Enhancing Network Security with Artificial Intelligence (AI)

Using DHCP Snooping and DAI

Hà Trọng Thắng

Faculty of Informatics, East Asia University of Technology

*Email: thanght@eaut.edu.vn

Abstract

The implementation of DHCP Snooping combined with Dynamic ARP Inspection (DAI) helps eliminate the risk of MAC address (physical address) and IP address (logical address) spoofing, preventing attackers from stealing data, while providing monitoring and detection capabilities for computer network attack behaviors.

However, this combination still has some limitations during operation, such as the detection of abnormalities or errors that can lead to network disconnections, causing system disruptions.

This research proposes a solution that applies artificial intelligence (AI) in combination with the implementation of DHCP Snooping and Dynamic ARP Inspection (DAI) to enhance computer network security more effectively.

Keywords: *AI, ARP Spoofing, DHCP Snooping, Dynamic ARP Inspection (DAI)*

1. Introduction

The rapid development of information technology has created a diverse ecosystem of interconnected devices, providing exceptional convenience for users. In this context, computer networks serve as the backbone, forming a crucial infrastructure for global connectivity, data transmission, and information exchange.

The exponential increase in connected devices and data traffic has driven continuous research in computer networking, particularly in the fields of security and information safety. Today, computer networks are not only a means of communication but also an essential component in various sectors, including business, education, healthcare, and media.

In Vietnam, cybersecurity has witnessed significant developments in recent years:

+ Number of cyberattacks: In 2024, over 659,000 cyberattacks were recorded, with 46.15% of organizations and enterprises experiencing at least one attack [1].

+ Increasing sophistication of attacks: Cyberattacks are becoming more advanced and complex, necessitating urgent measures to enhance security for internal networks, including LANs.

 DOI: https://doi.org/10.65153/80gm9r35

Raising awareness and investing in robust cybersecurity solutions are critical to protecting data, ensuring system stability, and maintaining the continuous operation of organizations and enterprises.

1.1. DHCP protocol (Dynamic Host Configuration Protocol):

As a network management protocol that simplifies IP address management and improves network performance, DHCP also carries many security risks if not properly protected, as it lacks a strong authentication mechanism.

One of the security vulnerabilities that can be exploited in DHCP is the DHCP Rogue attack. This is a method where attackers create a fake DHCP server connected to the LAN with the goal of assigning incorrect IP addresses to connected devices, causing service disruptions (DoS - Denial of Service), or redirecting users to a fake website. When users enter sensitive data on this website, all information will be recorded for attackers to use [2][3].

1.2. ARP protocol (Address Resolution Protocol):

ARP is an important protocol belonging to the Data Link Layer in the TCP/IP model. ARP functions to map IP addresses (logical addresses) to MAC addresses (physical addresses) by sending an ARP request as a broadcast packet over the network. The destination host with an IP address matching the request will respond with a unicast packet containing its MAC address [4].

However, ARP lacks an authentication mechanism, making it vulnerable to exploitation in sophisticated LAN attacks such as denial of service (DoS) or intercepting and redirecting data between two devices without detection MITM (Man-in-the-Middle) through ARP spoofing techniques [5].

2. Problem solving

This research paper outlines the DHCP and ARP protocols, the security vulnerabilities associated with them, and proposes a method of applying artificial intelligence (AI) combined with the implementation of DHCP Snooping and Dynamic ARP Inspection to mitigate risks and ensure a more secure network.

2.1. Network security with DHCP Snooping:

To address security vulnerabilities in computer networks related to DHCP, this research applies the DHCP Snooping technical solution, a set of techniques aimed at improving DHCP

network security. When a DHCP server assigns IP addresses to clients in a LAN, DHCP Snooping can be configured on a switch to monitor and control DHCP packets. This mechanism only allows clients with valid IP and MAC addresses to access the network.

By implementing DHCP Snooping techniques, computer network security can be enhanced by distinguishing between *Trusted Ports* and *Untrusted Ports*. This mechanism helps prevent clients from receiving IP addresses from a rogue DHCP server, while protecting the security of data and information on the network [2].

If a DHCP packet is received from a Trusted Port, the switch will allow the packet to be forwarded without being blocked.

If a DHCP packet is received from an Untrusted Port and it is identified as a packet from a DHCP server, the switch will block that packet.

DHCP Snooping Rate-Limiting is a mechanism that limits the number of DHCP packets sent through an interface. If the number of packets exceeds the set threshold, that port will transition to the err-disabled state (permanently disabling the interface) until it is manually restored. This can cause inconvenience for network administrators, as they have to identify the disabled port and restore it for the system to function normally again [6].

2.2. Network security with Dynamic ARP Inspection (DAI):

To prevent ARP Spoofing and eliminate the risk of MAC and IP address spoofing, this research proposes applying Dynamic ARP Inspection (DAI) techniques to secure the network, helping to prevent ARP Spoofing attacks by inspecting and verifying ARP packets before they are forwarded within the network.

Specifically, DAI works by monitoring and filtering ARP packets on the switch. It uses two main methods to authenticate ARP packets:

+ Verification using the DHCP Snooping Binding Table: When DAI is configured, the switch checks ARP packets and compares them with the DHCP Snooping Binding Table to ensure that the IP and MAC addresses in the ARP packet match the information in the DHCP Snooping Binding Table. If they do not match, the ARP packet will be blocked.

+ Classification of *Trusted Ports* and *Untrusted Ports*: with *Trusted Ports*, these ports allow sending and receiving ARP packets without inspection. This is usually applied to ports connected to other switches or ports connected to servers. With *Untrusted Ports*, these ports

 DOI: https://doi.org/10.65153/80gm9r35

will inspect all ARP packets sent from connected devices. If a forged ARP packet is detected, it will be immediately blocked. This is usually applied to ports connected to users such as PCs, laptops, and IoT devices [7].

However, this technique still has some limitations during operation, such as the detection of abnormalities or errors that can lead to disconnections, causing network system disruptions.

Therefore, this research proposes a solution to integrate artificial intelligence (AI) to assist in control and decision-making.

2.3. Network security with Artificial Intelligence (AI):

In the network model, there is a Monitoring (AI) computer that uses AI to act as a network monitoring system, helping to control DHCP Snooping and DAI (Dynamic ARP Inspection) operations within the network system. The Monitoring (AI) computer functions as an IDS/IPS to detect and respond to suspicious packets.

The Monitoring (AI) computer is installed with network and AI libraries such as:

- **scapy**: Used for capturing DHCP and ARP packets.
- **pandas**: Used for storing the valid MAC-IP table.
- **sklearn**: Machine Learning library (Scikit-Learn), used for AI to detect network attacks with the Random Forest model for packet classification [8][9].
- **joblib**: Helps to optimize processing performance and storage of the AI model.

With the use of these libraries, the monitoring program is built with modules, as follows:

- **scan_system**: Scans and collects MAC addresses, IP addresses, packet types (valid or attack) on the system and saves the data to the *dataset.csv* file for later AI training. The structure of the *dataset.csv* file is shown in *Table 1*. The execution time runs from several tens of minutes to several hours to have enough data.

MAC	IP	Packet Type (Label)
AA:BB:CC:DD:EE:FF	192.168.10.10	0 (Valid)
11:22:33:44:55:66	192.168.10.200	1 (Attack)

Table 1. Structure of the *dataset.csv* file

Tập 1, Số 1, 2025 DOI: https://doi.org/10.65153/80gm9r35

+ Explanation of the *dataset.csv* file structure:

The table represents the structure of the dataset.csv file, which is used for training an AI model to detect valid and attack packets.

- MAC address: The MAC address of the packet sender.
- IP address: The source IP address of the packet.
- Packet Type (Label): The classification of the packet: **0 (Valid)** for normal traffic and **1 (Attack)** for malicious traffic.

+ For example, in the table above:

- The packet with MAC address AA:BB:CC:DD:EE:FF and IP 192.168.10.10 is recorded as valid (0).
- The packet with MAC address 11:22:33:44:55:66 and IP 192.168.10.200 is recorded as an attack (1).
- The AI model will be trained on this dataset to predict whether a new packet is an attack.

- **train_ai**: Is run first to train the Random Forest model to predict valid/attack packets. Saves the model to the model.pkl file that the check_packet module will use to check packets.
- **packet_capture**: Is the main program, captures packets and calls other modules: If a DHCP packet is captured, it calls dhcp_snooping for processing. If an ARP packet is captured, it calls arp_inspection to check for validity.
- **dhcp_snooping**: Stores the MAC-IP mapping from the DHCP Offer packet and maintains a valid MAC-IP table and provides the *is_valid_mac_ip()* function for other modules to use.
- **arp_inspection**: Checks if the ARP packet is valid, if any anomalies are detected, it calls the check_packet module for AI evaluation.
- **check_packet**: Loads the trained AI model (*model.pkl*), checks if the packet has signs of an attack, if so, it sends a command to block the MAC/IP to the switch. The program runs continuously until the Ctrl+C key combination is used to stop.

 DOI: https://doi.org/10.65153/80gm9r35

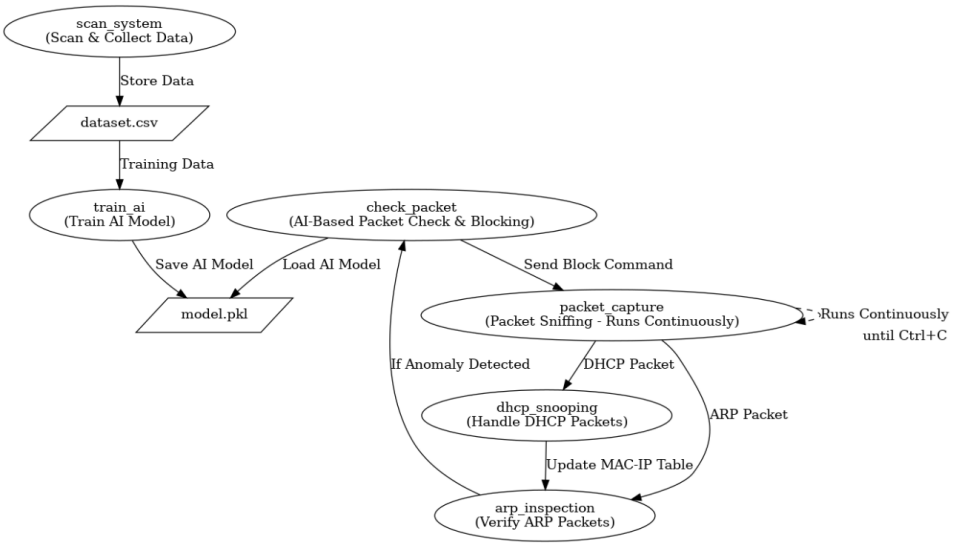

Figure 1. Workflow diagram of the modules

2.4. Network model deployment and system testing

In this research, simulations on GNS3 are used to emulate the network model, a Kali-Linux computer is used to perform experimental attacks. The *yersinia* and *ettercap* tools are used to simulate DHCP Rogue and ARP spoofing attack types.

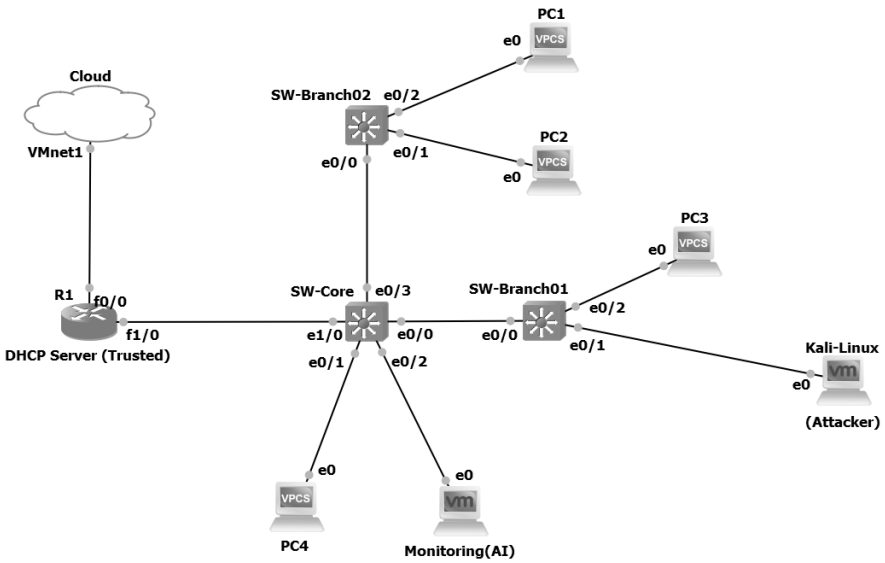

Figure 2. LAN network model

The network model includes:

- Cisco switch: Configured with DHCP Snooping and DAI.
- Monitoring (AI) computer (Ubuntu): Monitors DHCP and ARP packets, detects attacks.

Tập 1, Số 1, 2025 DOI: https://doi.org/10.65153/80gm9r35

- Client (VPCS): Receives IP from DHCP Server.
- Attacker (Kali Linux): Performs DHCP Spoofing and ARP Spoofing attacks.

System operation description:

1. Packet capture: The Monitoring (AI) computer runs Python using scapy to listen for DHCP and ARP packets.
2. DHCP packet authentication: Checks if the client is valid (based on the DHCP Snooping table).
3. ARP Spoofing detection: Checks if the ARP from the client is valid.
4. AI-Powered analysis: If any anomalies are detected, AI determines if it is an attack.
5. Command execution: If there are signs of an attack, the Monitoring (AI) computer sends a telnet command to the switch to block packets or reduce traffic, depending on the number of violating packets. AI decides whether to reduce traffic (Restrict) if the violation level is low or shutdown to completely block the port if there are too many violations. This ensures that the network system still operates but is not affected by attacks.

2.4.1. Security configuration:

To configure security mechanisms on the devices and perform data collection and training for AI, this process is carried out according to the algorithm steps outlined below.

Algorithm for network attack prevention:

Step 1: Configure the router (R1) as a DHCP Server.

Step 2: Enable DHCP Snooping on SW-Core and SW-Branch01, SW-Branch02.

Step 3: configure Trusted Ports and Untrusted Ports to prevent rogue DHCP servers.

Step 4: Limit the transfer rate of packets from Untrusted Ports to 10 packets per second to prevent flooding attacks.

Step 5: Enable Dynamic ARP Inspection (DAI) on all switches to prevent ARP spoofing.

Step 6: Configure port mirroring (SPAN - Switch Port Analyzer) on SW-Core to send all traffic to Monitoring (AI).

Step 7: The **scan_system** module scans the system to capture packets

 DOI: https://doi.org/10.65153/80gm9r35

Step 8: Train AI on the Monitoring (AI) computer.

Monitoring (AI) continuously inspects packets from the mirrored port.

Step 9: If a packet violates DHCP Snooping or ARP Inspection rules, Monitoring (AI) classifies the threat level:

if the number of violating packets is below the threshold (<= 100) then

Monitoring (AI) connects to the switch via Telnet and restricts bandwidth on the violating port.

else the number of violating packets exceeds the threshold (> 100) then

Monitoring (AI) sends a shutdown command to disable the violating port.

end if

Step 10: Before shutting down, Monitoring (AI) verifies the dataset.csv for legitimacy:

if IP address from an untrusted port does not match any entry in *dataset.csv*

then

Drop packets and shut down the port.

else if the MAC address from an untrusted port does not match any entry in *dataset.csv* then

Drop packets and shut down the port.

end if

In the algorithm above, the **scan_system** module scans the system to capture packets transmitted via the UDP protocol on the following ports: Port 67 (UDP): Captures DHCP Discover, Offer, Request, and ACK packets. Port 68 (UDP): Captures DHCP Reply packets. And ARP: Captures ARP Request and ARP Reply packets. The LAN topology is designed as shown in *Figure 2*, and the system performs packet capture scanning at intervals of 35 minutes..

The system performance on the monitoring (AI) computer is operating under a light load, specifically: CPU usage at 19.6%, RAM at 2.62GB / 7.17GB, and Swap at 0KB / 3.78GB. The number of processes includes 128 tasks and 433 threads. Thus, the test model has not yet affected the performance of the network system. This result is shown in *Figure 3*.

 DOI: https://doi.org/10.65153/80gm9r35

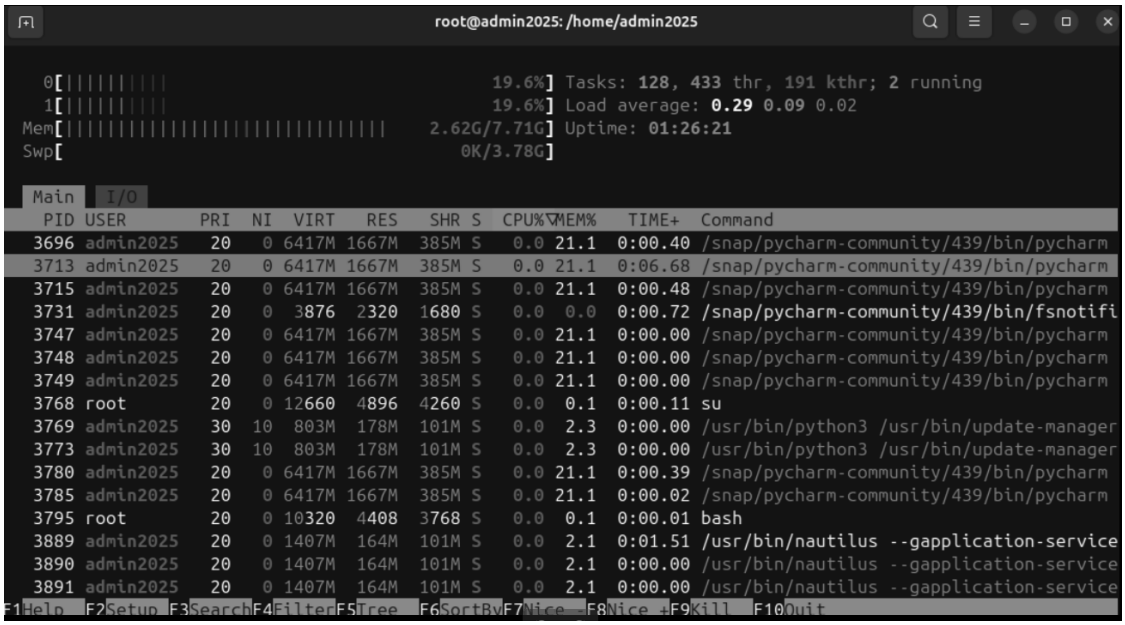

Figure 3. System performance.

2.4.2. System testing

To test the system, two scenarios are needed to check the operation of DHCP Snooping and Dynamic ARP Inspection, with each attack scenario recording log entries to review the system status when needed and to check the operation of the Monitoring (AI) computer when choosing to send telnet commands to the switch to block packets or reduce traffic, depending on the number of violating packets. AI decides whether to reduce traffic (Restrict) if the violation level is low (smaller than or equal to 100) or shutdown (greater than 100) to completely block the port if there are too many violations.

Scenario 1: DHCP Snooping detects a rogue DHCP Server

As an attacker, the Kali Linux computer will use the *yersinia* tool to send rogue DHCP packets with the following command: *yersinia dhcp -attack 1*

When this command is executed, packets are continuously sent until the network is affected or devices are unable to receive an IP address from a valid DHCP server.

To show the logs recorded on the switch device SW-01, the command executed on switch SW-01: *SW-01#show port-security*

The log displays information about Port Security on switch SW-01 as shown in *Figure 4*. The Security Action status when a security violation is detected with port Et0/0 has been

Shutdown due to 105 violations. Port Et0/1 is in Restrict mode, has recorded 31 violations but has not been shutdown, only logs and discards invalid packets.

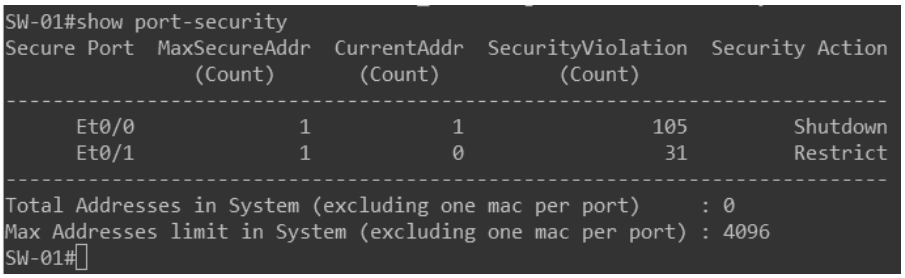

Figure 4. Check the Port-Security status on the switch

The SW-Core switch log shows that the device is recording a Telnet connection (vty1) from the Monitoring (AI) computer at IP address 192.168.20.18, performing port state changes to Restrict/Shutdown, and that it was remotely configured via a Telnet session (vty1) at different times on February 24 , as shown in the *Figure 5*.

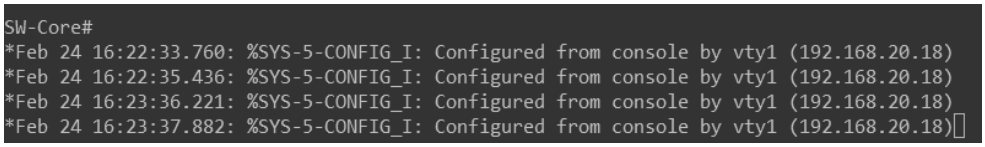

Figure 5. Telnet connection from the Monitoring (AI) computer to the switch

Scenario 2: ARP Spoofing (Man-in-the-Middle Attack)

In this attack scenario, the attacker uses the ettercap tool on Kali-Linux to perform an ARP attack: *arpspoof -i eth0 -t 192.168.20.100 192.168.20.11*

The result of this command is that it will perform an ARP spoofing attack, causing the machine at 192.168.20.100 to send packets to the attacking machine instead of to the machine at 192.168.20.11, which can lead to disruption, eavesdropping, or manipulation of network communications.

Surveillance Interface on a **Monitoring (AI)** computer:

The results indicate that the monitoring system successfully detected an ARP spoofing attack and applied port-security mechanisms on the switch to protect the network. The system identified a malicious ARP packet with MAC address: 00:50:79:66:68:04 and IP address: 192.168.20.11

 DOI: https://doi.org/10.65153/80gm9r35

The Monitoring AI analyzed the packet and issued a warning, determining that it was likely an attack. The RESTRICT mode of port-security was successfully activated to mitigate the threat, as shown in the *Figure 6*.

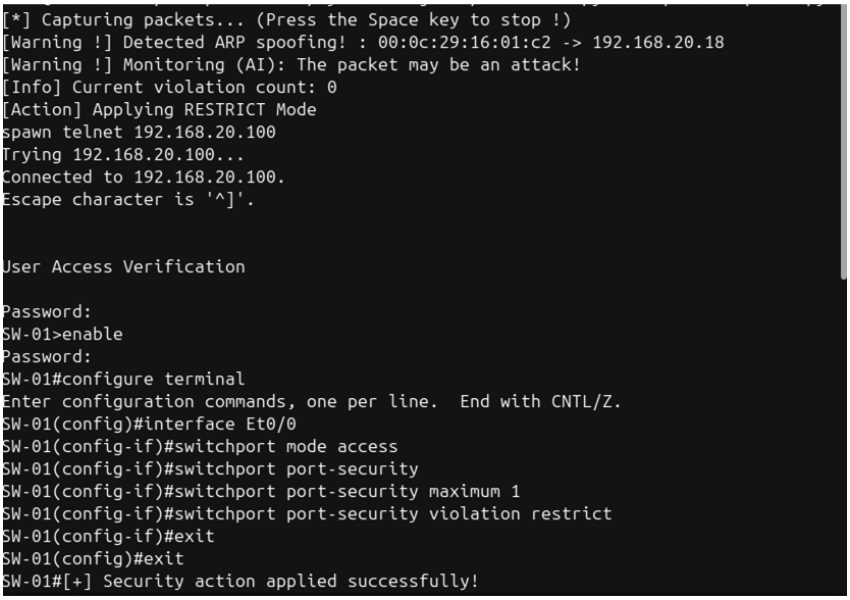

Figure 6. Current monitoring status of the Monitoring (AI) computer

In order to select the optimal AI model, the research compared several AI models, including: Random Forest, SVM, and XGBoost. Use the dataset collected from scan_system.

With the test results of 443 data samples in the *dataset.csv*, evaluation and performance comparison, evaluate the models using metrics: Accuracy, Precision, Recall, F1-score

ROC-AUC Score, as shown in the *Table 2*.

Model	Accuracy	Precision	Recall	F1-score	ROC-AUC
Random Forest	**1.000000**	**1.0**	**1.0**	**1.000000**	**1.000000**
SVM	0.988764	0.5	1.0	0.666667	0.994318
XGBoost	0.988764	1.0	0.0	0.000000	0.500000

Table 2. Evaluation and performance comparison

+ Explanation of the metrics in the performance comparison criteria:

- TP (True Positive): The number of samples that are actually 1 (Positive) and the model correctly predicts as 1.

 DOI: https://doi.org/10.65153/80gm9r35

- FP (False Positive): The number of samples that are actually 0 (Negative), but the model incorrectly predicts as 1.
- FN (False Negative): The number of samples that are actually 1 (Positive), but the model incorrectly predicts as 0.
- TN (True Negative): The number of samples that are actually 0 (Negative) and the model correctly predicts as 0.

o Accuracy: The ratio of correct predictions to the total data. When the data is balanced between valid and attack samples.

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}}$$

o Precision: In attack alerts, how many are correct.

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}}$$

o Recall: Among actual attack packets, how many are detected.

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}}$$

o F1-score: A balance between precision and recall.

$$\text{F1} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$

o ROC-AUC: The ability to distinguish between valid and attack packets.

$$\text{X} - \text{axis: False Positive Rate (FPR)} = \frac{\text{FP}}{\text{FP} + \text{TN}}$$

$$\text{Y} - \text{axis: True Positive Rate (TPR)} = \text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}}$$

+ The analysis of each model, as shown in *Figure 7*:

o Random Forest achieves a perfect score (1.0) in all metrics, indicating flawless classification on the test set.

o SVM has high accuracy (0.9887) and Recall = 1.0, but Precision = 0.5 → meaning it correctly predicts all positive samples but also has many false positives.

o XGBoost has Precision = 1.0, but Recall = 0.0, meaning it only predicts the negative class and fails to detect any positive samples.

Tập 1, Số 1, 2025 DOI: https://doi.org/10.65153/80gm9r35

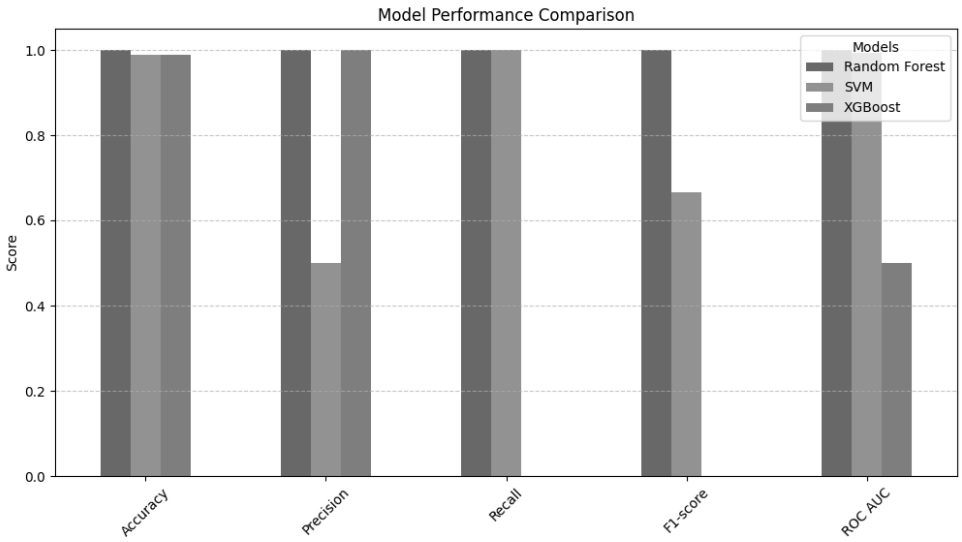

Figure 7. Model performance comparison

Moreover, the Random Forest model has several advantages, such as:

- Prevents overfitting: Random Forest is a powerful machine learning model due to its ability to create multiple independent decision trees and combine them, which helps minimize overfitting.
- Handles imbalanced data: In security problems, data is often imbalanced (e.g., very few attack instances compared to valid behavior).
- Flexibility: The model can work with various types of data (such as network data, system logs, or data from security sensors).

Based on these results, the research selected the Random Forest model, as it is a powerful tool in network security due to its ability to analyze and detect threats accurately and effectively.

3. Conclusion

This research proposes a solution that applies artificial intelligence (AI) using the Random Forest training model to predict valid or attack packets, while also providing threshold values to determine the port's state as restrict or shutdown. In addition, the solution combines DHCP Snooping with Dynamic ARP Inspection (DAI) to enhance security effectiveness for computer networks. This helps minimize risks when a port is shut down due to DHCP Snooping or DAI errors, avoiding misidentification situations that cause system interruptions, requiring administrators to manually intervene to restore the port to the Up state.

 DOI: https://doi.org/10.65153/80gm9r35

This system acts as an intelligent firewall, enhancing the security capabilities of computer networks while ensuring enterprises operate effectively and efficiently by providing reliability and reinforcing network solidity.

References

[1] Khánh An (2024), Hơn 659.000 vụ tấn công mạng cơ quan, doanh nghiệp năm 2024

Website: https://laodong.vn/ban-doc/hon-659000-vu-tan-cong-mang-co-quan-doanh-nghiep-nam-2024-1439390.ldo [Accessed on February 10, 2025]

[2] Pradana DA, Budiman AS (2021) The DHCP Snooping and DHCP Alert Method in Securing DHCP Server from DHCP Rogue Attack. IJID (International Journal on Informatics for Development). 2021;10(1):38-46.

[3] Andi Purnomo (April 2024). Implementation of DHCP Snooping Method to Improve Security on Computer Networks, Bit-Tech (Binary Digital - Technology), Vol.6, No.3

[4] Ren, Ming, Yanhui Tian, Siqi Kong, Dali Zhou, and Danping Li (2020). An Detection algorithm for ARP man-in-the-middle attack based on data packet forwarding behavior characteristics, *IEEE 5th Information Technology and Mechatronics Engineering Conference (ITOEC)*, pp. 1599-1604. IEEE, 2020.

[5] Hao, Guo, and Guo Tao (2009). Principles and Protection Against Man-in-the-Middle Attacks Based on ARP Spoofing. JIPS 5, no. 3 (2009): 131-134.

[6] Dara YC, Hariadi F, Lede PA (May 2023). Analysis of Network Security System Implementation Using DHCP Snooping and Switch Port Security Methods, JURNAL TEKNIK INFORMATIKA INOVATIF WIRA WACANA. 16;1(3):187-96.

[7] Hannah A. S. Adjei, Mr Tan Shunhua, George K. Agordzo, Yangyang Li, Gregory Peprah, Emmanuel S. A. Gyarteng (February 2021). SSL Stripping Technique (DHCP Snooping and ARP Spoofing Inspection), ICACT2021, ISBN 979-11-88428-07-6

[8] Sebastian Raschka, Vahid Mirjalili (September, 2017). Python Machine Learning: Machine Learning and Deep Learning with Python, scikit-learn and TensorFlow, 2nd Edition, Packt Publishing.

[9] https://scikit-learn.org/stable/index.html [Accessed on January 5, 2025].