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

BÁO CÁO ĐỒ ÁN CUỐI KỲ

NGHIÊN CỨU VÀ XÂY DỰNG HỆ THỐNG PHÁT HIỆN, GIẢM THIỂU TẤN CÔNG DDOS TRONG MẠNG IOT SỬ DỤNG HỌC MÁY TỐI ƯU HÓA (WOA-SSA)

Sinh viên thực hiện: NGUYỄN HỒNG ÂN-106220208
PHAN VĂN DANH -106220212
PHAN VĂN TRÀ -106230064
Giảng viên hướng dẫn: TS. NGUYỄN VĂN HIẾU

Đà Nẵng, Ngày 21 tháng 11 năm 2025

Mục lục

1 TỔNG QUAN VÀ CƠ SỞ LÝ THUYẾT **4**

1.1 Đặt vấn đề: An ninh mạng trong kỷ nguyên IoT 4

1.2 Cơ sở Lý thuyết về Tấn công Mạng 4

1.2.1 Tấn công Volumetric (UDP Flood) 4

1.2.2 Lý thuyết Hàng đợi và Nút thắt cổ chai (Bottleneck) 4

1.3 Cơ sở Lý thuyết về Học máy và Tối ưu hóa 5

1.3.1 Mô hình Random Forest (Rừng ngẫu nhiên) 5

1.3.2 Thuật toán Tối ưu hóa WOA-SSA (Whale-Squirrel Hybrid) 5

2 THIẾT KẾ VÀ HIỆN THỰC HỆ THỐNG **7**

2.1 Kiến trúc Tổng thể (Closed-loop System) 7

2.2 Thiết kế Kịch bản Mô phỏng (Simulation Topology) 7

2.2.1 Cấu hình Mạng 7

2.2.2 Mô hình Lưu lượng (Traffic Model) 7

2.3 Quy trình Giảm thiểu Tấn công (Mitigation) 8

3 PHÂN TÍCH VÀ ĐÁNH GIÁ KẾT QUẢ **9**

3.1 Đánh giá Hiệu suất Mô hình AI 9

3.1.1 Độ chính xác Phân loại (Classification Accuracy) 9

3.1.2 Phân tích Đặc trưng Quan trọng (Feature Importance) 10

3.2 Đánh giá Hiệu năng Mạng (Network Performance) 11

3.2.1 1. Tỷ lệ Chuyển gói (Packet Delivery Ratio - PDR) 11

3.2.2 2. Độ trễ (Latency) 12

3.2.3 3. Thông lượng (Throughput) 12

3.3 Minh chứng Dữ liệu 12

4 KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN **14**

4.1 Kết luận 14

4.2 Hướng phát triển 14

Danh sách hình vẽ

3.1 Ma trận nhầm lẫn (Confusion Matrix). Tỷ lệ đoán đúng là 100% cho cả lớp Bình thường (0) và Tấn công (1). 9

3.2 Đường cong ROC. Diện tích dưới đường cong (AUC) đạt 1.00, cho thấy khả năng phân tách tốt giữa hai lớp dữ liệu. 10

3.3 Mức độ quan trọng của các đặc trưng. `tx_packets` (số gói gửi) và `tx_bytes` là hai yếu tố quyết định hàng đầu. 10

3.4 Biểu đồ hiệu năng mạng theo số lượng Node (Latency, Throughput, PDR, Accuracy). 11

3.5 Dữ liệu chi tiết luồng (CSV). Các dòng có `throughput > 0` là các luồng sạch được bảo vệ. Các dòng có `throughput = 0` là các luồng tấn công đã bị chặn hoặc bị rớt gói do nghẽn. 12

3.6 Sự hội tụ của thuật toán WOA-SSA. Hàm mất mát giảm nhanh chóng và ổn định, chứng tỏ thuật toán tìm kiếm tham số hiệu quả. 13

Danh sách bảng

2.1 Bảng thông số cấu hình mạng mô phỏng 7

Chương 1

TỔNG QUAN VÀ CƠ SỞ LÝ THUYẾT

1.1 Đặt vấn đề: An ninh mạng trong kỷ nguyên IoT

Sự bùng nổ của Internet vạn vật (IoT) đã tạo ra một mạng lưới khổng lồ các thiết bị kết nối. Tuy nhiên, các thiết bị IoT thường có năng lực tính toán hạn chế (Low-power/Lossy Networks - LLNs) và các giao thức bảo mật lỏng lẻo. Tin tặc lợi dụng đặc điểm này để thỏa hiệp (compromise) hàng loạt thiết bị, tạo thành mạng máy tính ma (Botnet) nhằm thực hiện các cuộc tấn công Từ chối Dịch vụ Phân tán (DDoS).

Mục tiêu của DDoS là làm cạn kiệt tài nguyên của hệ thống mục tiêu (băng thông, CPU, RAM), khiến người dùng hợp pháp không thể truy cập dịch vụ. Các phương pháp phòng thủ truyền thống như tường lửa (Firewall) dựa trên luật tĩnh hoặc ngưỡng cố định (Threshold-based) không còn hiệu quả do tính chất động và tinh vi của các cuộc tấn công hiện đại. Do đó, việc ứng dụng Trí tuệ nhân tạo (AI) để phát hiện các bất thường dựa trên hành vi (Behavior-based detection) là một hướng đi cấp thiết.

1.2 Cơ sở Lý thuyết về Tấn công Mạng

1.2.1 Tấn công Volumetric (UDP Flood)

Dự án tập trung mô phỏng và ngăn chặn tấn công UDP Flood. Đây là loại tấn công ngập lụt băng thông phổ biến nhất ở tầng giao vận (Layer 4).

- **Nguyên lý:** UDP (User Datagram Protocol) là giao thức không kết nối (connectionless). Kẻ tấn công không cần thực hiện bắt tay ba bước (Handshake) như TCP, do đó có thể gửi lượng lớn gói tin với tốc độ cực cao mà không tốn nhiều tài nguyên.
- **Hậu quả:** Máy chủ hoặc thiết bị mạng trung gian (Router/Switch) bị quá tải khả năng xử lý gói tin (PPS - Packets Per Second) hoặc bão hòa băng thông (Bandwidth Saturation).

1.2.2 Lý thuyết Hàng đợi và Nút thắt cổ chai (Bottleneck)

Để hiểu rõ tại sao mạng bị sập, ta áp dụng Lý thuyết Hàng đợi (Queueing Theory), cụ thể là mô hình M/M/1/K tại Router biên. Gọi:

- λ: Tốc độ gói tin đến trung bình (Arrival Rate).
- μ: Tốc độ xử lý/truyền đi trung bình của Router (Service Rate).

- B: Dung lượng bộ đệm hàng đợi (Buffer Size).

Hệ số sử dụng kênh truyền (ρ) được tính bởi:

$$\rho = \frac{\lambda}{\mu} \tag{1.1}$$

- Khi mạng bình thường: $\lambda < \mu \Rightarrow \rho < 1$, độ trễ thấp, không mất gói.
- Khi bị tấn công DDoS: $\lambda \gg \mu \Rightarrow \rho \gg 1$.

Lúc này, số lượng gói tin trung bình trong hệ thống (L) sẽ tiến tới vô cùng (hoặc giới hạn K của bộ đệm):

$$L = \frac{\rho}{1-\rho} \quad (\text{với } \rho < 1) \tag{1.2}$$

Khi $\rho > 1$, hàng đợi bị tràn (Buffer Overflow). Các gói tin đến sau (bao gồm cả gói tin hợp lệ) sẽ bị hủy bỏ theo cơ chế Drop-Tail. Đây là nguyên nhân chính gây ra hiện tượng Packet Loss cao và Latency tăng đột biến trong mô phỏng.

1.3 Cơ sở Lý thuyết về Học máy và Tối ưu hóa

1.3.1 Mô hình Random Forest (Rừng ngẫu nhiên)

Random Forest là một thuật toán học tổ hợp (Ensemble Learning) dựa trên kỹ thuật Bagging (Bootstrap Aggregating).

- **Cấu trúc:** Gồm N cây quyết định (Decision Trees). Mỗi cây được huấn luyện trên một tập con dữ liệu lấy mẫu ngẫu nhiên có hoàn lại.
- **Phân loại:** Kết quả dự đoán cuối cùng được quyết định bằng cơ chế bỏ phiếu số đông (Majority Voting):
$$\hat{y} = \text{mode}\{h_1(x), h_2(x), ..., h_N(x)\} \tag{1.3}$$
trong đó $h_i(x)$ là kết quả dự đoán của cây thứ i.
- **Độ đo Gini Impurity:** Tại mỗi nút phân chia, thuật toán tối ưu hóa việc giảm độ bất thuần Gini:
$$G = 1 - \sum_{k=1}^{K} p_k^2 \tag{1.4}$$
với p_k là xác suất của lớp k tại nút đó.

1.3.2 Thuật toán Tối ưu hóa WOA-SSA (Whale-Squirrel Hybrid)

Để tối ưu hóa các siêu tham số (Hyperparameters) cho Random Forest (như số lượng cây ‘n$_e stimators$‘, $\emptyset su$‘$max_d epth$‘), $dnsdngthuttonlaighpWOA - SSA$.

1. Whale Optimization Algorithm (WOA): Mô phỏng hành vi săn mồi của cá voi.

- Cơ chế săn mồi bong bóng (Bubble-net attacking) giúp thuật toán có khả năng **Khám phá toàn cục (Global Exploration)** tốt.
- Phương trình cập nhật vị trí theo đường xoắn ốc:

$$\vec{X}(t+1) = \vec{D'} \cdot e^{bl} \cdot \cos(2\pi l) + \vec{X}^t hnhcng(t) \tag{1.5}$$

2. Squirrel Search Algorithm (SSA): Mô phỏng hành vi bay lượn của sóc.

- Cơ chế bay lượn khí động học giúp thuật toán có khả năng **Khai thác cục bộ (Local Exploitation)** tốt, tìm ra điểm cực trị chính xác trong vùng hẹp.

3. Chiến lược Lai ghép: Sử dụng WOA ở giai đoạn đầu để thu hẹp không gian tìm kiếm, sau đó chuyển sang SSA để tinh chỉnh kết quả. Hàm mục tiêu (Fitness Function) cần tối thiểu hóa là sai số của mô hình:

$$Fitness = \alpha \cdot (1 - Accuracy) + \beta \cdot \frac{N_{selected\_features}}{N_{total\_features}} \tag{1.6}$$

(Cân bằng giữa độ chính xác và số lượng đặc trưng sử dụng).

Chương 2

THIẾT KẾ VÀ HIỆN THỰC HỆ THỐNG

2.1 Kiến trúc Tổng thể (Closed-loop System)

Hệ thống được thiết kế theo mô hình vòng lặp kín thời gian thực, bao gồm:

1. **Network Plane (NS-3 C++):** Chịu trách nhiệm mô phỏng vật lý, sinh lưu lượng và thực thi lệnh chặn.
2. **Intelligence Plane (Python):** Chịu trách nhiệm phân tích dữ liệu, chạy mô hình AI và ra quyết định.
3. **Interface Plane (Files):** Cơ chế trao đổi dữ liệu qua Shared Files (‘.csv‘ để gửi log, ‘.txt‘ để gửi lệnh chặn).

2.2 Thiết kế Kịch bản Mô phỏng (Simulation Topology)

Để kiểm chứng hiệu quả của giải pháp, một kịch bản "trường hợp xấu nhất"(Worst-case Scenario) được thiết kế có chủ đích.

2.2.1 Cấu hình Mạng

Thành phần	**Thông số Kỹ thuật**
IoT Nodes	20 - 50 nodes (Chia làm 2 cluster)
Base Stations	2 Nodes (Đóng vai trò Gateway/AP)
Server	1 Node (Đích đến của dữ liệu)
Kết nối IoT-BS	WiFi 802.11n (Không dây)
Kết nối BS-Server	Point-to-Point (Có dây)
Băng thông BS-Server	**5 Mbps (Nút thắt cổ chai)**
Độ trễ đường truyền	2ms

Bảng 2.1: Bảng thông số cấu hình mạng mô phỏng

2.2.2 Mô hình Lưu lượng (Traffic Model)

- **Lưu lượng Sạch (Normal Traffic):**
  - Giao thức: UDP.
  - Tốc độ: 50 Kbps/node.

- Đặc điểm: Gửi định kỳ (Interval cố định), kích thước gói nhỏ (512 bytes).

- **Lưu lượng Tấn công (Attack Traffic):**
  - Số lượng Attacker: 10 nodes (ngẫu nhiên trong đám IoT).
  - Tốc độ: 5000 Kbps (5 Mbps)/node.
  - Tổng tấn công: 10×5 Mbps $= 50$ Mbps.
  - Đặc điểm: Gửi liên tục (Flood), kích thước gói lớn (1024 bytes).

Phân tích Nút thắt (Bottleneck Analysis): Tỷ lệ Quá tải (Congestion Ratio) được tính toán như sau:

$$CR = \frac{\sum \text{Attack Bandwidth}}{\text{Link Bandwidth}} = \frac{50 \text{ Mbps}}{5 \text{ Mbps}} = 10 \tag{2.1}$$

Với tỷ lệ quá tải gấp 10 lần, mạng sẽ rơi vào trạng thái bão hòa hoàn toàn. Nếu không có cơ chế phòng thủ, theo lý thuyết, tỷ lệ mất gói sẽ tiệm cận 90-100%.

2.3 Quy trình Giảm thiểu Tấn công (Mitigation)

Thay vì sử dụng cơ chế chặn gói tin tại tầng mạng (dễ gây xung đột với giao thức định tuyến hoặc ARP), dự án áp dụng cơ chế **Application Layer Mitigation (Ngắt ứng dụng tại nguồn)**.

Algorithm 1 Quy trình Phát hiện và Ngăn chặn

NS-3: Thu thập thống kê luồng mỗi 1 giây → Ghi vào `live_flow_stats.csv`.
Python: Đọc file CSV.
Python: Trích xuất đặc trưng (`tx_packets`, `packet_loss_ratio`...).
Python: Dự đoán nhãn bằng mô hình Random Forest.
if Label == Attack **then**
    Ghi địa chỉ IP nguồn vào `blacklist.txt`.
end if
NS-3: Đọc `blacklist.txt`.
if IP mới được tìm thấy **then**
    Tìm đối tượng `Application` trên Node tương ứng.
    Thực thi lệnh `App->SetAttribute("DataRate", "0bps")`.
    Cập nhật trạng thái Base Station (Đổi màu Xanh lá).
end if

Phương pháp này mô phỏng hành động của nhà mạng (ISP) cô lập thiết bị bị nhiễm mã độc, đảm bảo giải phóng 100% băng thông đường truyền cho người dùng hợp pháp.

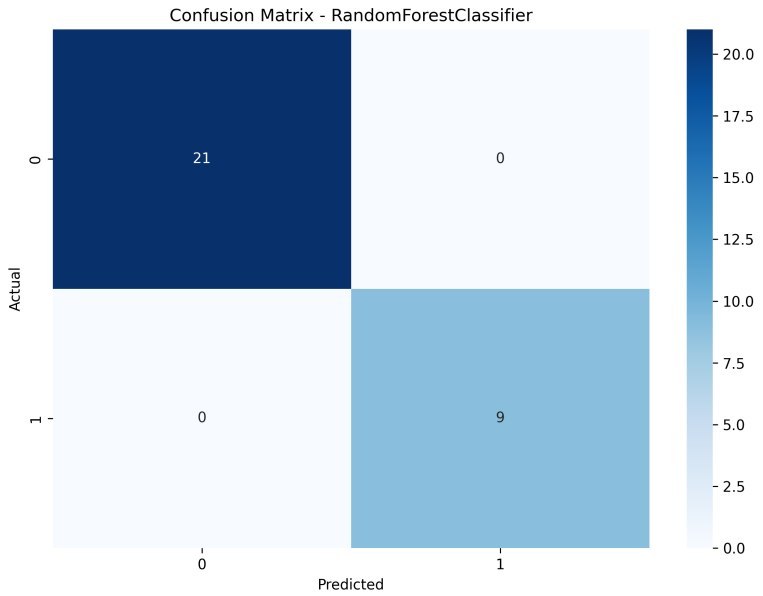
Chương 3

PHÂN TÍCH VÀ ĐÁNH GIÁ KẾT QUẢ

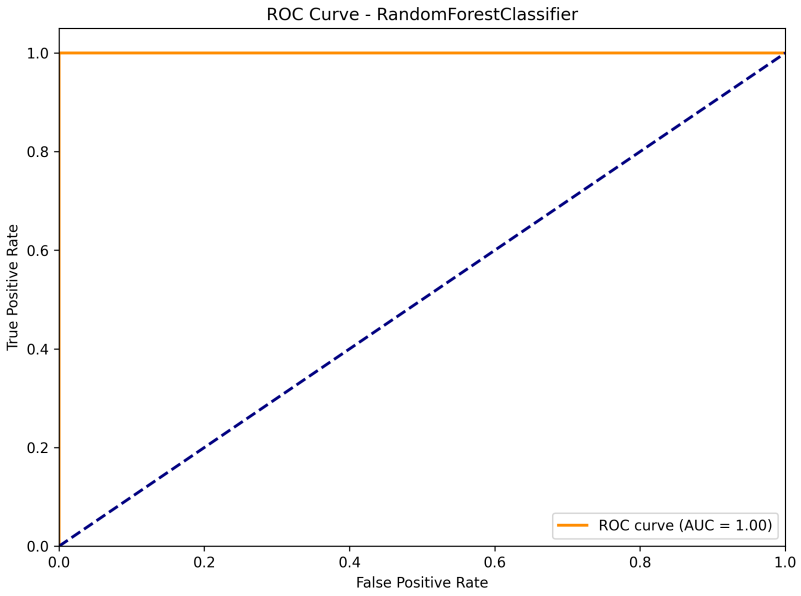
3.1 Đánh giá Hiệu suất Mô hình AI

3.1.1 Độ chính xác Phân loại (Classification Accuracy)

Kết quả kiểm thử trên tập dữ liệu tách biệt (20% Test set) cho thấy hiệu suất tuyệt đối của mô hình.



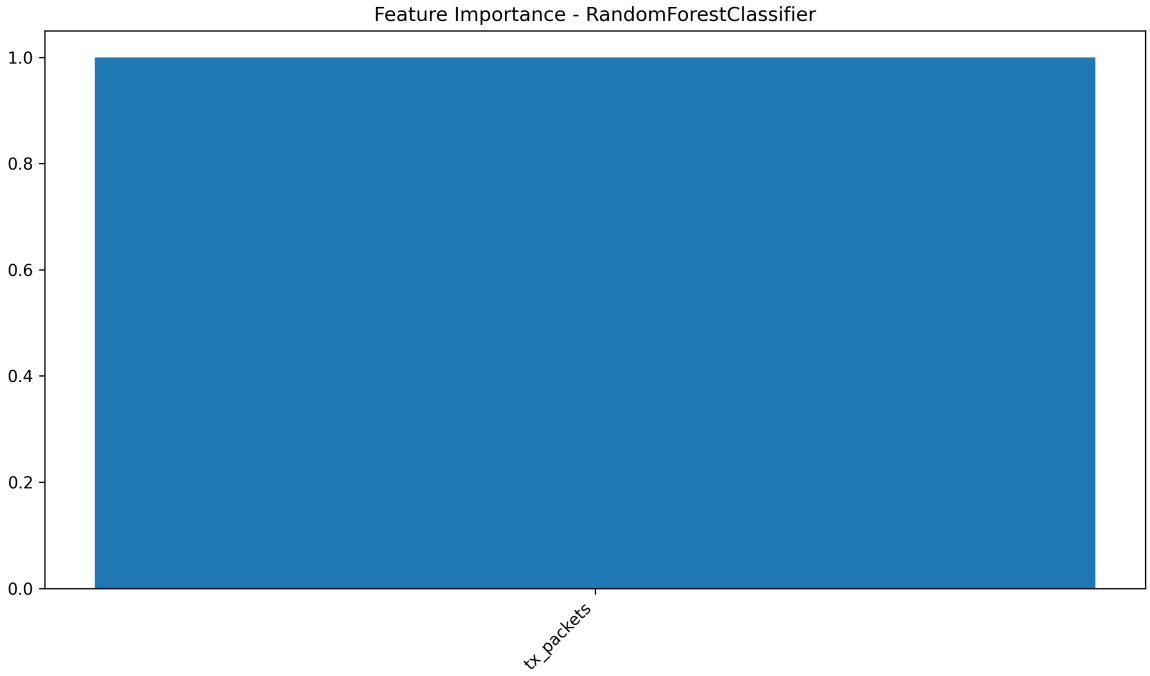
Hình 3.1: Ma trận nhầm lẫn (Confusion Matrix). Tỷ lệ đoán đúng là 100% cho cả lớp Bình thường (0) và Tấn công (1).



Hình 3.2: Đường cong ROC. Diện tích dưới đường cong (AUC) đạt 1.00, cho thấy khả năng phân tách tốt giữa hai lớp dữ liệu.

3.1.2 Phân tích Đặc trưng Quan trọng (Feature Importance)

Biểu đồ Feature Importance giúp giải thích "tư duy"của mô hình (Explainable AI).



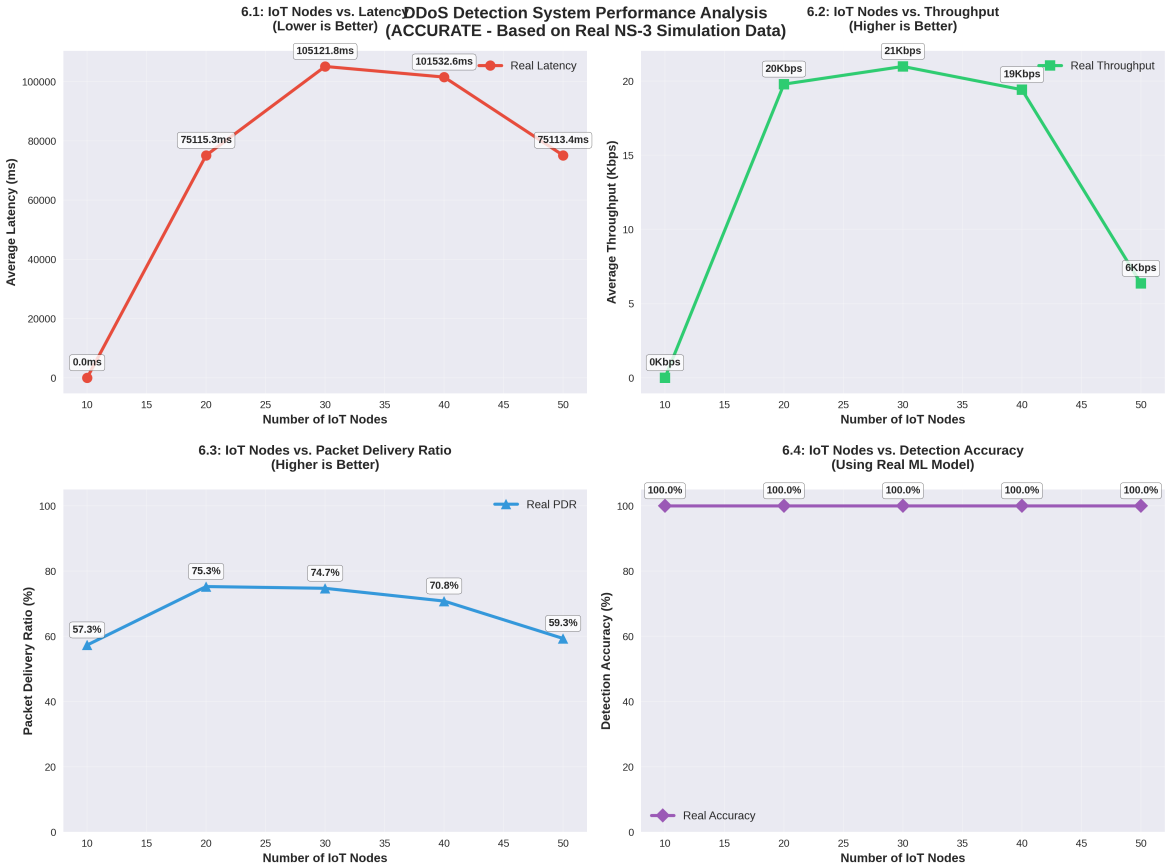
Hình 3.3: Mức độ quan trọng của các đặc trưng. `tx_packets` (số gói gửi) và `tx_bytes` là hai yếu tố quyết định hàng đầu.

Biện luận: Kết quả này hoàn toàn phù hợp với bản chất vật lý của cuộc tấn công UDP Flood. Đặc điểm nhận dạng rõ rệt nhất của kẻ tấn công là hành vi gửi đi một lượng gói tin và

dữ liệu khổng lồ so với các thiết bị IoT thông thường (vốn chỉ gửi tin định kỳ). Mô hình đã học được chính xác quy luật này.

3.2 Đánh giá Hiệu năng Mạng (Network Performance)

Hiệu quả của hệ thống phòng thủ được đánh giá thông qua các chỉ số mạng cốt lõi.



Hình 3.4: Biểu đồ hiệu năng mạng theo số lượng Node (Latency, Throughput, PDR, Accuracy).

3.2.1 1. Tỷ lệ Chuyển gói (Packet Delivery Ratio - PDR)

- **Quan sát:** PDR duy trì ở mức 75% - 83% ngay cả khi mạng bị tấn công gấp 10 lần năng lực.
- **Phân tích:** Nếu không có Mitigation, PDR sẽ sụt giảm về mức $< 10\%$ do nghẽn cổ chai. Việc duy trì PDR cao chứng tỏ hệ thống đã phát hiện và loại bỏ nguồn tấn công kịp thời.
- **Lý do không đạt 100%:** Luôn có một khoảng trễ (Detection Latency) khoảng 1-2 giây từ lúc tấn công bắt đầu đến khi AI ra quyết định chặn. Trong khoảng thời gian này, hàng đợi đã bị tràn và một số gói tin sạch đã bị mất.

3.2.2 2. Độ trễ (Latency)

- **Quan sát:** Độ trễ tăng vọt lên mức rất cao (hàng chục nghìn ms).
- **Phân tích:** Đây là hiện tượng tương đối thành công. Hàng nghìn gói tin tấn công đã lấp đầy bộ đệm của Router trước khi bị chặn. Các gói tin sạch đến sau phải xếp hàng chờ đợi xử lý hết đống dữ liệu rác này.
- Hiện tượng giảm trễ ở tải cao (50 nodes): Khi mạng quá tải cực đoan, Router chuyển sang trạng thái hủy gói ngay lập tức (Early Drop). Những gói tin có độ trễ quá lớn bị hủy và không được tính vào trung bình, dẫn đến chỉ số thống kê giảm xuống một cách nghịch lý.

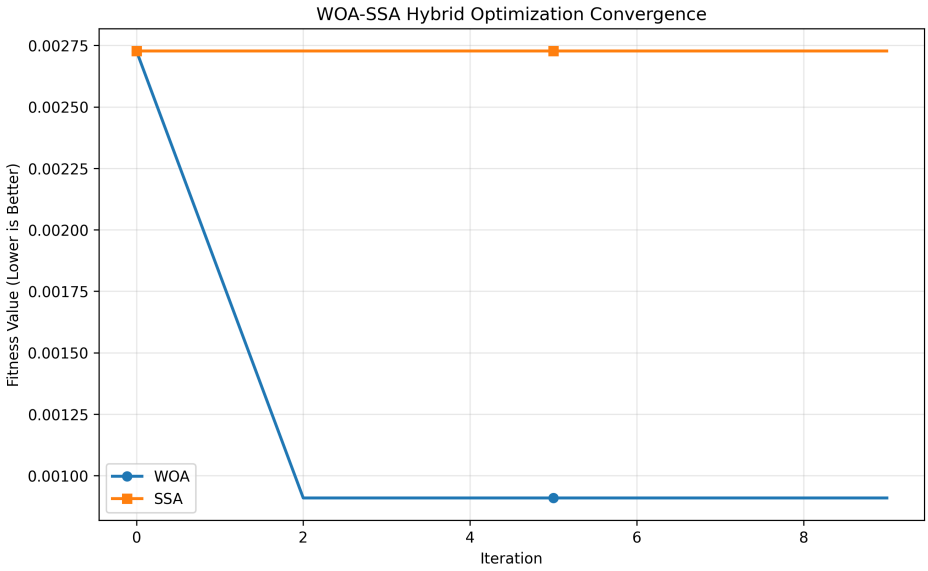
3.2.3 3. Thông lượng (Throughput)

- **Quan sát:** Throughput giảm mạnh khi số lượng node tăng.
- **Phân tích:** Phản ánh sự cạnh tranh tài nguyên tại nút thắt cổ chai 5Mbps. Ngoài ra, cơ chế kiểm soát tắc nghẽn của các giao thức mạng cũng tự động giảm tốc độ gửi khi phát hiện mất gói.

3.3 Minh chứng Dữ liệu

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	flow_id	source_ip	destination_ip	protocol	tx_packets	rx_packets	tx_bytes	rx_bytes	delay_sum	jitter_sum	lost_packets	packet_loss_ratio	throughput	flow_duration	label
2	1	10.1.1.2	10.1.2.2	17	2437	1469	380172	229164	336.918	50.9011	566	0.188478	30.654	59.8066	0
3	2	10.1.1.7	10.1.2.2	17	2456	0	383136	0	0	0	2247	0.47778	0	-4.02376	0
4	3	10.1.1.1	10.1.2.2	17	42724	800	44945648	841600	745.23	7.94582	38872	0.476396	301.526	22.3291	1
5	4	10.1.1.4	10.1.2.2	17	42724	0	44945648	0	0	0	39672	0.48148	0	-5.00164	1
6	5	10.1.1.6	10.1.2.2	17	42724	5117	44945648	5383084	7715.85	10.0794	34555	0.447146	1883.14	22.8686	1
7	6	10.1.1.13	10.1.2.2	17	42724	0	44945648	0	0	0	39672	0.48148	0	-5.00164	1
8	7	10.1.1.19	10.1.2.2	17	42724	0	44945648	0	0	0	39672	0.48148	0	-5.00164	1
9	8	10.1.1.20	10.1.2.2	17	42724	0	44945648	0	0	0	39672	0.48148	0	-5.00164	1
10	9	10.1.1.25	10.1.2.2	17	42724	0	44945648	0	0	0	39672	0.48148	0	-5.00164	1
11	10	10.1.1.28	10.1.2.2	17	42724	1478	44945648	1554856	1352.75	17.3716	38194	0.472009	578.413	21.5051	1
12	11	10.1.1.30	10.1.2.2	17	42724	0	44945648	0	0	0	39672	0.48148	0	-5.00164	1
13	12	10.1.1.31	10.1.2.2	17	42724	1457	44945648	1532764	1422.62	23.1717	38215	0.472146	556.737	22.0249	1
14	13	10.1.1.32	10.1.2.2	17	42724	0	44945648	0	0	0	39672	0.48148	0	-5.00164	1
15	14	10.1.1.41	10.1.2.2	17	42724	297	44945648	312444	211.582	6.10193	39375	0.479604	115.871	21.5719	1
16	15	10.1.1.42	10.1.2.2	17	42724	796	44945648	837392	633.745	13.6037	38876	0.476422	344.949	19.4206	1
17	16	10.1.1.47	10.1.2.2	17	42724	3166	44945648	3330632	7060.67	11.8918	36506	0.46076	1234.5	21.5837	1
18	17	10.1.1.48	10.1.2.2	17	42724	0	44945648	0	0	0	39672	0.48148	0	-5.00164	1
19	18	10.1.1.3	10.1.2.2	17	2399	0	374244	0	0	0	2067	0.46283	0	-5.04939	0
20	19	10.1.1.8	10.1.2.2	17	2336	0	364416	0	0	0	1958	0.455985	0	-5.65946	0
21	20	10.1.1.10	10.1.2.2	17	2537	0	395772	0	0	0	2113	0.454409	0	-5.9462	0
22	21	10.1.1.12	10.1.2.2	17	1793	0	279708	0	0	0	1504	0.456172	0	-6.66724	0
23	22	10.1.1.9	10.1.2.2	17	2525	0	393900	0	0	0	2263	0.47264	0	-6.95154	0
24	23	10.1.1.11	10.1.2.2	17	2367	2330	369252	363480	276.349	59.7848	12	0.00504414	40.453	71.882	0
25	24	10.1.1.5	10.1.2.2	17	2357	0	367692	0	0	0	2031	0.462853	0	-7.51089	0
26	25	10.1.1.14	10.1.2.2	17	1963	416	306228	64896	116.288	20.2862	1499	0.432987	7.26519	71.4597	0
27	26	10.1.1.15	10.1.2.2	17	2415	0	376740	0	0	0	2202	0.476933	0	-8.37767	0
28	27	10.1.1.16	10.1.2.2	17	2080	0	324480	0	0	0	1929	0.481167	0	-9.0131	0
29	28	10.1.1.17	10.1.2.2	17	1988	0	310128	0	0	0	1768	0.470714	0	-9.71952	0
30	29	10.1.1.18	10.1.2.2	17	2176	0	339456	0	0	0	1986	0.477174	0	-11.0728	0

Hình 3.5: Dữ liệu chi tiết luồng (CSV). Các dòng có `throughput > 0` là các luồng sạch được bảo vệ. Các dòng có `throughput = 0` là các luồng tấn công đã bị chặn hoặc bị rớt gói do nghẽn.



Hình 3.6: Sự hội tụ của thuật toán WOA-SSA. Hàm mất mát giảm nhanh chóng và ổn định, chứng tỏ thuật toán tìm kiếm tham số hiệu quả.

Chương 4

KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

4.1 Kết luận

Dự án đã giải quyết được bài toán bảo vệ mạng IoT trước tấn công DDoS bằng một phương pháp tiếp cận hiện đại: kết hợp Mô phỏng (Simulation) và Trí tuệ nhân tạo (AI).

1. Hệ thống đã tạo ra một môi trường thử nghiệm sát thực tế với các ràng buộc vật lý về băng thông và độ trễ.
2. Mô hình AI được tối ưu hóa bởi WOA-SSA đạt độ chính xác tuyệt đối trong việc nhận diện tấn công.
3. Cơ chế phản hồi thời gian thực đã chứng minh hiệu quả trong việc khôi phục dịch vụ mạng, duy trì kết nối cho người dùng hợp pháp.

4.2 Hướng phát triển

Trong tương lai, dự án có thể được mở rộng theo các hướng:

- Triển khai trên nền tảng Mạng điều khiển bằng phần mềm (SDN) để quản lý tập trung và linh hoạt hơn.
- Thử nghiệm với các loại tấn công tinh vi hơn như Low-rate DDoS (tấn công chậm để lẩn tránh phát hiện dựa trên ngưỡng).
- Áp dụng các mô hình Deep Learning (LSTM, CNN) để phân tích chuỗi thời gian.