A Study on ARP Attack Prevention Strategies Leveraging Software-Defined Networking

Xizi Wang

School of Computer and Software, Jincheng College, Sichuan University

Absrtact: ***With the continued advancement of cloud computing, growing attention has been directed toward dynamic networking, a trend that has in turn accelerated the development of Software-Defined Networking (SDN). SDN enables flexible control over traffic within local area networks (LANs), allowing for rapid detection of device anomalies resulting from various network attacks. By facilitating real-time traffic management, SDN provides a robust foundation for network security. Among the most vulnerable threats to local networks is the ARP attack, which, if successfully executed, can disrupt or completely halt communication. Through a detailed analysis of the ARP protocol and its operational principles, this paper identifies the primary types of ARP attacks. In response, an ARP attack prevention mechanism based on the SDN architecture is proposed. By enabling comprehensive monitoring and analysis of overall network traffic conditions, the proposed approach facilitates rapid response to ARP attacks and supports the implementation of effective countermeasures, thereby ensuring the normal operation of network devices within the LAN.***

Keywords: ARP attacks on local networks; MAC table; OpenFlow protocol; SDN technology.

1. INTRODUCTION

With the development of the network, the issue of cybersecurity is getting more and more attention. When the network protocol is established, the original intention is to make the communication between the network more convenient, but did not consider the security of the network, and then with the development of the network, there are a lot of things that threaten the network security. ARP attack is the most common and most problematic attack in the current local network. Once the local network is attacked by ARP, if it is not dealt with in time, it will not only make users unable to connect to the network normally, causing network congestion, but also cause data leakage. SDN is a new dynamic network architecture, which makes network management more convenient by combining data layer and control layer. Based on the analysis of the principle of ARP attack, this paper proposes a SDN based ARP attack prevention. Tang et al. (2020) focused on optimizing shallow-angle grating couplers for indium phosphide devices, providing critical insights for enhancing vertical emission efficiency in photonics systems .

The application of machine learning and deep learning has emerged as a transformative force. In human-computer interaction, Sun (2025) proposed adaptive interfaces powered by machine learning to deliver personalized user experiences, addressing the growing demand for tailored digital interactions . For structural health monitoring, Wu et al. (2025) developed a multi-level transfer learning approach for small-sample detection of concrete surface cracks in high-rise buildings, overcoming data scarcity challenges in practical engineering scenarios . In natural language processing, Xie et al. (2024) introduced a Conv1D-based model to advance legal citation text classification, improving accuracy in multi-class legal document processing , while Xu et al. (2024) leveraged YOLOv5 for real-time detection of crown-of-thorns starfish, demonstrating the potential of deep learning in marine ecological surveillance . Xu et al. (2024) also explored strategies to enhance user experience and trust in large language model (LLM)-based conversational agents, a key consideration for the widespread adoption of AI chatbots . In medical imaging, Tian et al. (2024) enhanced the U-Net model with GSConv modules and ECA attention mechanisms for more accurate brain tumor segmentation, contributing to improved diagnostic support . Cybersecurity and privacy preservation in federated learning have also garnered significant attention. Deng and Yang (2025) proposed multi-layer defense strategies to mitigate membership reasoning attacks, addressing critical privacy vulnerabilities in distributed learning frameworks . In digital economy and marketing, Yi (2025) developed a contextual bandits-with-knapsacks approach for real-time fair-exposure ad allocation, promoting equitable opportunities for small and medium-sized businesses (SMBs) and underserved creators , while Zhao et al. (2025) optimized deep learning models for dynamic market behavior prediction, enabling more agile business decision-making . Yang et al. (2025) designed a full-cycle intelligent risk control system for online lending, integrating AI-driven closed-loop management across pre-loan, mid-loan, and post-loan stages to enhance credit security . Shen et al. (2025) applied the whale optimization algorithm to financial payment fraud detection, improving the efficiency of anomaly detection in transaction data , and Ren (2024) introduced a feature

fusion-based model for smoking detection, advancing public safety monitoring systems . Ximeng and Yiming (2026) proposed an offline conservative reinforcement learning framework for transaction authorization, balancing fraud risk reduction and customer experience optimization , while Zhou (2025) developed a collaborative filtering model based on user behavior for digital precision distribution of automotive social media content in private domain platforms . Wensi (2026) explored AI-assisted marketing content generation for non-standard industrial automation solutions, streamlining content creation in niche B2B sectors . In data management and graph analytics, Yang et al. (2021) presented Huge, an efficient and scalable subgraph enumeration system, addressing performance bottlenecks in large-scale graph data processing , and Ukey et al. (2022) proposed an efficient k-nearest neighbor (kNN) join algorithm for dynamic high-dimensional data, enhancing the responsiveness of data analysis applications

2. SDN AND ARP

2.1 SDN architecture

Software defined network (SDN) is a kind of dynamic network innovation architecture, which manages the network centrally through the application of network controller and network installation device. OpenFlow's core technology separates and separates the network device plane of the switch from the data plane, the switch is only responsible for high-speed forwarding, and all control and management is fully centralized in the controller, so that the traffic of the entire network can be controlled flexibly.

The architecture of software defined network is divided into 3 layers, from the surface layer to the bottom layer respectively for the management plane, control plane, data forwarding plane. The management plane includes various applications, the control plane is the most important part of SDN, and the foundation facility plane is mainly responsible for digital processing and state collection. SDN adopts a centralized control plane, which mainly uses the control and forwarding interface to control the equipment, so it has the characteristics of separation of control and forwarding.

2.2 OpenFlow protocol

In order to implement the architecture of the SDN network, it is necessary to create a communication interface standard, and this interface is OpenFlow, which exists between the SDN controller and the data forwarding plane. The OpenFlow controller belongs to the control plane and forwards to the data plane device through the OpenFlow switch of the southbound interface. The OpenFlow standard protocol allows the controller to directly access a forwarding plane.

A flow is a transport path that is packeted by OpenFlow. According to the needs of the operator, you can set the functions through the software to make a flow table information, OpenFlow road table will have these information. By creating a secure connection between the control and the forwarding plane, OpenFlow provides the contents of the control waylist to the network settings on the forwarding plane.

2.3 Principle of ARP attack

2.3.1 Principle of ARP

ARP (Address Resolution Protocol) Address resolution protocol. In the TCP / IP environment, each host is assigned an IP address. Logical address & mdash; — This is the internationally recognized way to mark the host's address. In order for it to be transmitted within the local network, both parties need to know each other's MAC addresses. However, there is a problem with how the IP address is converted to the MAC address. Then there is a protocol specifically responsible for solving this problem, this protocol is called the ARP protocol, this protocol belongs to the network layer. ARP can find out the MAC address of this host in the same local network according to the IP address of the destination host given by the user. The destination address is searched by sending ARP packets, which are encapsulated in MAC frames for transmission. In every computer installed with TCP / IP, there will be an ARP table, placed in the ARP table is the corresponding MAC address for each IP address. In this way, when two hosts A and B want to communicate with each other, they need to know the MAC address, and they first check the ARP table. If there is a corresponding MAC address in the ARP Table, then they can communicate directly; However, if the corresponding mapping relationship is not found, the IP address that you want to communicate will be filled in the MAC frame, and the host will broadcast in the local network. The source IP

address is its own IP address, the destination IP is the IP address that wants to communicate, the source MAC is its own MAC address, the destination address is filled in 0 because it is not known how much. When other hosts find that their IP address is the same as the destination IP address in the ARP message, they will send an ARP Reply to fill in their MAC address to respond. But this response is unicast because it knows the destination IP and MAC address.

2.3.2 Types of ARP attacks

In fact, the ARP attack virus we call is not a virus in the traditional sense, but a general term for the spread of the vulnerability of the ARP protocol. Common attack methods are ARP spoofing attack and flooding attack, which pose a serious threat to network security. ARP is based on the complete trust of hosts in the network, so it has serious security flaws. The ARP address map table relies on the dynamic update of the cache in the computer, and only stores the recently used address map relationship. A host on a LAN can send an ARP Reply message at will, and when another host receives a Reply message, it will not detect whether the message is a valid address, but will be recorded directly in the host's ARP table. Then when the malicious person impersonates the destination host to conduct an ARP Reply, the host that receives the Reply response is also unknown.

If an attacker sends a forged ARP Request or ARP Reply message, the core exchange machine such as important equipment has been refreshing its ARP table. Then the really useful real ARP mapping will be refreshed by the false mapping, and after a period of time, the ARP table on the exchange will be full of false mapping. The true and effective ARP mapping relationship has long been refreshed. Then when the real host comes to communicate, it cannot find the corresponding MAC address, which may cause network channel blocking and poor communication quality of the network, which is called ARP Flood Attack.

ARP deception is when a host sends an ARP broadcast package, all hosts within the LAN receive the package, the ARP attacker receives the corresponding information, and the ARP actor impersonates other devices to perform the ARP response. This information contains the IP address and the host's MAC address. When the host receives the ARP Reply packet in the local network, There is no way to confirm that, but to store the corresponding IP-MAC mapping relationship directly in the ARP table, so that when a host wants to communicate with this host, the MAC address viewed is false and is always communicating with a false host. That is, an ARP attacker can send false and inauthentic ARP Reply messages to all source hosts, deceive hosts by copying MAC addresses, and make it difficult for the messages sent by the source host to reach the target host or to reach a non-target host.

3. SDN PROTECTION AGAINST ARP ATTACKS

3.1 Traditional ARP prevention

Now the traditional anti-ARP attack softwares such as ARP firewall, 360 and so on are all belong to the application layer, but the ARP attack is launched from the data link layer, so the anti-ARP attack softwares are not fundamentally improved. Now commonly used technology is to set static ARP address binding, IP address and MAC address to carry out the corresponding binding. In this case, the ARP table will not be dynamically updated, and the static ARP table exists in every device, so there will be no malicious attack, so that the ARP table has been refreshed. Setting the corresponding port binding on the switch is similar to this technology. If a large number of malicious and false IP addresses are found to be continuously coming in from a single port number, causing traffic congestion to the device or making normal data communication impossible for the device, Then set the corresponding port binding, bind the MAC address to the port, so that the port can only pass through a specific MAC address. In this case, even if there is a malicious fake IP attack, it is not possible to enter the device through this port.

3.2 ARP Prevention under SDN

Traditional prevention cannot implement measures according to the current cyber environment. Now the rise of SDN allows us to flexibly control network traffic, so ARP prevention based on SDN will be more flexible. The SDN architecture consists of three layers: application plane, control plane, and infrastructure plane. The infrastructure plan contains basic network facilities, including equipment supporting the OpenFlow protocol. The network control plane includes the detection and prevention of ARP attacks, the statistical management of network traffic and so on. The main functions of the infrastructure plane are data processing, and status collection, so consider a traffic monitoring. Set a basic traffic incoming and outgoing size, and when the traffic reaches the trigger condition, there is reason to suspect a large number of malicious message attacks, known as flood attacks,

and an ARP attack is detected and blocked for each incoming packet. The detection and blocking of ARP attacks is to detect digital packet, and if it meets the conditions, take relevant measures to the received packet to prevent it from causing deeper damage to the network. By using the characteristics of SDN controller, when the exchange machine is attacked by ARP, it can quickly react and implement corresponding measures. The specific process is shown in Figure 1 SDN architecture.

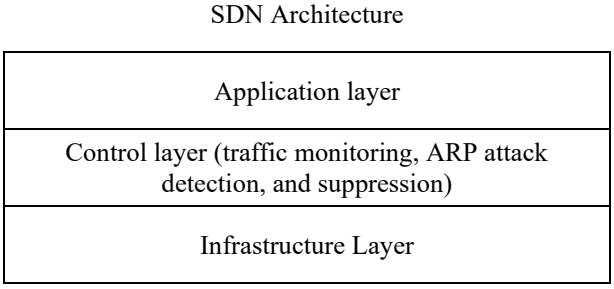

Figure 1: SDN architecture

When the ARP attack is detected, every incoming digital packet will be detected. If it is not ARP, it will be processed by other exchanges. If it is an ARP message, it will parse the source IP, MAC address and destination IP address as well as the port number entered. Based on the extracted source IP and MAC address, query the switch's ARP table to compare. If the IP sends too many ARP packets within a certain period of time, it will be judged an ARP attack, and the packet will be discarded, restricted at the corresponding port number, and a warning to the switch to promptly alert the administrator. The specific workflow is shown in Figure 2 for ARP attack detection.

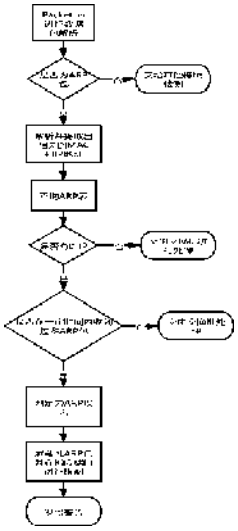

Figure 2: ARP attack detection

4. CONCLUSION

We must have a very deep understanding of the ARP protocol. As a trusted and widely used protocol, ARP was originally designed to be flawed, and it is this design flaw that has led to the current ARP attacks and the flood of ARPs. Nowadays, with the rapid growth of cloud computing, the need for dynamic network sources is increasing, which drives the growth of software defined network (SDN). After analyzing the principles and types of ARP attacks as well as traditional measures to prevent attacks,In this paper, how to use SDN to detect ARP attack and prevent ARP attack in computer system network and telecommunication system is proposed, so as to improve the efficiency and security of the network.

REFERENCES

[1] Tang, Y., Kojima, K., Gotoda, M., Nishikawa, S., Hayashi, S., Koike-Akino, T., ... & Klamkin, J. (2020). Design and Optimization of Shallow-Angle Grating Coupler for Vertical Emission from Indium Phosphide Devices.
[2] Sun, L. (2025, November). Adaptive Interfaces for Personalized User Experience: A Machine Learning Approach. In Proceedings of the 2025 International Conference on Artificial Intelligence and Sustainable Development (pp. 457-462).
[3] Wu, J., Luo, L., & Liao, N. (2025). Small-Sample Object Detection of Surface Cracks in Concrete Structures of High-Rise Buildings via Multi-Level Transfer Learning. Innovation & Technology Advances, 3(2), 57–72. https://doi.org/10.61187/ita.v3i2.262
[4] Xie, Y., Li, Z., Yin, Y., Wei, Z., Xu, G., & Luo, Y. (2024). Advancing Legal Citation Text Classification A Conv1D-Based Approach for Multi-Class Classification. Journal of Theory and Practice of Engineering Science, 4(02), 15–22. https://doi.org/10.53469/jtpes.2024.04(02).03
[5] Xu, G., Xie, Y., Luo, Y., Yin, Y., Li, Z., & Wei, Z. (2024). Advancing Automated Surveillance: Real-Time Detection of Crown-of-Thorns Starfish via YOLOv5 Deep Learning. Journal of Theory and Practice of Engineering Science, 4(06), 1–10. https://doi.org/10.53469/jtpes.2024.04(06).01
[6] Xu, Y., Gao, W., Wang, Y., Shan , X., & Lin, Y.-S. (2024). Enhancing user experience and trust in advanced LLM-based conversational agents. Computing and Artificial Intelligence, 2(2), 1467. https://doi.org/10.59400/cai.v2i2.1467
[7] Tian, Q., Wang, Z., & Cui, X. (2024). Improved Unet brain tumor image segmentation based on GSConv module and ECA attention mechanism. arXiv preprint arXiv:2409.13626.
[8] Deng, X., & Yang, J. (2025, August). Multi-Layer Defense Strategies and Privacy Preserving Enhancements for Membership Reasoning Attacks in a Federated Learning Framework. In 2025 5th International Conference on Computer Science and Blockchain (CCSB) (pp. 278-282). IEEE.
[9] Yi, X. (2025, October). Real-Time Fair-Exposure Ad Allocation for SMBs and Underserved Creators via Contextual Bandits-with-Knapsacks. In Proceedings of the 2025 2nd International Conference on Digital Economy and Computer Science (pp. 1602-1607).
[10] Zhao, S., Lin, Y., Yang, X., Lu, Q., Xue, H., & Jiang, G. (2025). Optimization of Deep Learning Models for Dynamic Market Behavior Prediction. arXiv preprint arXiv:2511.19090.
[11] Yang, X., Xue, H., Hu, Q., & Zhang, Y. (2025, October). Design of a full-cycle intelligent risk control system for pre-loan, mid-loan, and post-loan lending: AI-driven closed-loop management of online credit security. In Proceedings of the 2025 2nd International Conference on Digital Economy and Computer Science (pp. 1022-1027).
[12] Shen, Zepeng, et al. "Research on Application of Whale Optimization Algorithm in Financial Payment Fraud Detection." 2025 4th International Conference on Artificial Intelligence, Internet and Digital Economy (ICAID). IEEE, 2025.
[13] Z. Ren, "A Novel Feature Fusion-Based and Complex Contextual Model for Smoking Detection," 2024 6th International Conference on Communications, Information System and Computer Engineering (CISCE), Guangzhou, China, 2024, pp. 1181-1185, doi: 10.1109/CISCE62493.2024.10653351.
[14] Ximeng, Y., & Yiming, Z. (2026). Offline Conservative RL for Transaction Authorization: Smartly Balancing Fraud Risk and Customer Friction. Journal of Economic Theory and Business Management, 3(1), 1-9.
[15] Zhou, Z. (2025, November). Digital precision distribution strategy for social media content on private domain platforms in the automotive industry: a collaborative filtering model based on user behavior. In Proceedings of the 2025 International Conference on Digital Society and Intelligent Computing (pp. 516-521).
[16] Wensi, L. (2026). AI-Assisted Marketing Content Generation for Non-Standard Industrial Automation Solutions. Journal of Economic Theory and Business Management, 3(1), 18-25.
[17] Yang, Z., Lai, L., Lin, X., Hao, K., & Zhang, W. (2021, June). Huge: An efficient and scalable subgraph enumeration system. In Proceedings of the 2021 international conference on management of data (pp. 2049-2062).
[18] Ukey, N., Yang, Z., Zhang, G., Liu, B., Li, B., & Zhang, W. (2022, August). Efficient knn join over dynamic high-dimensional data. In Australasian Database Conference (pp. 63-75). Cham: Springer International Publishing.