòng một cách thích hợp và cộng tất cả các thông lượng này để được thông lượng TCP tổng cộng.

3.2 Mô hình mạng và các giả thiết

Mô hình mạng được thể hiện trong Hình 3.1 bao gồm N_c dòng TCP với dữ liệu không hạn chế. Kích thước gói tin TCP là M_{TCP} bytes. Phiên bản TCP là NewReno. Mỗi khi bên nhận nhận được một gói tin TCP với dữ liệu mới, nó gửi ngay một gói tin ACK với kích thước M_{ACK} bytes về bên gửi với thời gian trễ xử lý gói tin bằng không.[1] Tất cả các liên kết trong mạng có băng thông nt_bw Mbps và thời gian trễ truyền một chiều là nt_dl mili giây, trừ liên kết giữa router R0 và router R1 có băng thông bn_bw Mbps và thời gian trễ truyền một chiều là bn_dl mili giây. Bởi vì bn_bw rất nhỏ so với nt_bw, liên kết giữa router R0 và router R1 trở thành điểm tắc nghẽn của mạng. Hàng đợi tại liên kết nghẽn cổ chai có thể chứa tối đa B gói tin. Tất cả các liên kết sử dụng cơ chế hàng đợi drop tail. Trong mạng có một máy tấn công tên là UDP. Máy tấn công này gửi các gói tin với một kích thước không đổi là M_{UDP} bytes. Nói chung, mẫu lưu lượng tấn công được thể hiện như trong Hình 2.1.

Luận án chỉ xem xét các tấn công LDDoS với chu kỳ tấn công $T_a \geq 1$ giây và thành công, gây ra hiện tượng timeout cho tất cả các dòng TCP sau mỗi đợt bùng nổ gói tin tấn công.

[1] Giả thiết này phù hợp với trường hợp của TCP không sử dụng báo nhận trễ. Khi chúng ta làm việc với TCP sử dụng cơ chế báo nhận trễ, nó sẽ không còn phù hợp và sẽ bị loại bỏ.



Hình 3.1: Cấu trúc mạng.

3.3 Trường hợp một dòng TCP không sử dụng báo nhận trễ

Phần này sẽ ước lượng thông lượng của một dòng TCP đơn trong điều kiện có tấn công LDDoS sử dụng phân tích lý thuyết. Có hai trường hợp có thể xảy ra: (1) kích thước cửa sổ không bị chia đôi trước khi timeout và (2) kích thước cửa sổ bị chia đôi một hoặc nhiều lần trước khi timeout.

3.3.1 Kích thước cửa sổ tắc nghẽn không bị chia đôi trước khi timeout

3.3.2 Kích thước cửa sổ tắc nghẽn bị chia đôi ít nhất một lần trước khi timeout

3.3.3 Các kết quả mô phỏng

4 kịch bản tấn công được thực hiện với sơ đồ mạng như trong Hình 3.1 trong đó $N_c = 1$, $M_{TCP} = 1040$ bytes. Kích thước của các gói tin báo nhận là 40 bytes.

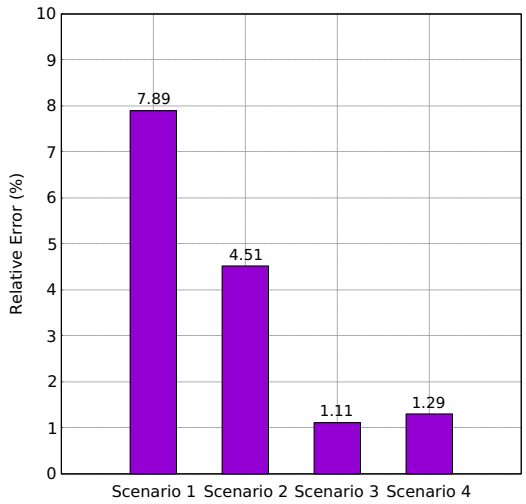
Các tham số được thay đổi là thời gian trễ mạng nt_dl và chu kỳ tấn công T_a. Các tham số tấn công LDDoS: $n = 20$, $g = 20$, $m = 1$, $M_{UDP} = 50$ bytes, $T_b = 200$ mili giây, $R_b = nt\_bw = 100$ Mbps.

Kịch bản tấn công thứ nhất với $nt\_dl = 22$ mili giây, kịch bản tấn công thứ hai với $nt\_dl = 2$ mili giây, và kịch bản tấn công thứ ba có $nt\_dl = 7$ mili giây. Tất cả ba kịch bản tấn công đó đều có chu kỳ tấn công $T_a = 2$ giây. Kịch bản tấn công thứ tư với $nt\_dl = 2$ mili giây nhưng với chu kỳ tấn công $T_a = 5$ giây.

Trong thí nghiệm này, $bn\_bw = 5$ Mbps, $bn\_dl = 6$ mili giây, kích thước hàng đợi tại liên kết nghẽn cổ chai $B = 50$ gói tin. Tất cả các mô phỏng trong thí nghiệm đều bắt đầu tại thời điểm 0 và kết thúc tại thời điểm 240 trong đó dòng TCP khởi động tại thời điểm 20 và kết thúc tại thời điểm 240 trong khi các tấn công LDDoS bắt đầu tại thời điểm 120 và kết thúc tại thời điểm 220 (đơn vị là giây). Với mỗi kịch bản tấn công, chúng tôi ghi lại thông lượng TCP trong khoảng thời gian [160, 180] (giây). Khoảng thời gian này nằm hoàn toàn trong khoảng thời gian tấn công (từ thời điểm 120 đến thời điểm 220). Các kết quả mô phỏng được so sánh với ước lượng lý thuyết đối với mỗi kịch bản tấn công sử dụng tiêu chí lỗi tương đối (*relative error*) để xác định tính chính xác của phương pháp đưa ra. Lỗi tương đối được tính

như sau:

$$\text{Lỗi tương đối} = \frac{\left|\text{Kết quả lý thuyết} - \text{Kết quả mô phỏng}\right|}{\text{Kết quả mô phỏng}}$$



Hình 3.11: Các kết quả so sánh với một dòng TCP.

Hình 3.11 cho thấy lỗi tương đối nhỏ hơn 10% đối với tất cả các kịch bản tấn công (giá trị trung bình là 3.7%, nhỏ hơn rất nhiều so với 10% của phương pháp của Luo). Đặc biệt, lỗi tương đối rất nhỏ khi thời gian trễ truyền hai chiều khá nhỏ so với $T_a - 1$, hoặc khi chu kỳ tấn công T_a lớn.

3.4 Trường hợp nhiều dòng TCP đồng nhất và không sử dụng báo nhận trễ

Trường hợp này là sự tổng quát hóa của trường hợp một dòng ở trên.

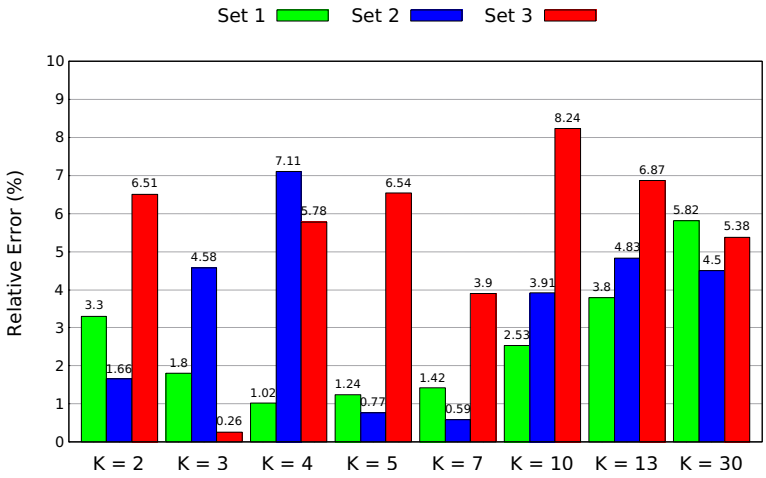
3.4.1 Kích thước cửa sổ tắc nghẽn không bị chia đôi trước khi timeout

3.4.2 Kích thước cửa sổ tắc nghẽn bị chia đôi ít nhất một lần trước khi timeout

3.4.3 Các kết quả mô phỏng

Trong phần này chúng tôi thực hiện các mô phỏng sử dụng cấu trúc mạng như trong Hình 3.1 trong đó $N_c = K > 1$. Các mô phỏng được chia thành 3 tập, trong mỗi tập giá trị của nt_dl được cố định nhưng số lượng các dòng TCP được thay đổi. Cụ thể, mỗi tập bao gồm 8 mô phỏng với $K = 2$, $K = 3$, $K = 4$, $K = 5$, $K = 7$, $K = 10$, $K = 13$, và $K = 30$. Tập thứ nhất tương ứng với $nt\_dl = 22$ ms, tập thứ hai với $nt\_dl = 2$ ms, và tập thứ ba với $nt\_dl = 7$ ms. Các tham số của các dòng TCP, của tấn

công LDDoS, và các tham số của môi trường mạng tương tự như trong trường hợp của một dòng TCP. Sau mỗi mô phỏng, thông lượng TCP trong khoảng thời gian tấn công được lưu lại và so sánh với giá trị thông lượng TCP theo lý thuyết. Giá trị lỗi tương đối nhỏ hơn 10% với tất cả các mô phỏng (giá trị trung bình là 3.85%, nhỏ hơn nhiều so với phương pháp của Luo).



Hình 3.19: Các kết quả so sánh thông lượng TCP của 3 tập mô phỏng.

3.5 Trường hợp một hoặc nhiều dòng TCP đồng nhất và sử dụng báo nhận trễ

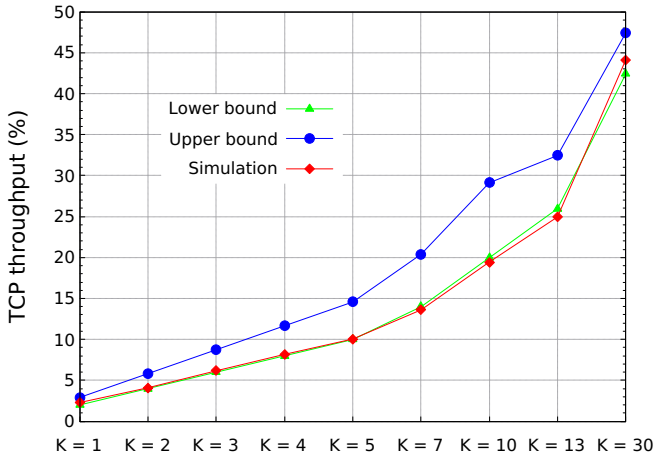
Trong trường hợp này, vì các dòng TCP có thể dùng hai cách khác nhau để tăng kích thước cửa sổ tắc nghẽn trong giai đoạn khởi động chậm sau khi bị timeout nên chúng tôi đưa ra hai giá trị ước lượng lý thuyết: một giá trị tối đa và một giá trị tối thiểu của thông lượng. Ở đây, do sử dụng cơ chế báo nhận trễ nên trong giai đoạn tránh tắc nghẽn, mỗi dòng TCP sẽ chỉ tăng kích thước cửa sổ tắc nghẽn lên xấp xỉ một nửa gói tin sau mỗi khoảng thời gian RTT.

3.5.1 Kích thước cửa sổ tắc nghẽn không bị chia đôi trước khi timeout

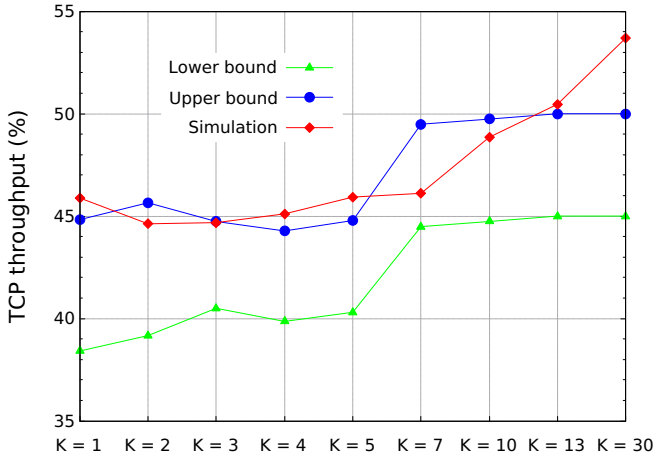
3.5.2 Kích thước cửa sổ tắc nghẽn bị chia đôi ít nhất một lần trước khi timeout

3.5.3 Các kết quả mô phỏng

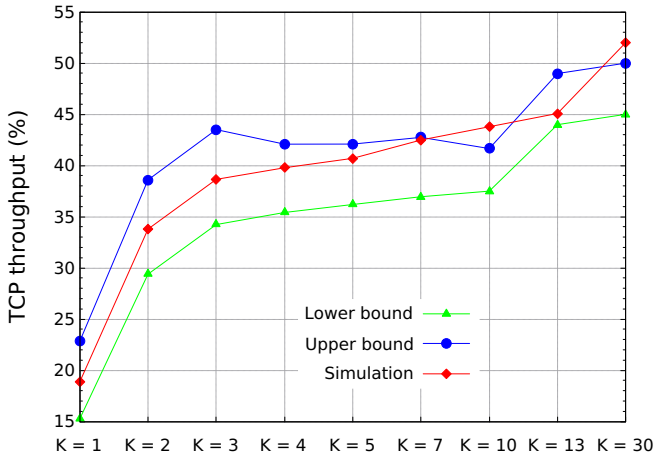
Ba tập mô phỏng như phần trước được thực hiện với TCP sử dụng cơ chế báo nhận trễ và $ack\_dl = 100$ mili giây. Các kết quả được thể hiện như trong các hình sau. Khi nt_dl nhỏ như trong Hình 3.22, đường các kết quả mô phỏng tiệm cận với đường cận trên. Khi nt_dl lớn như trong Hình 3.21, đường các kết quả mô phỏng sát với đường cận dưới. Khi nt_dl có giá trị trung bình như trong Hình 3.23, các kết quả mô phỏng hầu hết nằm trong khoảng giữa từ giá trị cận dưới đến giá trị cận trên.



Hình 3.21: Các kết quả của tập mô phỏng thứ nhất với $nt\_dl = 22$ mili giây.



Hình 3.22: Các kết quả của tập mô phỏng thứ hai với $nt\_dl = 2$ mili giây.



Hình 3.23: Các kết quả của tập mô phỏng thứ ba với $nt\_dl = 7$ mili giây.

Chương 4

Chống tấn công DDoS tốc độ thấp

4.1 Giới thiệu

Từ năm 1998, đơn vị thiết kế Internet *IETF* đã đề nghị triển khai các thuật toán quản lý hàng đợi tích cực cho các router trên Internet với mục đích tránh tắc nghẽn mạng và thay thế thuật toán quản lý hàng đợi drop-tail truyền thống. Một trong những thuật toán quản lý hàng đợi tích cực được nhiều người biết đến là Random Early Detection (RED). RED cung cấp nhiều lợi ích cho lưu lượng mạng, tuy nhiên nó không thể chống lại các tấn công LDDoS. Một số thuật toán khác dựa trên RED như RED-PD cũng không đạt hiệu quả mong muốn. Vì vậy RED cần được cải thiện và nâng cấp để chống tấn công LDDoS tốt hơn. Sau đây, chúng tôi sẽ trình bày về tiếp cận dựa trên độ đo CPR, nó là sự kết hợp giữa thuật toán RED với độ đo CPR để phân biệt và lọc gói tin từ các dòng tấn công LDDoS.

4.2 Tiếp cận dựa trên CPR

Độ đo CPR (*Congestion Participation Rate – CPR*) được đề xuất bởi Changwang Zhang và đồng nghiệp. CPR của một dòng F_i được tính như sau:

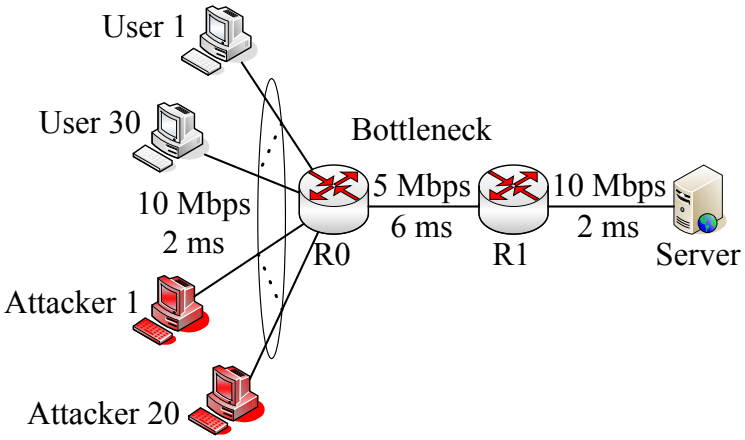
$$\theta_i = \sum_{t \in T^*} S_{i,t} \Big/ \sum_{t \in T} S_{i,t} \tag{4.1}$$

trong đó $S_{i,t}$ là số lượng gói tin của dòng F_i đến router trong khoảng thời gian [t, $t + d$], d được lựa chọn thông qua thực nghiệm và bằng 1 mili giây tương ứng với tần số lấy mẫu là 1000 Hz. T^* là tập các khoảng thời gian lấy mẫu khi liên kết đầu ra bị tắc nghẽn, và T là tập tất cả các khoảng thời gian lấy mẫu. Liên kết đầu ra được coi là bị tắc nghẽn trong một khoảng thời gian lấy mẫu nếu có ít nhất một gói tin bị loại bỏ tại hàng đợi trong khoảng thời gian đó.

Dựa trên một ngưỡng CPR, ký hiệu là τ, các tác giả đã đề xuất một tiếp cận tích hợp vào phía trước của khối RED để phát hiện và lọc các dòng tấn công LDDoS. Ý tưởng chính của tiếp cận là nếu một dòng gói tin có giá trị CPR lớn hơn τ, nó sẽ bị coi là dòng tấn công và tất cả các gói tin tiếp theo của nó sẽ bị loại bỏ, ngược lại dòng gói tin sẽ được coi là thông thường và tất cả gói tin của nó sẽ không bị loại bỏ và được chuyển cho khối RED xử lý. Độ đo CPR đã được đề xuất nhưng các tác giả chưa đánh giá hiệu năng của tiếp cận. Sau đây chúng tôi sẽ trình bày về vấn đề này.

4.3 Hiệu năng của tiếp cận dựa trên CPR

Để đánh giá hiệu năng của tiếp cận dựa trên CPR, chúng tôi thực hiện 9 mô phỏng, mỗi mô phỏng sử dụng tiếp cận với một giá trị τ cụ thể từ 0.1 đến 0.9. Tất cả mô phỏng đều bắt đầu tại thời điểm 0 giây và kết thúc tại thời điểm 240 giây, sử dụng cấu trúc mạng như Hình 4.1.

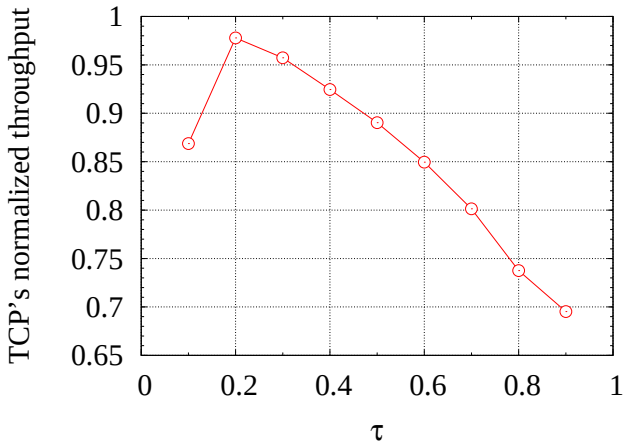


Hình 4.1: Cấu trúc mạng mô phỏng.

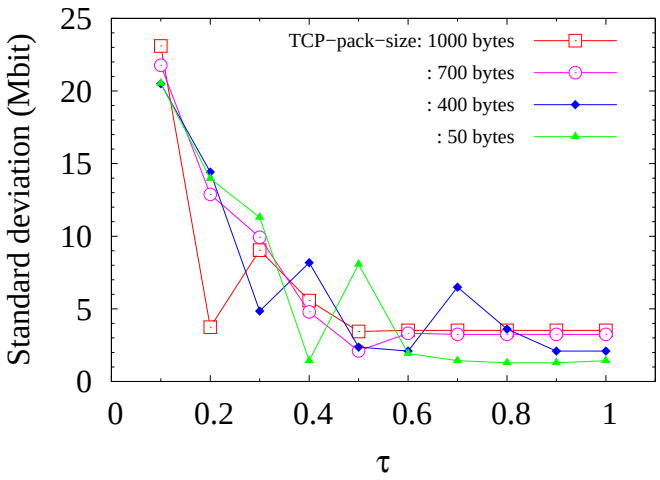
Có 30 dòng TCP xuất phát từ User 1 đến User 30 và kết thúc tại Server, sử dụng ứng dụng truyền file FTP với dữ liệu không hạn chế. Phiên bản TCP là NewReno với kích thước gói tin là 1000 byte. Các dòng TCP đều bắt đầu truyền gói tin tại thời điểm 20 giây và kết thúc tại thời điểm 240 giây. Chúng tôi tạo một kịch bản tấn công LDDoS với các tham số $n = 20$, $g = 20$, $m = 1$, $\sigma = 1$ giây. Mỗi dòng tấn công LDDoS xuất phát từ một trong 20 máy tính tấn công từ Attacker 1 đến Attacker 20 và cũng kết thúc tại Server, gửi gói tin UDP với kích thước 50 byte, và có các tham số $T_a = 20$ giây, $T_b = 200$ mili giây, $R_b = 5$ Mbit/giây. Tấn công bắt đầu tại thời điểm 120 giây và kết thúc tại thời điểm 220 giây. Kích thước hàng đợi của liên kết nghẽn cổ chai là 50 gói tin. Tiếp cận dựa trên CPR được triển khai tại router R0, trong khi tất cả các liên kết khác sử dụng hàng đợi drop-tail. Khoảng thời gian lấy mẫu là 1 mili giây. Thông lượng TCP trong khoảng thời gian tấn công từ thời điểm 120 giây tới thời điểm 220 giây được chuẩn hóa với băng thông của liên kết nghẽn cổ chai để thu được kết quả như Hình 4.2.

4.4 Ảnh hưởng của tiếp cận đối với sự công bằng của các kết nối TCP mới

Một số mô phỏng được thực hiện trong đó tiếp cận dựa trên CPR được triển khai tại router R0 với một giá trị τ cụ thể thay đổi từ 0.1 đến 0.9. Mỗi giá trị của τ được kết hợp với 4 kích thước gói tin TCP khác nhau, tạo nên tổng cộng 36 mô phỏng. 4 mô phỏng khác tương ứng với $\tau = 1$ không phải sử dụng giá trị đó của τ mà sử dụng giá trị τ thay đổi theo thời gian (được trình bày trong phần 4.5.3). Trong mỗi mô phỏng, có 10 dòng TCP bắt đầu tại thời điểm 20 giây và kết thúc tại thời điểm 240 giây. Tại thời điểm



Hình 4.2: Thông lượng TCP chuẩn hóa trong điều kiện có tấn công DDoS tốc độ thấp.



Hình 4.3: Độ lệch chuẩn của thông lượng tốt của 10 dòng TCP mới.

120 giây, 10 dòng TCP mới bắt đầu, mỗi dòng cách nhau 0.1 giây, đều kết thúc tại thời điểm 220 giây. Thông lượng tốt[1] của mỗi dòng TCP mới được ghi lại. Độ lệch chuẩn (*standard deviation*) của các thông lượng tốt được tính với giá trị trung bình là 1/20 băng thông của liên kết nghẽn cổ chai nhân với 100 giây (bằng 25 Mbit). Kết quả trong Hình 4.3 cho thấy phương thức tương thích ngưỡng có thể đảm bảo chia sẻ băng thông công bằng cho các kết nối TCP mới khi không có tấn công xảy ra.

4.5 Phương thức tương thích ngưỡng đề xuất

Phương thức tương thích τ được đề xuất với mục đích vừa bảo tồn thông lượng TCP cao trong điều kiện có tấn công LDDoS vừa đảm bảo chia sẻ băng thông công bằng cho các kết nối TCP mới.

[1]Thông lượng tốt của một dòng là băng thông nhận được tại đích của dòng đó, đã loại bỏ các gói tin có số tuần tự trùng lắp.

4.5.1 Hiện tượng hội tụ giá trị CPR của các dòng tấn công DDoS tốc độ thấp

4.5.2 RED và tỉ lệ lấy mẫu tắc nghẽn CSR

4.5.3 Phương thức tương thích ngưỡng CPR

Hình 4.6 là đề xuất phương thức tương thích τ theo thời gian của chúng tôi.

τ is initiated to 0.8;
Every *sampling period* miliseconds:
    If *the outgoing link is congested* then
        $\tau = \tau - \alpha$;
        If (τ < 0.2) then τ = 0.2;
    Else
        $\tau = \tau + \beta$;
        If (τ > 0.8) then τ = 0.8;
    End if

Fixed parameters:
sampling period: time; 1 miliseconds
α: decrement; 0.06
β: increase factor; 0.015

Hình 4.6: Phương thức tương thích ngưỡng đề xuất.

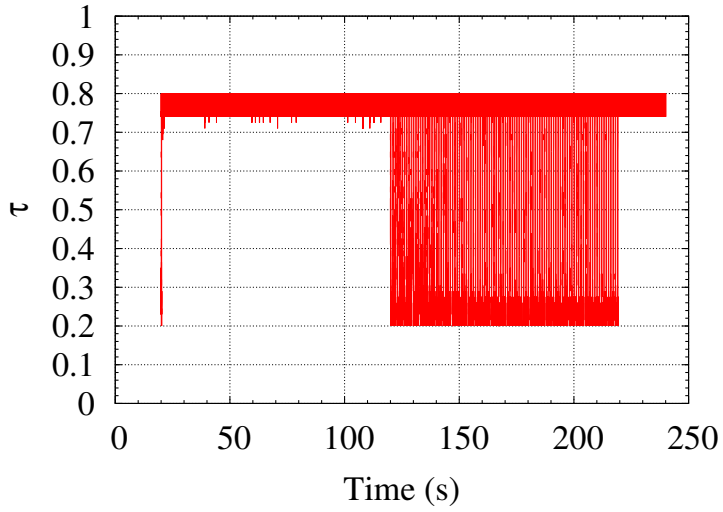
4.6 Đánh giá thực nghiệm

4.6.1 Sự tương thích ngưỡng

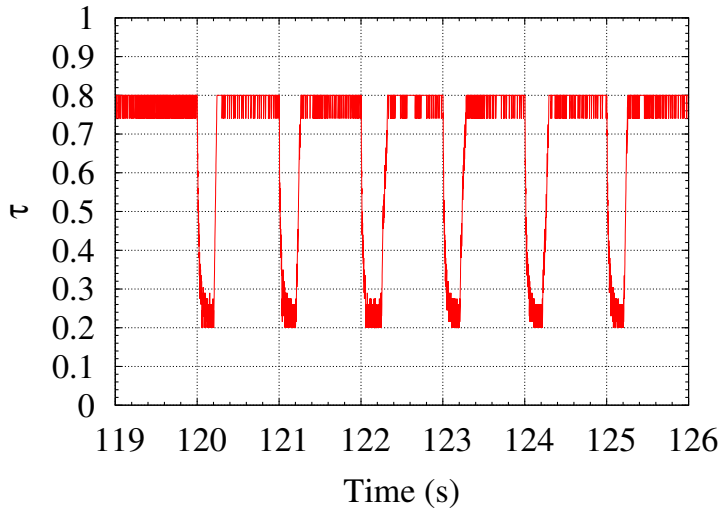
Để xác thực các phân tích ở trên, chúng tôi thực hiện lại mô phỏng trong phần 4.3 với một thay đổi là sử dụng phương thức tương thích τ từ thời điểm 0 giây thay vì sử dụng giá trị τ cố định. Sự tương thích của τ trên toàn thời gian mô phỏng và trong một khoảng thời gian ngắn từ thời điểm 119 giây tới thời điểm 126 giây được thể hiện lần lượt trong các Hình 4.7 và 4.8.

4.6.2 Hiệu năng của tiếp cận dựa trên CPR có tương thích ngưỡng

Để đánh giá hiệu năng của tiếp cận dựa trên CPR có tương thích ngưỡng, chúng tôi thực hiện 3 tập các mô phỏng: (1) Tăng cường tần số tấn công (*Attack Frequency Intensification – AFI*) (2) Tăng chiều dài các đợt bùng nổ gói tin tấn công (*Attack burst Width Intensification – AWI*) và (3) Tăng cường tốc độ các



Hình 4.7: Tương thích τ trên toàn thời gian mô phỏng.

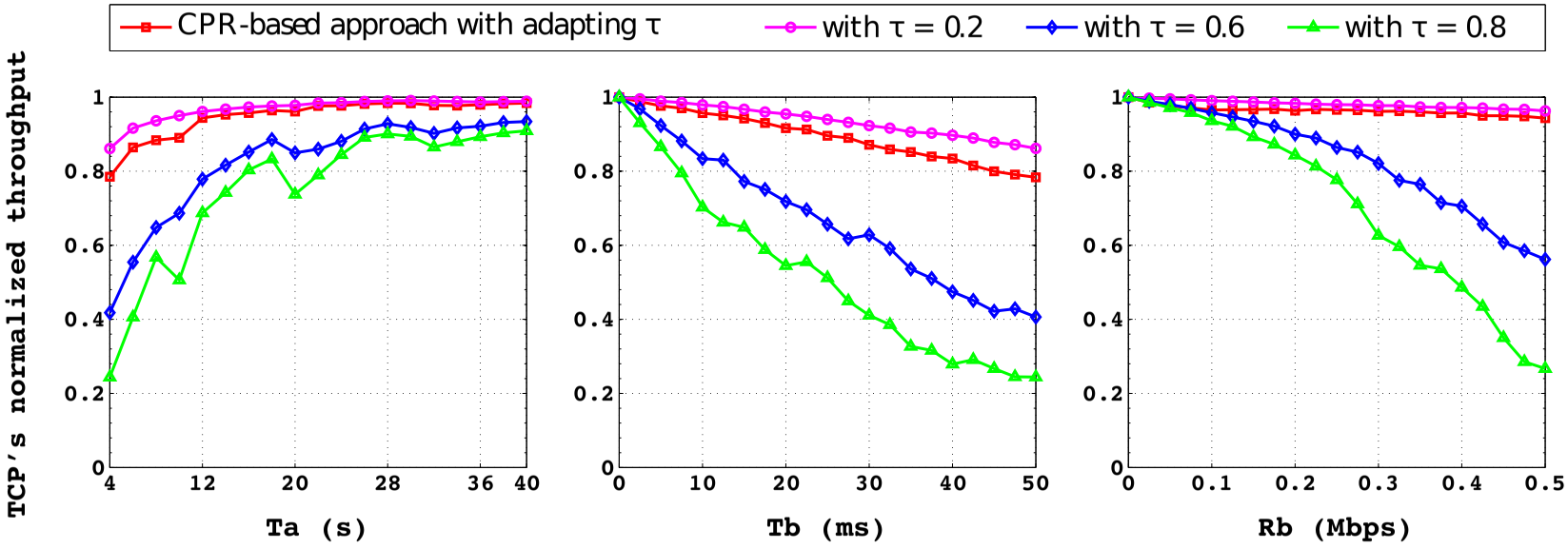


Hình 4.8: Tương thích τ trong khoảng thời gian [119, 126] giây.

đợt bùng nổ gói tin tấn công (*Attack burst Rate Intensification – ARI*) với các tham số như ở trong bảng 4.1. Phương thức tương thích τ luôn được bật tại thời điểm 0 giây. Để so sánh, chúng tôi cũng sử dụng tiếp cận dựa trên CPR với 3 giá trị τ cố định là $\tau = 0.2$, $\tau = 0.6$, và $\tau = 0.8$. Trong Hình 4.9, chúng ta thấy rằng tiếp cận dựa trên CPR có tương thích ngưỡng kém hơn một chút so với tiếp cận dựa trên CPR với $\tau = 0.2$ (thể hiện bằng các đường màu đỏ nhạt), trong khi tiếp cận dựa trên CPR với $\tau = 0.6$ hoặc $\tau = 0.8$ (thể hiện lần lượt bằng các đường màu xanh dương và xanh lá cây) kém hơn nhiều.

Bảng 4.1: Các tham số của tấn công DDoS tốc độ thấp.

Categories	LDDoS attack				Single flow			Aggregate flow		
	n	**g**	**m**	σ	T_a **(s)**	T_b **(ms)**	R_b **(Mbps)**	T_a^+ **(s)**	T_b^+ **(ms)**	R_b^+ **(Mbps)**
AFI	20	20	1	$T_a/20$	[4, 40]	200	5	[0.2, 2]	200	5
AWI	20	20	1	T_b	1	[0, 50]	5	1	[0, 1000]	5
ARI	20	1	20	0	1	200	[0, 0.5]	1	200	[0, 10]



Hình 4.9: Thông lượng TCP chuẩn hóa trong điều kiện có tấn công DDoS tốc độ thấp.

Chương 5

Các kỹ thuật tăng hiệu năng của tiếp cận dựa trên CPR

5.1 Vấn đề hiện tại của tiếp cận dựa trên CPR và các ý tưởng đề xuất

Tiếp cận dựa trên CPR là một kỹ thuật dựa trên dòng bởi vì nó tính giá trị CPR cho mỗi dòng gói tin đi qua một router. Nó chia thời gian thành những khoảng thời gian lấy mẫu nhỏ liên tiếp không chồng lên nhau. Giá trị CPR của mỗi dòng gói tin luôn luôn được cập nhật tại thời điểm cuối của mỗi khoảng thời gian lấy mẫu. Điều này có thể dẫn đến hàng đợi đầy chỉ sau một khoảng thời gian lấy mẫu và duy trì trạng thái này sau đó nếu một kẻ tấn công sắp xếp một cuộc tấn công DDoS quy mô lớn với nhiều máy tính tham gia.

CPR của mỗi dòng gói tin nên được cập nhật ngay tại thời điểm khi một gói tin bị loại bỏ ngẫu nhiên bởi thuật toán RED. Để thực hiện ý tưởng này, chúng tôi đề xuất độ đo tỉ lệ khoảng thời gian tắc nghẽn (*Congestion Interval Rate – CIR*). Giá trị CIR của một dòng F_i được tính bởi:

$$\zeta_i = |T^*|/|T| \tag{5.1}$$

trong đó $|T^*|$ và $|T|$ lần lượt là những ký hiệu cho số lượng phần tử trong tập T^* và T tương ứng. T^* là tập các khoảng thời gian lấy mẫu khi dòng F_i hoạt động và liên kết đầu ra bị tắc nghẽn. T là tập các khoảng thời gian lấy mẫu khi dòng F_i hoạt động. Một dòng gói tin được coi là hoạt động trong một khoảng thời gian lấy mẫu nếu nó có ít nhất một gói tin đến router trong khoảng thời gian lấy mẫu đó. Liên kết đầu ra được coi là bị tắc nghẽn trong một khoảng thời gian lấy mẫu nếu khối RED loại bỏ ít nhất một gói tin trong khoảng thời gian lấy mẫu đó.

5.2 Các kết quả mô phỏng

5.2.1 Giá trị CIR của các dòng TCP trong điều kiện bình thường

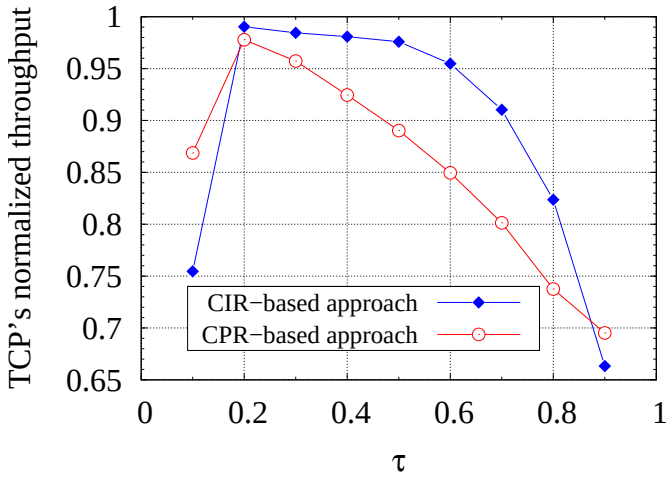
5.2.2 Sự khác nhau về giá trị CIR giữa các dòng TCP và các dòng tấn công DDoS tốc độ thấp

Trong phần này chúng ta sẽ tìm hiểu sự khác nhau giữa giá trị CIR của các dòng TCP và giá trị CIR của các dòng tấn công LDDoS. Ba tập mô phỏng như trong phần 4.6.2 được thực hiện. Các giá trị CIR nhỏ nhất, lớn nhất và trung bình của các dòng TCP và các giá trị tương ứng đối với các dòng tấn công LDDoS được ghi lại. Kết quả được thể hiện trong Hình 5.5. Như vậy, độ đo CIR có thể phân biệt được các dòng tấn công LDDoS và các dòng TCP thông thường.

5.2.3 So sánh hiệu năng của tiếp cận dựa trên CPR và tiếp cận dựa trên CIR

a) Với một mẫu tấn công cụ thể:

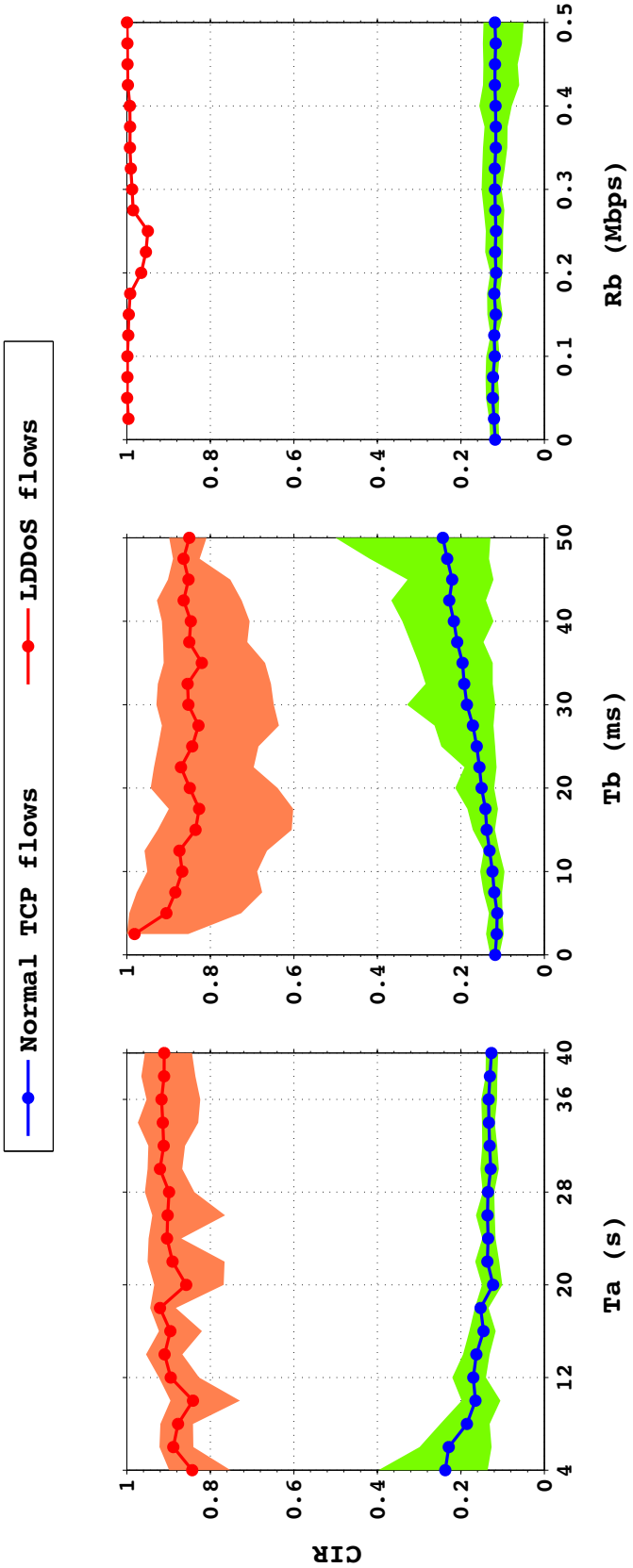
Để so sánh hiệu năng của hai tiếp cận với một mẫu tấn công cụ thể, trong phần này chúng tôi thực hiện hai tập các mô phỏng, mỗi tập tương ứng với việc sử dụng một trong hai tiếp cận tại router R0. Mỗi tập bao gồm 9 mô phỏng tương ứng với việc sử dụng τ với các giá trị từ 0.1 đến 0.9. Tất cả các mô phỏng bắt đầu tại thời điểm 0 giây và kết thúc tại thời điểm 240 giây. Kịch bản tấn công LDDoS với các tham số $n = 20$, $g = 20$, $m = 1$, $\sigma = 1$ giây. Mỗi dòng tấn công LDDoS với các tham số: $M_{UDP} = 50$ byte, $T_a = 20$ giây, $T_b = 200$ mili giây, $R_b = 5$ Mbit/giây. Tấn công bắt đầu tại thời điểm 120 giây và kết thúc tại thời điểm 220 giây. Thông lượng TCP trong khoảng thời gian tấn công từ thời điểm 120 giây tới thời điểm 220 giây được chuẩn hóa với băng thông của liên kết nghẽn cổ chai để nhận được kết quả như trong Hình 5.6.



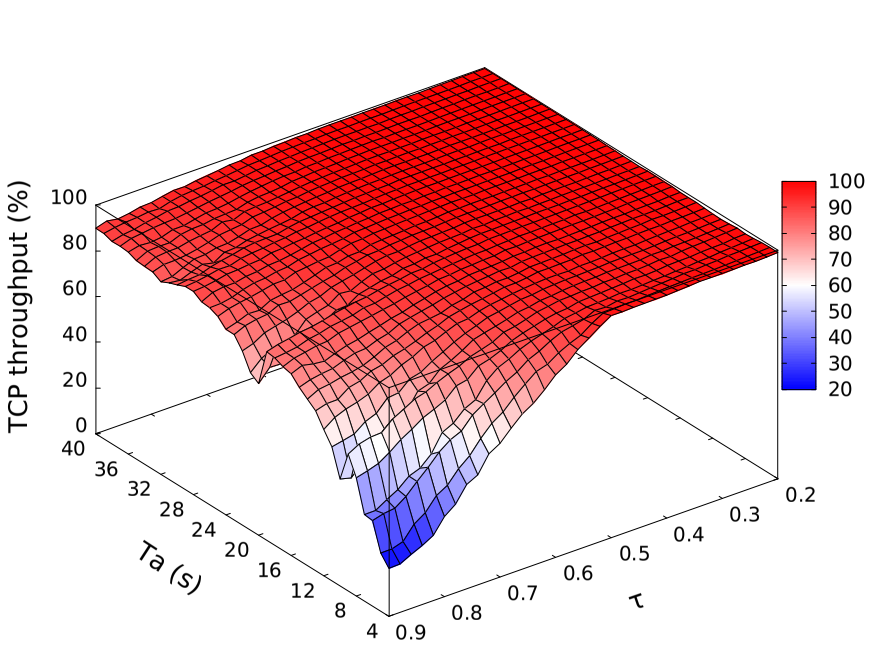
Hình 5.6: Thông lượng TCP chuẩn hóa trong điều kiện có tấn công LDDoS khi sử dụng hai tiếp cận tại router.

b) Với các mẫu tấn công khác nhau:

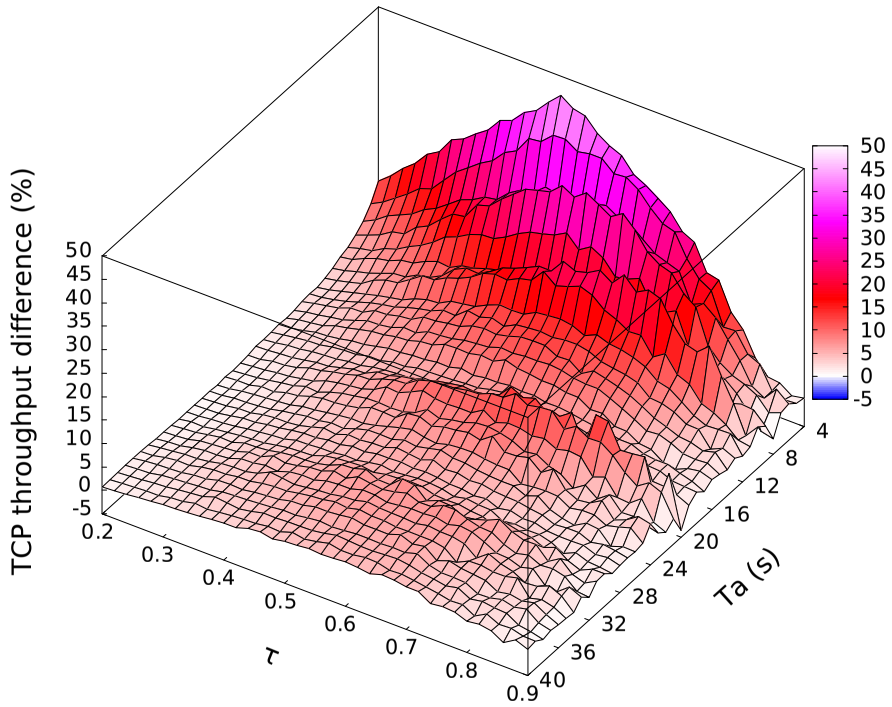
Để so sánh hiệu năng của hai tiếp cận với các mẫu tấn công khác nhau, chúng tôi thực hiện 2 tập các mô phỏng, mỗi tập tương ứng với việc sử dụng một trong các tiếp cận tại router R0. Trong mỗi tập, giá trị ngưỡng τ được thay đổi từ 0.2 đến 0.9. Với mỗi giá trị của τ, chúng tôi thực hiện 3 tập các mô phỏng, AFI, AWI, và ARI như trong phần 4.6.2. Các Hình 5.7a, 5.8a, và 5.9a thể hiện thông lượng TCP khi sử dụng tiếp cận dựa trên độ đo CIR tại router R0 và các Hình 5.7b, 5.8b, và 5.9b thể hiện hiệu của thông lượng nhận được bởi tiếp cận dựa trên độ đo CIR và thông lượng nhận được bởi tiếp cận dựa trên độ đo CPR. Như vậy, tiếp cận dựa trên độ đo CIR có thể bảo vệ thông lượng TCP tốt hơn so với tiếp cận dựa trên độ đo CPR khi có tấn công LDDoS xảy ra.



Hình 5.5: Sự khác nhau về giá trị CIR giữa các dòng TCP thông thường và các dòng tấn công DDoS tốc độ thấp.

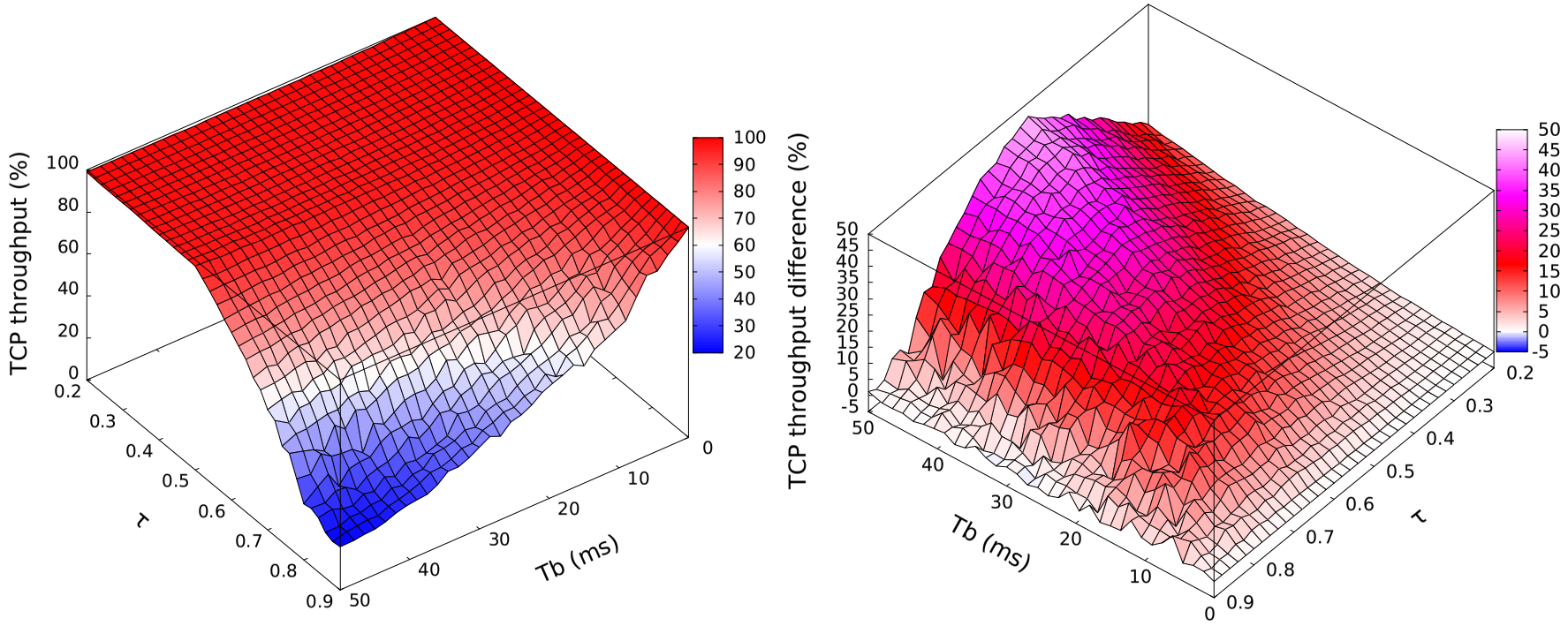


(a) Thông lượng TCP.



(b) Sự khác nhau về thông lượng TCP.

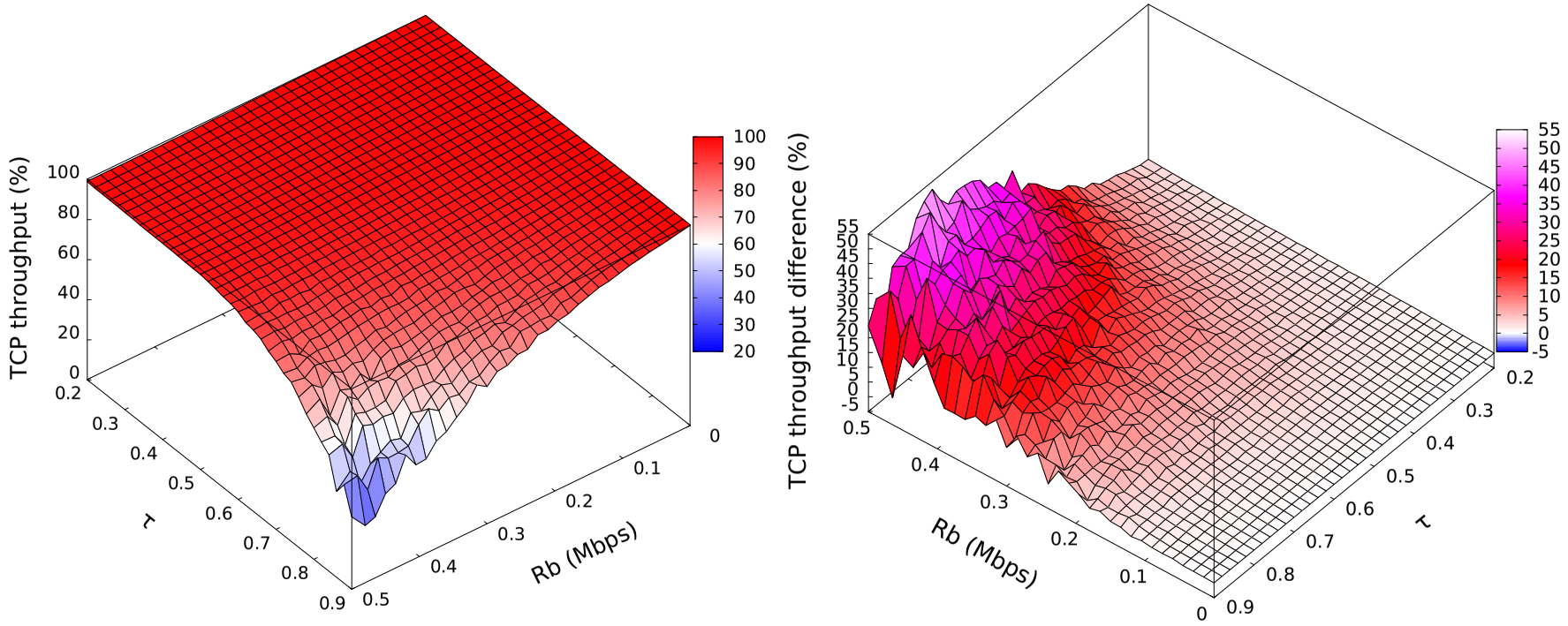
Hình 5.7: Kết quả so sánh hai tiếp cận với T_a thay đổi.



(a) Thông lượng TCP.

(b) Sự khác nhau về thông lượng TCP.

Hình 5.8: Kết quả so sánh hai tiếp cận với T_b thay đổi.



(a) Thông lượng TCP.

(b) Sự khác nhau về thông lượng TCP.

Hình 5.9: Kết quả so sánh hai tiếp cận với R_b thay đổi.

Chương 6

Kết luận

Luận án trình bày nghiên cứu về hành vi và thông lượng tổng cộng của các dòng TCP trong điều kiện có tấn công LDDoS. Mặc dù mới chỉ dừng lại xem xét một mô hình mạng đơn giản bao gồm một hoặc nhiều dòng TCP với thời gian trễ truyền giống nhau và cùng đi qua một liên kết nghẽn cổ chai, nghiên cứu đã đưa ra cái nhìn sâu sắc dựa trên những phân tích cụ thể, nhấn mạnh và làm rõ các yếu tố có ảnh hưởng lớn đến sự thay đổi đa dạng của thông lượng TCP theo số lượng các dòng TCP tham gia, các biến thể được sử dụng của giao thức TCP (với báo nhận trễ hoặc không), hay thời gian trễ truyền chung của chúng.

6.1 Những đóng góp chính chủa luận án

1. Luận án đã đề xuất một phương pháp mới để ước lượng thông lượng TCP trong điều kiện có tấn công LDDoS, kết hợp giữa phân tích rời rạc cho giai đoạn khởi động chậm và phương pháp xấp xỉ liên tục cho giai đoạn tránh tắc nghẽn của các dòng TCP để đạt được sự chính xác cần thiết và phù hợp.

2. Luận án đã phân tích và nghiên cứu hiệu năng của một phương pháp hỗ trợ router chống tấn công LDDoS cụ thể, đó là tiếp cận dựa trên độ đo CPR. Qua đó, luận án đề xuất hai ý tưởng để cải tiến và tăng cường hiệu năng của phương pháp này:

    - Thứ nhất là đề xuất phương thức tương thích ngưỡng CPR theo thời gian để giúp tiếp cận bảo tồn được thông lượng TCP cao trong điều kiện có tấn công LDDoS đồng thời có thể chia sẻ băng thông công bằng cho các kết nối TCP mới trong điều kiện bình thường khi không có tấn công.
    - Thứ hai là đề xuất một độ đo mới gọi là CIR thay thế độ đo cũ CPR với mục đích là giúp bảo vệ thông lượng TCP tốt hơn trong việc chống tấn công DDoS nói chung và LDDoS nói riêng.

6.2 Các hướng nghiên cứu tiếp theo trong tương lai

Luận án này mới chỉ dừng lại xem xét thông lượng TCP với các dòng TCP đồng nhất nên một trong những hướng nghiên cứu tiếp theo của chúng tôi có thể là nghiên cứu thông lượng TCP với các dòng TCP không đồng nhất. Ngoài ra, chúng tôi cũng muốn tìm hiểu thêm về Linux TCP bởi vì nó sử dụng một cơ chế khác biệt để tính thời gian chờ phát lại gói tin so với cơ chế truyền thống.

DANH MỤC CÔNG TRÌNH KHOA HỌC CỦA TÁC GIẢ LIÊN QUAN ĐẾN LUẬN ÁN

[$C1$] **Minh Viet Kieu**, Dai Tho Nguyen, Thanh Thuy Nguyen (2017), "Using CPR Metric to Detect and Filter Low-Rate DDoS Flows", The Eighth International Symposium on Information and Communication Technology, pp. 325 – 332.

[$C2$] **Minh Viet Kieu**, Dai Tho Nguyen, Thanh Thuy Nguyen (2018), "Techniques for Improving Performance of the CPR-Based Approach", The Ninth International Symposium on Information and Communication Technology, pp. 163 – 168.

[$C3$] **Minh Viet Kieu**, Dai Tho Nguyen, Thanh Thuy Nguyen (2020), "A Way to Estimate TCP Throughput under Low-Rate DDoS Attacks: One TCP Flow", The fourteenth RIVF International Conference on Computing and Communication Technologies, pp. 334 – 341.

Danh mục này gồm 03 công trình./.