

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG



TRẦN QUANG HÙNG

**NGHIÊN CỨU PHÁT HIỆN TẤN CÔNG DDOS DỰA TRÊN IP
ENTROPY**

Chuyên ngành : Hệ thống thông tin

Mã số : 60.48.01.04

TÓM TẮT LUẬN VĂN THẠC SĨ

HÀ NỘI - 2016

Luận văn được hoàn thành tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Người hướng dẫn khoa học: TS. HOÀNG XUÂN DẬU

Phản biện 1:

Phản biện 2:

Luận văn sẽ được bảo vệ trước Hội đồng chấm luận văn thạc sĩ tại Học viện Công nghệ Bưu chính Viễn thông

Vào lúc: giờ ngày tháng năm

Có thể tìm hiểu luận văn tại:

- Thư viện của Học viện Công nghệ Bưu chính Viễn thông

MỤC LỤC

DANH MỤC CÁC THUẬT NGỮ, CÁC CHỮ VIẾT TẮT	iv
DANH MỤC CÁC HÌNH VẼ, ĐỒ THỊ.....	v
LỜI MỞ ĐẦU	1
CHƯƠNG 1: TỔNG QUAN VỀ TẤN CÔNG DOS/DDOS VÀ CÁC BIỆN PHÁP PHÒNG CHỐNG.....	3
1.1. Khái quát về DoS/DDoS.....	3
1.1.1. Tấn công DoS và các dạng tấn công DoS.....	3
1.1.1.1 Giới thiệu về tấn công DoS.....	3
1.1.1.2 Các dạng tấn công DoS.....	3
1.1.1.3 Một số kỹ thuật tấn công DoS	3
1.1.2. Tấn công DDoS và kiến trúc tấn công DDoS	3
1.1.3 Phân loại tấn công DDoS.....	3
1.1.3.1. Dựa trên phương pháp tấn công.....	3
1.1.3.2. Dựa trên mức độ tự động	3
1.1.3.3. Dựa trên giao thức mạng	4
1.1.3.4. Dựa trên phương thức giao tiếp	4
1.1.3.5. Dựa trên cường độ tấn công.....	4
1.1.3.6. Dựa trên việc khai thác các lỗ hổng an ninh.....	4
1.2. Các biện pháp phòng chống tấn công DDoS	4
1.2.1. Dựa trên vị trí triển khai.....	4

1.2.2. Dựa trên giao thức mạng.....	4
1.2.3. Dựa trên thời điểm hành động	4
1.3. Mô tả bài toán của Luận văn	4
1.4. Kết luận chương	5
CHƯƠNG 2: PHÁT HIỆN TẤN CÔNG DDoS DỰA TRÊN IP ENTROPY.....	6
2.1. Khái quát về entropy	6
2.1.1. Khái niệm entropy và ứng dụng trong phát hiện bất thường mạng.....	6
2.1.2. Shannon entropy và entropy tham số.....	6
2.1.2.1 Shannon entropy	6
2.1.2.2 Entropy tham số.....	7
2.1.3. Một số dạng entropy khác.....	7
2.1.3.1 N-gram entropy.....	7
2.1.3.2 T-Thông tin và T-entropy	7
2.2. Mô hình phát hiện tấn công DDoS dựa trên entropy của IP nguồn7	
2.2.1. Giới thiệu mô hình.....	7
2.2.2. Hoạt động của mô hình.....	9
2.2.2.1 Giai đoạn huấn luyện.....	9
2.2.2.2 Giai đoạn phát hiện.....	10
2.3. Kết luận chương	11

CHƯƠNG 3: THỬ NGHIỆM VÀ KẾT QUẢ	12
3.1. Thử nghiệm phát hiện tấn công DDoS dựa trên tập dữ liệu gói tin offline	12
3.1.1. Giới thiệu các bộ dữ liệu thử nghiệm.....	12
3.1.2. Các thử nghiệm và kết quả.....	12
3.1.2.1 Tính mẫu entropy trong giai đoạn huấn luyện.....	12
3.1.2.2 Các thử nghiệm phát hiện	13
3.2. Mô hình hệ thống phát hiện tấn công DDoS online dựa trên entropy	18
3.3. Kết luận chương	19
KẾT LUẬN	20
DANH MỤC TÀI LIỆU THAM KHẢO	21

DANH MỤC CÁC THUẬT NGỮ, CÁC CHỮ VIẾT TẮT

CPU	Central Processing Unit	Bộ xử lý trung tâm
DDoS	Distributed Denial of Service	Tấn công từ chối dịch vụ phân tán
DNS	Domain Name System	Hệ thống phân giải tên miền
DoS	Denial of Service	Tấn công từ chối dịch vụ
HTTP	Hypertext Transfer Protocol	Giao thức truyền tải siêu văn bản
HTTPS	Hypertext Transfer Protocol Secure	Giao thức truyền tải siêu văn bản an toàn
ICMP	Internet Control Message Protocol	Giao thức thông báo điều khiển mạng internet
IDS	Intrusion Detection System	Hệ thống phát hiện xâm nhập
IP	Internet Protocol	Giao thức kết nối Internet
IPS	Intrusion Prevention System	Hệ thống phòng chống xâm nhập
P2P	Peer to peer	Mạng ngang hàng
SIP	Session Initiation Protocol	Giao thức khởi tạo phiên
SMTP	Simple Mail Transfer Protocol	Giao thức truyền tải thư điện tử đơn giản
SYN	Synchronization	Đồng bộ hóa
TCP	Transport Control Protocol	Giao thức điều khiển truyền vận
UDP	User Datagram Protocol	Giao thức gói dữ liệu người dùng

DANH MỤC CÁC HÌNH VẼ, ĐỒ THỊ

Số hiệu hình	Hình vẽ	Trang
Hình 2.1	Mô hình phát hiện tấn công DDoS dựa trên entropy của IP nguồn	8
Hình 3.1	Entropy của các gói tin hợp pháp theo cửa sổ thời gian	13
Hình 3.2	Entropy của lưu lượng hỗn hợp với cửa sổ 2 giây	14
Hình 3.3	Entropy của lưu lượng hỗn hợp với cửa sổ 5 giây	15
Hình 3.4	Entropy của lưu lượng mạng bình thường với cửa sổ 100 gói tin	16
Hình 3.5	Entropy của lưu lượng mạng hỗn hợp với cửa sổ 1000 gói tin	17
Hình 3.6	Entropy của lưu lượng mạng hỗn hợp với cửa sổ 10000 gói tin	17
Hình 3.7	Mô hình hệ thống phát hiện tấn công DDoS online dựa trên entropy	19

LỜI MỞ ĐẦU

1. Lý do chọn đề tài

Cùng với sự phát triển như vũ bão của mạng Internet hiện nay, các hình thức tấn công từ chối dịch vụ phân tán (DDoS) cũng đã và đang phát triển một cách mạnh mẽ trong những năm gần đây. Tấn công từ chối dịch vụ gây cạn kiệt tài nguyên hệ thống hoặc ngập lụt đường truyền, làm gián đoạn quá trình cung cấp dịch vụ cho người dùng hợp pháp, hoặc nguy hiểm hơn là có thể khiến toàn bộ hệ thống ngừng hoạt động. Nguy hiểm hơn nữa là tấn công DDoS rất khó phát hiện và chưa có cách phòng chống hiệu quả do số lượng các host bị điều khiển tham gia tấn công thường rất lớn và nằm rải rác ở nhiều nơi. Vì vậy đây là một mối đe dọa thường trực đối với hệ thống mạng và máy chủ dịch vụ của các cơ quan và tổ chức.

Do tính chất đặc biệt nguy hiểm của DDoS, nhiều giải pháp phòng chống đã được nghiên cứu và đề xuất trong những năm qua nhằm phát hiện và chống lại các cuộc tấn công dạng này. Tuy nhiên, cho đến hiện nay gần như chưa có giải pháp đơn nhất nào có khả năng phòng chống DDoS một cách toàn diện và hiệu quả do tính chất phức tạp, quy mô lớn cùng với tính phân tán rất cao của tấn công DDoS.

Trên cơ sở đó, tôi đã lựa chọn đề tài: "**Nghiên cứu phát hiện tấn công DDoS dựa trên IP entropy**". Đề tài nhằm tập trung nghiên cứu phương pháp phát hiện sớm tấn công DDoS dựa trên tính toán entropy của địa IP của các nguồn khởi phát tấn công, là một trong các

hướng nghiên cứu có được nhiều nhà nghiên cứu quan tâm và cho kết quả khả quan.

2. Cấu trúc của luận văn

Luận văn gồm 3 chương:

Chương 1: Tổng quan về tấn công DoS/DDoS và các biện pháp phòng chống.

Chương 2: Phát hiện tấn công DDoS dựa trên IP entropy.

Chương 3: Thử nghiệm và kết quả.

Trong đó luận văn tập trung vào chương 2 và chương 3 với mục đích nghiên cứu một mô hình phát hiện tấn công DDoS dựa trên IP entropy sau đó thực hiện các thử nghiệm nhằm đánh giá tính hiệu quả của phương pháp này.

3. Mục đích nghiên cứu

- Nghiên cứu tổng quan về tấn công DoS/DDoS
- Nghiên cứu và thử nghiệm mô hình phát hiện thông qua IP entropy.

4. Đối tượng nghiên cứu

- Các dạng tấn công DoS/DDoS trên mạng máy tính

5. Phạm vi nghiên cứu

- Nghiên cứu và thử nghiệm biện pháp phòng chống tấn công DDoS được thực hiện trên tầng IP của các máy chủ đích hoặc router mạng đích.

6. Phương pháp nghiên cứu

- Phương pháp nghiên cứu lý thuyết
- Phương pháp thực nghiệm, phân tích kết quả

CHƯƠNG 1: TỔNG QUAN VỀ TẤN CÔNG DOS/DDOS VÀ CÁC BIỆN PHÁP PHÒNG CHỐNG

1.1. Khái quát về DoS/DDoS

1.1.1. Tấn công DoS và các dạng tấn công DoS

1.1.1.1 Giới thiệu về tấn công DoS

Tấn công từ chối dịch vụ (Denial of Service – DoS) là một tổ hợp các cách thức tấn công mà một người làm cho một hệ thống không thể sử dụng, hoặc làm cho hệ thống đó chậm đi một cách đáng kể với người dùng bình thường, bằng cách làm quá tải tài nguyên của hệ thống.

1.1.1.2 Các dạng tấn công DoS

1.1.1.3 Một số kỹ thuật tấn công DoS

1.1.2. Tấn công DDoS và kiến trúc tấn công DDoS

1.1.2.1 Giới thiệu về DDoS

Tấn công từ chối dịch vụ phân tán (Distributed Denial of Service) là một dạng tấn công DoS phát triển ở mức độ cao hơn. Đối với tấn công DoS, lưu lượng tấn công thường chỉ được khởi phát từ một, hoặc một số ít host nguồn trong khi lưu lượng tấn công DDoS lại được khởi phát từ rất nhiều host nằm rải rác trên mạng Internet.

1.1.2.2. Kiến trúc tấn công DDoS

1.1.3 Phân loại tấn công DDoS

1.1.3.1. Dựa trên phương pháp tấn công

1.1.3.2. Dựa trên mức độ tự động

1.1.3.3. Dựa trên giao thức mạng

1.1.3.4. Dựa trên phương thức giao tiếp

1.1.3.5. Dựa trên cường độ tấn công

1.1.3.6. Dựa trên việc khai thác các lỗ hổng an ninh

1.2. Các biện pháp phòng chống tấn công DDoS

1.2.1. Dựa trên vị trí triển khai

1.2.2. Dựa trên giao thức mạng

1.2.3. Dựa trên thời điểm hành động

1.3. Mô tả bài toán của Luận văn

Bài toán của luận văn là nghiên cứu phát hiện tấn công DDoS dựa trên IP nguồn entropy. Bằng cách tính toán hệ số entropy của IP nguồn của các gói tin gửi đến, chúng ta có thể phát hiện được thời điểm mà tin tặc phát động một cuộc tấn công mạng. Phương pháp này bao gồm hai giai đoạn chính là giai đoạn huấn luyện và giai đoạn phát hiện. Tại giai đoạn huấn luyện, hệ số entropy của IP nguồn của các gói tin sẽ được tính toán khi lưu lượng mạng diễn ra một cách bình thường. Từ đó chúng ta sẽ có được một hồ sơ mạng bao gồm các trạng thái của mạng là bình thường. Trong giai đoạn thứ hai hay giai đoạn phát hiện, entropy của IP nguồn của các gói tin sẽ được tính toán một cách liên tục và so sánh với hồ sơ mạng đã có trước đó, nếu giá trị của entropy thay đổi nằm ngoài giới hạn cho phép thì đồng nghĩa với việc đã có một cuộc tấn công DDoS xảy ra.

1.4. Kết luận chương 1

Chương 1 trình đã đưa ra một cách nhìn tổng quan về phương thức tấn công mạng DoS/DDoS như các dạng tấn công, kiến trúc tấn công, phân loại các dạng tấn công DoS/DDoS. Thêm vào đó, một số biện pháp phòng chống cơ bản cũng đã được đưa ra với mục đích ngăn chặn các cuộc tấn công mạng. Với sự phát triển liên tục và nhanh chóng của mạng Internet hiện nay thì việc nghiên cứu và đưa ra các biện pháp phòng chống tấn công mạng DoS/DDoS là thật sự cần thiết.

CHƯƠNG 2: PHÁT HIỆN TẤN CÔNG DDoS DỰA TRÊN IP ENTROPY

2.1. Khái quát về entropy

2.1.1. Khái niệm entropy và ứng dụng trong phát hiện bất thường mạng

Entropy là thước đo của sự không chắc chắn (uncertainty) có thể được sử dụng để tổng hợp phân bố của các tính chất ở dạng rút gọn, chẳng hạn như số đơn (single number). Có nhiều các dạng entropy, nhưng chỉ có một số ít được ứng dụng cho việc phát hiện các bất thường trong mạng và phổ biến nhất là Shannon entropy [11]. Shannon entropy được ứng dụng như entropy tương đối và entropy có điều kiện để phát hiện các dấu hiệu bất thường trong mạng.

2.1.2. Shannon entropy và entropy tham số

2.1.2.1 Shannon entropy

Định nghĩa về entropy được xuất hiện lần đầu vào những năm 1950 bởi Clausius trong ngành nhiệt động lực học [19]. Năm 1948 Shannon đưa entropy vào lý thuyết thông tin [20]. Trong lý thuyết thông tin, entropy là một thước đo của sự không chắc chắn liên quan đến một biến ngẫu nhiên. Càng nhiều các biến ngẫu nhiên thì entropy càng lớn và ngược lại, biến càng chắc chắn thì entropy càng nhỏ. Đối với một phân bố xác suất $p(X = x_i)$ của một biến rời rạc, ngẫu nhiên X , Shannon entropy được định nghĩa như sau:

$$H_s(X) = \sum_{i=1}^n p(x_i) \log_a \frac{1}{p(x_i)} \quad (1)$$

X là một đặc trưng (feature) mà có thể nhận các giá trị $\{x_1 \dots x_n\}$ và $p(x_i)$ là hàm khối xác suất của đầu ra x_i . Entropy của X cũng có thể được hiểu là giá trị kỳ vọng của $\log_a \frac{1}{p(x)}$. Cơ sở của logarit có thể sử dụng là $a = 2$ (nhị phân), $a = e$ (tự nhiên) hoặc $a = 10$ (thập phân).

2.1.2.2 Entropy tham số

2.1.3. Một số dạng entropy khác

2.1.3.1 N-gram entropy

2.1.3.2 T-Thông tin và T-entropy

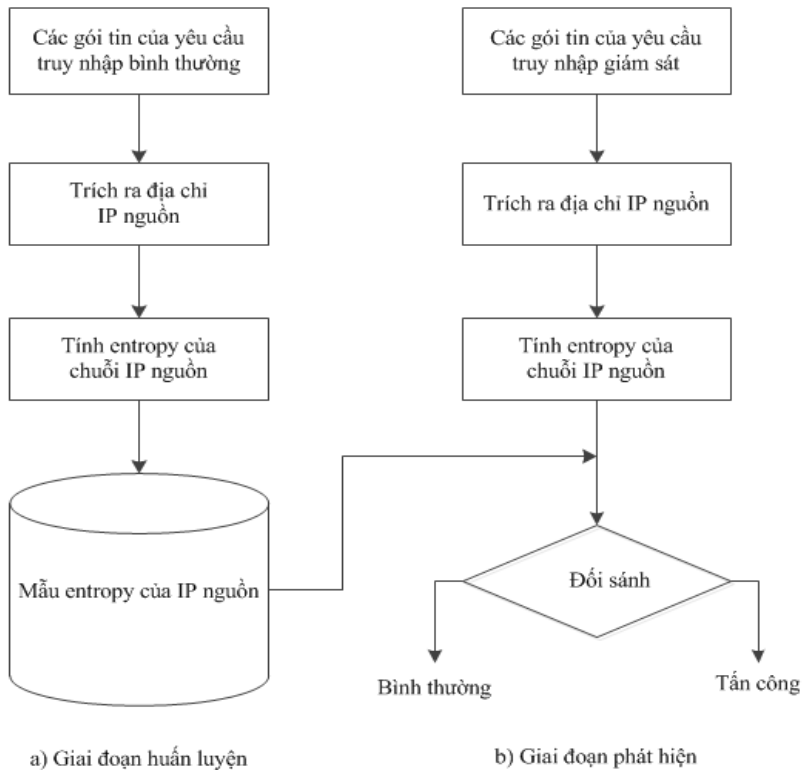
2.2. Mô hình phát hiện tấn công DDoS dựa trên entropy của IP nguồn

2.2.1. Giới thiệu mô hình

Mặc dù đặc điểm của tấn công DDoS là các nguồn khởi phát tấn công có số lượng lớn và phân tán trên mạng Internet, tấn xuất gửi các yêu cầu tấn công từ mỗi host đến máy nạn nhân là khá lớn. Ngoài ra, do các địa chỉ IP giả mạo thường được sử dụng trong các yêu cầu tấn công DDoS, nên miền địa chỉ IP nguồn của các yêu cầu giả mạo có nhiều khác biệt so với miền IP của các yêu cầu hợp lệ [23][24][25]. Trên cơ sở tính các mẫu entropy của IP nguồn của các yêu cầu truy nhập khi hệ thống ở trạng thái làm việc bình thường, có thể giám sát phát hiện tấn công DDoS trên cơ sở liên tục tính entropy

IP nguồn của các yêu cầu truy nhập và so sánh với các mẫu entropy đã thu thập trong trạng thái làm việc bình thường.

Mô hình phát hiện tấn công DDoS dựa trên entropy của IP nguồn gồm 2 giai đoạn: huấn luyện và phát hiện như biểu diễn trên Hình 2.1.



Hình 2.1: Mô hình phát hiện tấn công DDoS dựa trên entropy của IP nguồn

2.2.2. Hoạt động của mô hình

Mô hình phát hiện tấn công DDoS dựa trên entropy của IP nguồn gồm 2 giai đoạn: (a) huấn luyện và (b) phát hiện.

2.2.2.1 Giai đoạn huấn luyện

Giai đoạn huấn luyện gồm các bước:

- Thu thập dữ liệu: Dữ liệu các gói tin IP dùng cho huấn luyện được thu thập trong điều kiện hệ thống làm việc bình thường, không có tấn công DDoS. Các gói tin được thu thập liên tục trên card hoặc cổng mạng, hoặc có thể sử dụng các tập dữ liệu các gói tin IP có sẵn.
- Trích địa chỉ IP nguồn: Địa chỉ IP nguồn của từng gói tin được trích ra phục vụ cho tính toán giá trị entropy.
- Tính entropy của chuỗi IP nguồn: sử dụng phương pháp của sổ trượt theo thời gian để tính entropy của dữ liệu huấn luyện. Entropy được tính toán bởi công thức (21) mô tả ở mục 2.1.3 với $K=1$ và loggrith cơ số 2. Công thức (21) trở thành:

$$H = - \sum_{i=1}^n (p_i \log_2 p_i)$$

Trong đó p_i là giá trị của xác suất xuất hiện của IP thứ i gửi các yêu cầu đến máy chủ trên tổng số các IP đang gửi yêu cầu trong khoảng thời gian của cửa sổ trượt. Kết quả các giá trị entropy được lưu thành file để sử dụng cho giai đoạn phát hiện đồng thời các kết quả này cũng cho

phép quản trị viên có thể tính toán được giá trị của entropy khi mạng hoạt động trong thời điểm không có tấn công nằm trong khoảng nào.

2.2.2.2 *Giai đoạn phát hiện*

Giai đoạn phát hiện gồm các bước:

- Thu thập dữ liệu: Dữ liệu các gói tin IP được thu thập trong điều kiện giám sát hệ thống, được thực hiện tương tự như trong giai đoạn huấn luyện.
- Trích địa chỉ IP nguồn: Địa chỉ IP nguồn của từng gói tin được trích ra phục vụ cho tính toán giá trị entropy giống như trong giai đoạn huấn luyện.
- Tính entropy của chuỗi IP nguồn: sử dụng phương pháp cửa sổ trượt theo thời gian để tính entropy của dữ liệu giám sát. Cách thức tính toán entropy và kích thước cửa sổ trượt được chọn giống như giai đoạn huấn luyện, sau đó các kích thước của cửa sổ trượt sẽ tăng dần trong các thử nghiệm sau để xem xét ảnh hưởng của kích thước cửa sổ lên khả năng phân biệt entropy của miền lưu lượng bình thường và miền lưu lượng mạng bị tấn công.
- Đối sánh với tập entropy mẫu: Thực hiện đối sánh các giá trị entropy của dữ liệu giám sát với mẫu entropy thu được trong giai đoạn huấn luyện. Kết quả của quá trình đối sánh là dữ liệu giám sát bình thường (khi hệ số entropy vẫn nằm trong khoảng giá trị của entropy được tính toán trong giai đoạn huấn luyện) hay có tấn công

DDoS (khi hệ số entropy nằm ngoài khoảng giá trị của entropy được tính toán trong giai đoạn huấn luyện).

2.3. Kết luận chương 2

Chương 2 đã đưa ra một cách khái quát về entropy đồng thời cũng đưa ra và so sánh một số các entropy khác nhau như Shannon entropy, entropy tham số, *T-entropy* và *N-gram* entropy. Ngoài ra, chương 2 cũng đã đưa ra kiến trúc và phương thức hoạt động của mô hình phát hiện tấn công mạng sử dụng IP entropy.

CHƯƠNG 3: THỬ NGHIỆM VÀ KẾT QUẢ

3.1. Thử nghiệm phát hiện tấn công DDoS dựa trên tập dữ liệu gói tin offline

3.1.1. Giới thiệu các bộ dữ liệu thử nghiệm

Luận văn sử dụng 2 bộ dữ liệu NZIX và CAIDA để thử nghiệm mô hình phát hiện tấn công DDoS dựa trên entropy của địa chỉ IP nguồn.

Bộ dữ liệu NZIX [26] là bộ dữ liệu thu thập theo định dạng Ethernet bởi Network Research Group của trường đại học Waikato, New Zealand. Bộ dữ liệu gồm có 835 triệu gói tin với tổng dung lượng 200 GB được thu thập liên tục trong 5 ngày vào tháng 7 năm 2000. Trong bộ dữ liệu này, luận văn chỉ sử dụng file dữ liệu có mã số 20000709-000000 chứa 21 triệu gói tin với dung lượng 530 MB cho thử nghiệm. Công cụ Libtrace được sử dụng để đọc các file dữ liệu lưu các gói tin.

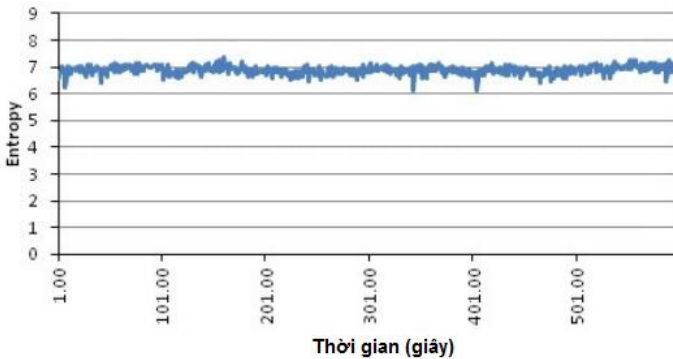
Bộ dữ liệu CAIDA [27] được sử dụng là CAIDA "DDoS Attack 2007" chứa vết lưu lượng mạng khoảng 1 giờ hệ thống bị tấn công DDoS vào ngày 4 tháng 8 năm 2007, từ 20:50:08 UTC đến 21:56:16 UTC. Tấn công DDoS này gây ngập lụt toàn bộ đường truyền kết nối máy chủ đích với Internet. Bộ dữ liệu được chia thành 5 file với dung lượng không nén khoảng 21GB.

3.1.2. Các thử nghiệm và kết quả

3.1.2.1 Tính mẫu entropy trong giai đoạn huấn luyện

Thực hiện tính toán entropy trên phần trích tập dữ liệu NZIX trong thời gian 600 giây. Cửa sổ thời gian kéo dài trong 1 giây nghĩa

là giá trị của entropy được tính toán từng giây cho các luồng dữ liệu hợp lệ trong mạng. Kết quả tính toán entropy biểu diễn trên đồ thị Hình 3.1. Giá trị của entropy trong đồ thị nằm trong khoảng 6.0 tới 7.3, điều này cho thấy rằng giá trị của entropy nằm trong khoảng tương đương nhau trong suốt khối dữ liệu gói tin và không có sự biến thiên quá lớn trong miền giá trị của entropy.



Hình 3.1: Entropy của các gói tin hợp pháp theo cửa sổ thời gian
3.1.2.2 Các thử nghiệm phát hiện

a. Kịch bản 1

Kịch bản này xem xét ảnh hưởng của một cuộc tấn công DDoS lên giá trị entropy: Kết hợp phần lưu lượng mạng trong 600 giây được trích ra từ bộ dữ liệu NZIX với một phần dữ liệu tấn công DDoS trích từ bộ dữ liệu CAIDA, bắt đầu từ giây thứ 300 và kết thúc vào giây 360. Kịch bản này tập trung vào việc phát hiện tấn công dựa trên địa chỉ nguồn.

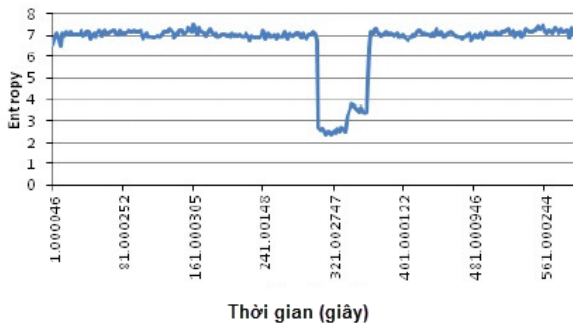
(*) Tính toán entropy sử dụng cửa sổ kích thước 1 giây:

Trước khi cuộc tấn công bắt đầu, entropy địa chỉ nguồn nằm hoàn toàn trong phạm vi 6,0-7,3. Trong cuộc tấn công, entropy giảm

xấp xỉ 4 và chỉ đạt ở mức gần 2,0. Tổng số lần tính entropy là 600. Như vậy, có thể thấy entropy sinh bởi các gói tin tấn công có giá trị khác biệt hoàn toàn so với entropy sinh với gói tin hợp lệ. Điều này cho phép phát hiện các cuộc tấn công một cách chính xác.

(*) Tính toán entropy sử dụng cửa sổ kích thước 2 giây:

Thực hiện kiểm tra luồng dữ liệu hợp pháp cả hợp pháp và cả dữ liệu tấn công trong mạng trong cùng một thời gian: tính entropy cho cả lưu lượng hợp pháp và lưu lượng tấn công được tính toán sau mỗi 2 giây. Tổng số lần tính entropy là 300. Kết quả tính toán entropy biểu diễn trên đồ thị Hình 3.2.



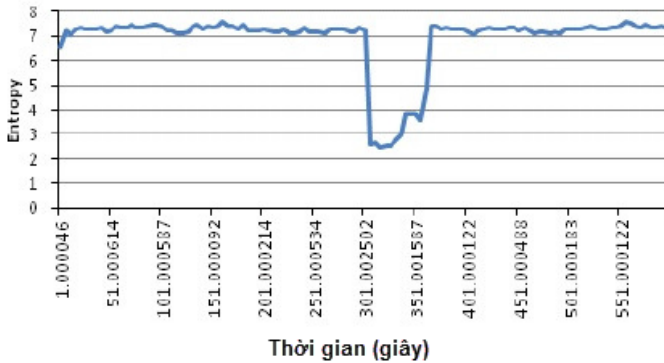
Hình 3.2: Entropy của lưu lượng hỗn hợp với cửa sổ 2 giây

Trong thời gian từ 1 giây đến 300 giây, giá trị của entropy trong đồ thị này nằm trong phạm vi 6,3- 7,4 và thời gian từ 300 giây đến 360 giây, giá trị của entropy rơi xuống trong khoảng 2,3-3,8. Sau đó, giá trị của entropy trở lại nằm trong phạm vi hẹp 6,3-7,4 trong khoảng thời gian từ 360 giây đến 600 giây. Kết quả chỉ ra rằng khi giá trị entropy nằm giữa 6,3-7,4, thì hệ thống mạng hoạt động bình

thường, chỉ khi giá trị entropy giảm đột ngột, hệ thống mạng đã bị tấn công giữa khoảng thời gian 300 giây đến 360 giây.

(*) Tính toán entropy sử dụng cửa sổ kích thước 5 giây:

Entropy được tính bằng cách lấy độ dài của cửa sổ thời gian là 5 giây.



Hình 3.3: Entropy của lưu lượng hỗn hợp với cửa sổ 5 giây

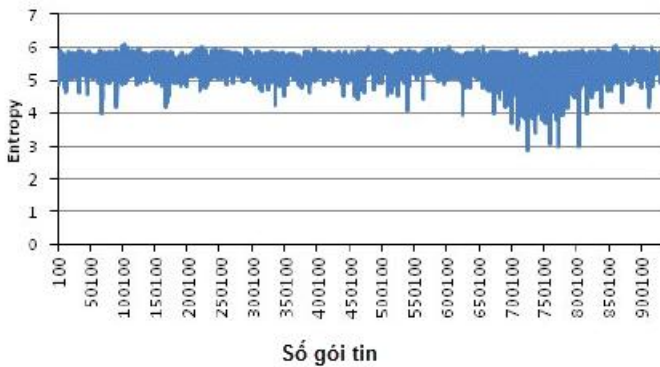
Đồ thị trên Hình 3.3 cho thấy rằng trong suốt thời gian tấn công, giá trị của entropy nằm trong khoảng giữa 2,4-3,9, trong khi đó giá trị entropy nằm giữa khoảng 7,0-7,6 thì chỉ có lưu lượng mạng hợp pháp.

b. Kịch bản 2

Thử nghiệm ở kịch bản 2 tập trung xác định mật độ các gói tin khi hệ thống mạng bình thường và mật độ gói tin khi hệ thống mạng bị tấn công DDoS. Kịch bản này cũng sử dụng bộ dữ liệu lưu lượng mạng trong 600 giây như Kịch bản 1. Có 9.050.000 gói tin được chuyển qua mạng trong khoảng thời gian này. Trong kịch bản này, entropy được tính toán theo cửa sổ là số gói tin.

(*) Cửa sổ số gói tin là 100 với toàn bộ lưu lượng mạng bình thường

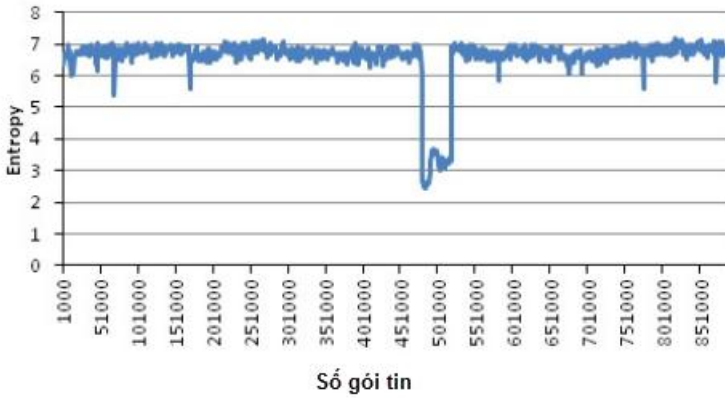
Kết quả biểu diễn trên Hình 3.4, trong đó trục x biểu thị cho số lượng gói tin và trục y biểu thị cho các giá trị entropy của cửa sổ 100 gói tin. Như vậy, 90.500 lần entropy được tính toán và thể hiện trong đồ thị, vì vậy đồ thị trở nên đông đúc hơn và các giá trị được biểu rất dày. Trong biểu đồ này, giá trị của entropy nằm giữa 3,0-6,1, khi chỉ có lưu lượng mạng hợp pháp được lưu thông qua mạng.



Hình 3.4: Entropy của lưu lượng mạng bình thường với cửa sổ 100 gói tin

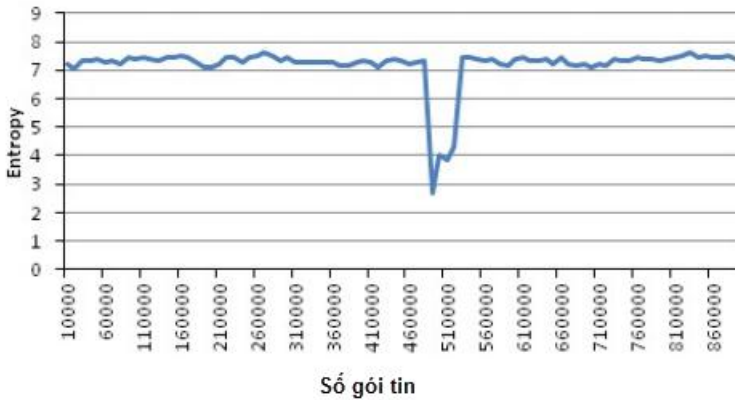
(*) Cửa sổ số gói tin là 1000 với lưu lượng mạng hỗn hợp

Sử dụng lưu lượng mạng hỗn hợp tương tự kịch bản 1, thực hiện tính toán với cửa sổ gói tin được thực hiện như là 1000 gói tin. Giá trị của entropy trong đồ thị này nằm trong phạm vi 5,2-7,1, khi mạng đang ở giai đoạn bình thường và khi giá trị giảm đột ngột xuống và nằm giữa khoảng 2,3-2,9 đồng nghĩa với việc đã có một cuộc tấn công.



Hình 3.5: Entropy của lưu lượng mạng hỗn hợp với cửa sổ 1000 gói tin

(*) Cửa sổ số gói tin là 10000 với lưu lượng mạng hỗn hợp



Hình 3.6: Entropy của lưu lượng mạng hỗn hợp với cửa sổ 10000 gói tin

Tương tự như trên, Hình 3.6 biểu diễn entropy được tính toán sau mỗi 10.000 gói. Giá trị của entropy trong đồ thị này nằm trong

phạm vi 7,0-7,5, khi lưu lượng mạng bình thường và khi giá trị giảm đột ngột xuống và nằm giữa khoảng 2,8-3,9, thì đã có một cuộc tấn công.

3.1.2.3 Một số nhận xét

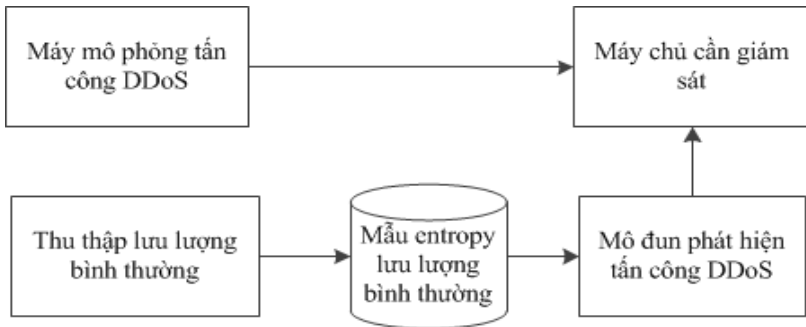
Từ các thử nghiệm, có thể rút ra một số nhận xét:

- Miền giá trị của entropy (theo thời gian hoặc theo số gói tin) của lưu mạng bình thường thường khá ổn định trong một khoảng hẹp, trong khi đó miền giá trị của entropy của lưu mạng khi bị tấn công có sự khác biệt rõ nét với miền giá trị của entropy của lưu mạng bình thường. Như vậy, có thể sử dụng phân bố giá trị entropy để nhận dạng tấn công DDoS một cách chính xác.
- Kích thước cửa sổ thời gian có ảnh hưởng đến giá trị entropy, tuy nhiên nó không ảnh hưởng quyết định đến khả năng phân biệt lưu mạng khi bị tấn công và lưu mạng bình thường. Chọn kích thước cửa sổ lớn có thể giảm được số lượng tính toán, nhưng giảm khả năng phát hiện sớm tấn công. Ngược lại, chọn kích thước cửa sổ nhỏ làm tăng khả năng phát hiện sớm tấn công, nhưng yêu cầu lượng tính toán lớn hơn.

3.2. Mô hình hệ thống phát hiện tấn công DDoS online dựa trên entropy

Luận văn thử nghiệm mô hình hệ thống phát hiện tấn công DDoS online dựa trên entropy của IP nguồn như biểu diễn trên Hình 3.7. Theo mô hình này, dữ liệu gói tin được thu thập trong điều kiện

máy chủ hoạt động bình thường để tính toán mẫu entropy sử dụng cho giai đoạn phát hiện. Mô đun phát hiện thực hiện việc giám sát, bắt các gói tin gửi từ người dùng đến máy chủ để tính toán entropy cho phát hiện tấn công DDoS. Công cụ mô phỏng sinh tấn công DDoS dùng cho thử nghiệm phát hiện. Kết quả phát hiện tương tự với các thử nghiệm thực hiện với các tập dữ liệu offline.



Hình 3.7: Mô hình hệ thống phát hiện tấn công DDoS online dựa trên entropy

3.3. Kết luận chương 3

Chương 3 mô tả các thử nghiệm và kết quả phát hiện các cuộc tấn công DDoS sử dụng các tập dữ liệu NZIX và CAIDA. Qua các thử nghiệm chúng ta có thể thấy mô hình phát hiện tấn công thông qua việc tính toán entropy là đáng tin cậy do entropy của lưu lượng tấn công có miền giá trị khác biệt rõ nét với miền giá trị của entropy khi lưu lượng mạng bình thường. Tuy nhiên, các thử nghiệm mới chỉ được thực hiện trên một tập dữ liệu nhỏ, cần có nhiều thử nghiệm với các tập dữ liệu khác để có đánh giá khách quan hơn.

KẾT LUẬN

Các kết quả đạt được

- Trình bày khái quát về tấn công DoS/DDoS, bao gồm các kỹ thuật tấn công DoS điển hình và kiến trúc tấn công DDoS;
- Hệ thống hóa các giải pháp phòng chống tấn công DDoS;
- Xây dựng và thử nghiệm mô hình phát hiện tấn công DDoS dựa trên entropy của IP nguồn;
- Thử nghiệm mô hình hệ thống phát hiện tấn công DDoS online dựa trên entropy.

Hướng nghiên cứu tiếp theo

Luận văn có thể được nghiên cứu tiếp theo các hướng sau:

- Thực hiện bổ sung các thử nghiệm trên các phần dữ liệu lớn hơn của tập dữ liệu NZIX và CAIDA, và thử nghiệm trên các tập dữ liệu khác để có đánh giá tổng thể và khách quan hơn;
- Xem xét, đánh giá về hiệu năng và khả năng phát hiện sớm tấn công DDoS của mô hình phát hiện.

DANH MỤC TÀI LIỆU THAM KHẢO

Tài liệu tiếng Việt

- [1] Hoàng Xuân Dâu, 2014, Phân loại tấn công DDoS và các biện pháp phòng chống, Tạp chí Thông tin và Truyền thông.
- [2] Nguyễn Thị Phương Nhung, 2015, Nghiên cứu và đánh giá cơ chế phòng chống tấn công DDoS cho máy chủ.

Tài liệu tiếng Anh

- [3] Saman Taghavi Zargar, James Joshi, Member and David Tippe, 2013, A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks, IEEE Communications Surveys & Tutorials.
- [4] P. J. Criscuolo, 2000, Distributed Denial of Service, Tribe Flood Network 2000 and Stacheldraht CIAC-2319, Department of Energy Computer Incident Advisory Capability (CIAC), UCRL-ID-136939, Rev. 1., Lawrence Livermore National Laboratory.
- [5] Jelena Mirkovic, Janice Martin and Peter Reiher, 2004, A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms, ACM SIGCOMM Computer Communication Review.
- [6] Jameel Hashmi, Manish Saxena, and Rajesh Saini, 2012, Classification of DDoS Attacks and their Defense Techniques using Intrusion Prevention System, International Journal of Computer Science & Communication Networks.
- [7] Rajkumar, Manisha Jitendra Nene, 2013, A Survey on Latest DoS Attacks: Classification and Defense Mechanisms, International

Journal of Innovative Research in Computer and Communication Engineering.

[8] Christos Douligeris and Aikaterini Mitrokotsa, 2003, DDoS Attacks And Defense Mechanisms: A Classification, Signal Processing and Information Technology.

[9] P.Grünwald, P.Vitányi, 2003, Kolmogorov Complexity and Information Theory. With an Interpretation in Terms of Questions and Answers. J. Logic Lang, 12, 497–529.

[10] A.Teixeira, A.Matos, A.Souto, L.Antunes, 2011, Entropy Measures vs. Kolmogorov Complexity, 13, 595–611.

[11] Claude E.Shannon, 1951, Prediction and Entropy of Printed English. The Bell System Technical Journal,30:50–64.

[12] Mark R. Titchener, 1998, A Deterministic Theory of Complexity, Information, and Entropy. In Proceedings of IEEE Information Technology Workshop, page 80.

[13] C.Reimann, P.Filzmoser, R.G.Garrett, 2005, Background and threshold: critical comparison of methods of determination. Sci. Total Environ., 346, 1–16.

[14] M.Szpyrka, B.Jasiul, K.Wrona, F.Dziedzic, 2013, Telecommunications Networks Risk Assessment with Bayesian Networks. In Computer Information Systems and Industrial Management; Saeed, K., Chaki, R., Cortesi, A., Wierchoń, S., Eds.; Volume 8104, Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany,; pp. 277–288.

- [15] M.Hall, E.Frank, G.Holmes, B.Pfahring, P.Reutemann, I.Witten, *The WEKA Data Mining Software: An Update*. SIGKDD Explor. Newslett. 2009, 11, 10–18.
- [16] A. Wagner; B. Plattner, 2005, Entropy Based Worm and Anomaly Detection in Fast IP Networks. In Proceedings of the 14th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprise (WETICE'05), Linköping University, Linköping, Sweden; pp. 172–177.
- [17] S.Ranjan; S.Shah; A.Nucci; M.Munafo; R.Cruz ; S.Muthukrishnan , 2007 DoWitcher: Effective Worm Detection and Containment in the Internet Core. In Proceedings of 26th IEEE International Conference on Computer Communications (INFOCOM 2007), Anchorage, AL, USA; pp. 2541–2545.
- [18] Gu, Y.; McCallum, A.; Towsley D., 2005, Detecting Anomalies in Network Traffic Using Maximum Entropy Estimation. In Proceedings of the 5th ACM SIGCOMM Conference on Internet Measurement (IMC '05), Berkeley, CA, USA; pp. 32–32.
- [19] R. Clausius, T. Hirst, 1867, *The Mechanical Theory of Heat: With its applications to the steam-engine and to the physical properties of bodies*; J. van Voorst: London, UK.
- [20] C. Shannon, 1948, *A Mathematical Theory of Communication*. Bell Syst. Tech. J., 27, 379–423.
- [21] C. Tsallis, 1988, Possible generalization of Boltzmann-Gibbs statistics. J. Stat. Phys. 1988, 52, 479–487.

- [22] A. Renyi, 1970, Probability Theory; Enlarged version of Wahrscheinlichkeitsrechnung, Valoszinusegyszamitas and Calcul des probabilites. English translation by Laszlo Vekerdi; North-Holland: Amsterdam, The Netherlands.
- [23] Jaswinder Singh, Monika Sachdeva And Krishan Kumar, 2013, Detection Of Ddos Attacks Using Source Ip Based Entropy, International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR), ISSN 2249-6831, Vol. 3, Issue 1.
- [24] Przemyslaw Berezinski, Bartosz Jasiul, and Marcin Szpyrka, 2015, An Entropy-Based Network Anomaly Detection Method, Entropy journal.
- [25] N. Jeyanthi, and N. Ch. Sriman Narayana Iyengar, 2012, An Entropy Based Approach to Detect and Distinguish DDoS Attacks from Flash Crowds in VoIP Networks, International Journal of Network Security, Vol.14, No.5, PP.257-269.
- [26] Softflowd-Flow-based, *Network Traffic Analyser*. Available online: <http://code.google.com/p/softflowd/> (accessed on 16 April 2015).
- [27] NfSen-Netflow *Sensor*. Available online: <http://nfsen.sourceforge.net> (accessed on 16 April 2015).
- [25] B.Jasiul, M.Szpyrka, J.Sliwa, *Detection and Modeling of Cyber Attacks with Petri Nets*. Entropy 2014, 16, 6602–6623.

- [26] NZIX Datasets,
<http://www.wand.net.nz/wits/nzix/2/20000709-000000.gz>,
[truy nhập tháng 5/2016].
- [27] The CAIDA UCSD "DDoS Attack 2007" Dataset,
<http://www.caida.org> /data/passive/ddos-20070804_dataset.xml,
[truy nhập tháng 5/2016].