VB-ARP: Boyer–Moore Majority Voting Algorithm Based Defense for ARP Spoofing

S.M. Morsy[1], and Dalia Nashat[2]
[1]Faculty of Computers and Information Technology, The Egyptian E-Learning University, Giza, Egypt
[2]Department of Information Technology, Faculty of Computers and Information, Assuit University, Assiut, Egypt

A man-in-the-middle attack (MITM) is considered one of the main significant concerns for many network security. MITM involves an unauthorized third party secretly accessing communication between endpoints to intercept or modify transmitted data. The most common and dangerous network attack is Address Resolution Protocol (ARP) spoofing-based MITM. ARP spoofing-based MITM attack exploits ARP protocol weakness to associate the attacker's MAC address with the IP address for an intended legitimate host. Several defense schemes have been proposed to counteract ARP spoofing, but they possess limitations, such as dependence on static entries in the cache table or a central server that is susceptible to being a single point of failure.

This paper presents VB-ARP, a novel ARP spoofing attack defense scheme. VB-ARP is designed to identify defective ARP packets by using a voting mechanism based on the Boyer-Moore majority (BMMV) algorithm. First, we collect all ARP packets which received from the original ARP packets and voting reply packets to create the suspect list. Then, identifying the ARP Spoofing attacks is carried out by analyzing ARP packets, applying BMMV, and calculating the probabilities of the suspect list entries. In addition, VB-ARP prevents ARP spoofing attacks by transmitting a trap packet to the suspected hosts. Also, preventing adding entries to the cache table without ensuring their validity, and blocking detected attacks.

***Index Terms*—Man-in-the-middle, ARP, ARP Spoofing, Boyer-Moore Algorithm.**

I. Introduction

MITM attack is a type of cyberattack where an attacker intercepts the communication between two parties secretly to alter or steal the transmitted data. This can be easily accomplished on the local area and wi-fi networks [1], [2]. Typically, the attacker may be located by various means, like eavesdropping, intercepting, and modifying network traffic or on a wifi connection. Also, it may impersonate a trusted website, device, or service [3], [4]. The main goal of MITM attacks is gaining access to sensitive or personal data, such as passwords or financial information. It is a severe security threat and can be challenging to identify; even the attacker often can remain hidden and unnoticed [5], [6].

Spoofing is a kind of impersonation technique in which a malicious device (Attacker) can spoof a host, server, or any legitimate device. Spoofing a host, especially, can have serious concern for computer networks. One of the most crucial types of spoofing is to poison the ARP cache, which is a severe and dangerous form of MITM attack. The MITM attack is able to monitor and modify all the transferred data between two trusted hosts on the network to fill the cache table with malicious IP and MAC associations [7], [8].

The ARP protocol is one of the most essential protocols for LAN communication. It is extensively used whenever a device wants to communicate with other devices in the network. At the same time, the MAC address of the destination host is required for transmitting packets between hosts. To get the destination MAC address, the host asks about it by sending a request as a form of broadcasting to other hosts on the LAN whenever the intended MAC address does not exist in the cache table. Therefore, it waits for a reply from the legitimate host that owns this MAC address. The ARP protocol has leaked in the authentication, so it is possible to accept more than one reply from any number of hosts, whether this host is legitimate or not. As a result, that makes it vulnerable to many attacks [9]–[13].

In the ARP protocol, operating systems maintain a cache table of ARP replies from different hosts to minimize the number of ARP requests that are sent as broadcast packets. When a host receives any ARP reply, it will automatically update its ARP cache table with the new <IP, MAC> association entry. It is acknowledged that the <IP, MAC> mapping that received in the ARP reply is used to update the ARP cache table, even if that sender's IP address is already present in the table [14], [15].

Due to various reasons, ARP spoofing is pivotal in network attacks, particularly ARP spoofing-based MITM attacks. First, the ARP spoofing makes it hard to distinguish ARP cache table pairs with spoofed mappings from legitimate ones. Second, the ARP spoofing causes all transmitted packets to be directed to an incorrect destination. Finally, ARP spoofing makes detecting sources of malicious mapping extremely challenging and highly complicated because it binds the host IP address with attacker MAC address [16]–[19].

This paper presents VB-ARP, a new detection scheme based on a voting mechanism. The main objective of VB-ARP is to provide ARP authentication by eliminating the ARP poisoning problem. However, the major security issue for the ARP protocol is that it easily binds the attacker's MAC address with a victim's IP address. So, it must work as expected by effectively acting as a virtual translator between the host IP address and its MAC address. Another main objective of this new scheme is to provide reliable address resolution functionality, detect all aspects of ARP spoofing, and then prevent them.

Manuscript received August 20, 2024; revised January 7, 2025. Corresponding author: Dalia Nashat (email: dnashat@aun.edu.eg).

Therefore, the proposed scheme provides a defense technique against ARP attacks, which are considered a crucial concern in the computer network. The main contribution of this scheme is that it is backward compatible with the current ARP protocol, and it avoids a single point of failure issue. Moreover, the proposed scheme does not need any upgrading in Ethernet switches or modification of DHCP, and it proposed a fully automated process, and there is no headache for Admin.

A. Boyer–Moore Majority Vote Algorithm

The Boyer-Moore majority vote (BMMV) algorithm [20] is a voting algorithm that is managed in a linear time and can be used to identify a majority element in a given set of elements. By default, the element that occurs more than $N/2$ is the majority element, where N is the number of items in the sequence. The algorithm initiates by creating two variables: candidate and counter. In the beginning, the initial value of the counter variable is zero because no candidates have been chosen yet. Then, it selects the first element in the sequence as a candidate, and the counter increments to one. For all remaining items in the sequence, if the element is equal to the candidate, then the counter is incremented by one. Otherwise, every time a new element is not equal to the candidate, the counter is decremented. In case that the counter is decremented and reaches zero, it chooses the following element as a new candidate [21]–[23].

For example if we have the following sequences $2, 2, 1, 1, 3, 2, 2$ the algorithm works as shown in Figure 1.

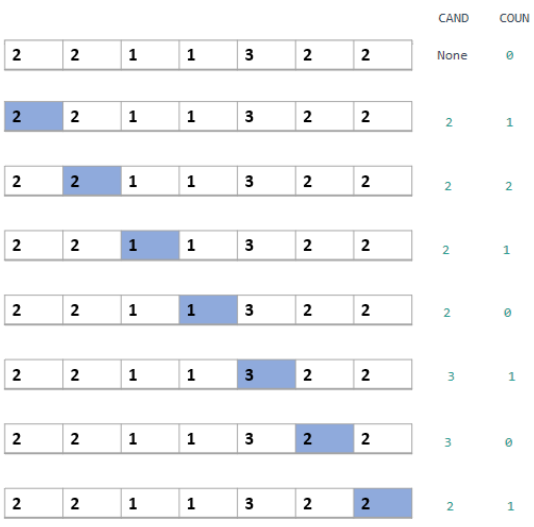

Fig. 1. Boyer–Moore majority algorithm

In this scheme, we employed the Boyer-Moore majority vote algorithm to determine the trusted MAC address that has more than half of the votes.

II. Related Work

Nam et al. [24] investigated and developed a collaborative approach to protect hosts against ARP cache table attacks, especially MITM attacks. This approach uses fair voting among the neighboring host nodes. The approach works whenever the number of legitimate hosts is greater than the number of malicious hosts. The concept behind this approach is to protect a host by resolving the mapping processes between IP-to-MAC addresses through the fair voting mechanism. To achieve fairness in voting, they used the uniform transmission capability of Ethernet LAN.

Authors in [25] proposed a technique that is backward-compatible with ARP to detect and prevent MITM-based ARP poisoning. This technique is based on ICMP and voting over a centralized server (CS). Whole packets that pass within a network are monitored and analyzed by CS. Also, CS sends a trap ICMP packet and analyzes the terms of the ICMP reply to determine the identity of the host. Legitimate CS can be chosen by voting from other hosts to prevent attackers. Moreover, CS maintains two tables, primary and secondary, in which data is stored for a specific time for validating <IP, MAC>pairs.

A client/server-based intrusion detection system (CSIDS) was proposed in [26] to detect and prevent ARP poisoning attacks instead of working with the original stateless ARP protocol. This protocol (CSIDS) depends on a client/server model for exchanging and controlling the resolution messages between the system and its members. CSIDS must send a CSIDS control message to the server for each suspicious packet to verify whether the host addresses are in its cache table unless it uses the voting technique for each host in the LAN. Upon receiving the answers, the server replies to the requested client with a positive or negative packet. They noticed that the voting process takes time, which leads to an increase in the lag between sending the query packet to the server and waiting for the response from the server.

Authors in [27] presented an algorithm that depends on sniffing and analyzing all incoming ARP packets. The basic step for detecting conflicts between addresses involves comparing the real MAC address with the response MAC address of the sniffed ARP packet. Once the ARP packet is captured, it is analyzed to extract the source MAC address of the sniffed packet and the legitimate sender's physical address. If a conflict is found between the legitimate MAC address and the response MAC address, it indicates the occurrence of an ARP attack. Also, this paper relies on static entries to prevent ARP spoofing.

The research paper [28] proposes a new approach to prevent ARP spoofing based on man-in-the-middle attacks in local networks. The proposed method uses a mathematical model to detect and prevent unauthorized access to network communication. The model is based on identifying malicious behavior by analyzing network packets and comparing them to legitimate traffic patterns. The proposed approach is effective in preventing ARP spoofing-based MITM attacks, and it is also shown to be computationally efficient and scalable in large networks. Moreover, this article concludes that the proposed method could be a valuable addition to existing network security measures for preventing man-in-the-middle attacks.

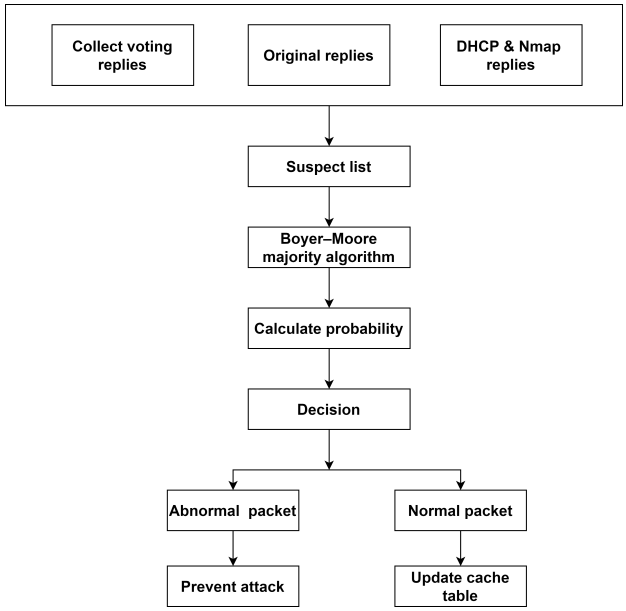

Fig. 2. VB-ARP overall architecture

III. Proposed Scheme

A. Overall Scheme Architecture

The proposed detection scheme, referred to as VB-ARP, must be deployed in each host within the computer network. The main idea behind VB-ARP is exploring the presence of ARP spoofing attacks. Identifying the ARP spoofing attack attempts is performed by checking the validation of reply packets and leveraging a neighbor's voting. Our scheme classifies pakcets into two cases, which are called normal and spoofing cases. The normal case means that each incoming packet must contain the same destination MAC address in its field. On the contrary, ARP attacks aim to associate the destination IP address with a malicious MAC address, causing the packet to be transmitted to the attacker instead of a legitimate host. So, in spoofing cases, the incoming packets may contain different MAC addresses [29] or some of them have a different MAC address. Also, we should consider that spoofing can easily poison the cache table by request or gratuitous packets. Figure 2 shows the overall architecture of our scheme, which is applied in local area networks.

B. VB-ARP Design

The proposed scheme involves analyzing ARP packets to defend a network against ARP spoofing. We have presented the overall architecture in the last subsection, which we will go into further detail about below.

- The processing packet technique in each host is responsible for managing replies flowing from several inputs. Replies are classified into three types depending on their source (i.e., Original replies, DHCP-Nmap replies, and Voting replies). Original replies are responses from a legitimate host sent by an authentic ARP. Voting is an essential step in the scheme. It is expected that the host with the intended IP address will provide a response packet once the host sends a broadcast request to determine the destination MAC address. The primary requirement for our VB-ARP's voting mechanism is that each neighbor contains the desired IP address in their cache table, sending a response. Also, we can get the intended MAC address from the DHCP server and Nmap tool. The second step is generating a suspect list. It consists of all received replies associated with this request for detecting the malicious packet efficiently.
- Since the BMMV algorithm finds the element that occurs more than $N/2$ from a specific sequence of elements, in our proposed scheme, BMMV is used to find the pair that has the majority of occurrences in the suspect list. To apply the BMMV algorithm to get the most occurred pair, the sequence of elements is equivalent to the suspect list and pairs equivalent to the candidates.
- After getting the most occurred element, calculate its probability. In the normal case, the probability of all packets must be equally likely, which is calculated by $1/R$ and R the total number of packets received.
  - If equal to 1, this means all packets are normal. Therefore, update the cache table of a host with the legitimate pair.
  - Otherwise there is a abnormal packets, which means attacker attempts to poison cache table.
- It must be ensured that the inserted pair in the ARP table is legitimate to prevent attacks from poisoning it. So, prevention is carried out once the attack has been detected. To prevent an attack must know its IP first. We get the attacker's IP address via the Nmap tool because it associates its MAC address with the victim's IP address. Then, VB-ARP assigns a host randomly to send a trap broadcast request to ask about the attacker's MAC address after getting it according to its IP address.
- After determine malicious MAC address. All host notified with attacker's information.

IV. Experiments and Results

To evaluate the practicality of our proposed scheme, we implement it through a VMware workstation 16 pro. The VMware workstation consists of nine virtual machines: a DHCP server, Admin, Host A, Host B, Host C, Host D, Host E, Host F, and an Attacker. Ubuntu desktop version 20.04.2.0 is the virtual machine operating system. To verify the effectiveness and creditability of the proposed scheme. All details for each component in the experiment are listed in Table I.

- **Detection phase:**
  In case a host sends an ARP request, other hosts with the desired MAC address in their cache table should send a voting reply. Voting replies differ from the original ones sent from the intended destination. The original reply in normal cases must be only one packet. Also, it is considered an essential entry to determine the attacks. All types of replies are added to the suspect list and displayed as a report shown in Figure 3. This report displays all

TABLE I
VB-ARP NETWORK COMPONENTS

Name	IP Address	MAC Address
Host A	192.168.1.11	00:0c:29:9c:48:e9
Host B	192.168.1.8	00:0c:29:21:41:b7
Host C	192.168.1.10	00:0c:29:d4:bc:47
Host D	192.168.1.12	00:0c:29:9e:d6:b5
Host E	192.168.1.51	00:0c:29:bf:b0:75
Host F	192.168.1.13	b0:cf:50:ea:a8:99
Admin	192.168.1.40	00:0c:29:be:64:d1
DHCP Server	192.168.1.16	00:0c:29:72:cd:a5
Attacker	192.168.1.55	00:0c:29:ef:fe:e3

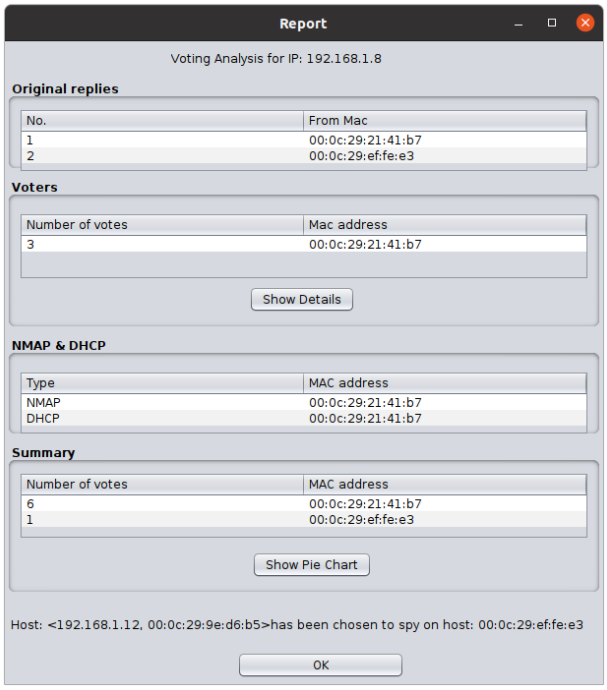

Fig. 3. Replies report

details of replies when host A sends a broadcast request to ask about host B's MAC address.
VB-ARP report views original and voter replies, number of voters, DHCP-Nmap, and summary. The report contains the suspect list. Then, calculate the probability of MAC addresses. In the suspect list, there are two MAC addresses. The probability of 00:0c:29:21:41:b7 is 0.85714, and the of 00:0c:29:ef:fe:e3 is 0.1428. Therefore, an alert message appears to notify about the presence of an attack. The details of vote messages are described in figure 4. Finally, a pie chart to display the overall results 5.

- **Prevention phase:**
The first host, "192.168.1.12," has been chosen to spy on the host with the MAC address "00:0c:29:ef:fe:e3". The selected host sends an ARP request, as shown in figure 6. Once the attacker sends a malicious reply, all hosts are notified.

Now, we present a comparison of ARP spoofing detection schemes shown in table II. Several factors stand out to measure scheme efficiency, such as compatibility with ARP

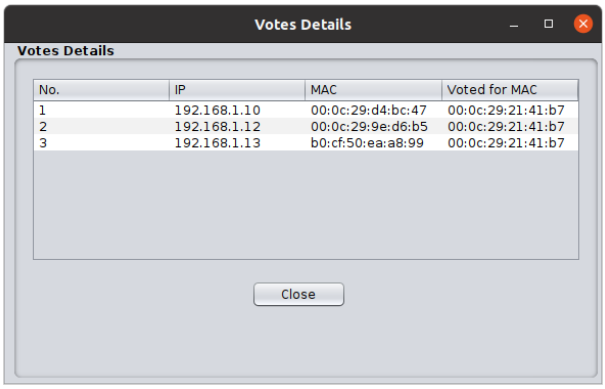

Fig. 4. Voting replies

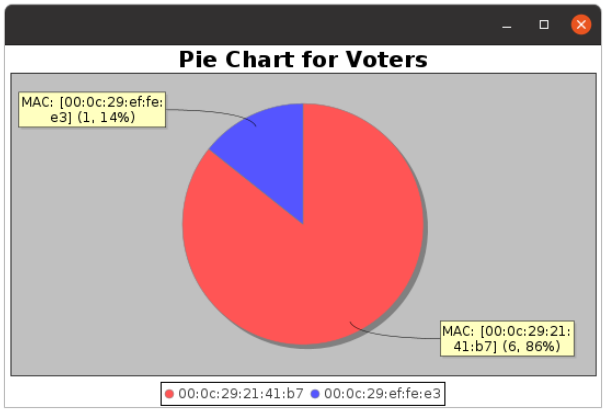

Fig. 5. Overall result by pie chart

and depending on the server. The comparison shows that VB-ARP doesn't rely on a server to avoid a single point of failure issue. In addition, it is effective to forbid adding malicious entries in the cache table and deals with graitious ARP packets.

V. CONCLUSION

This paper presented an approach for efficiently detecting ARP spoofing attacks called VB-ARP. Our scheme is based on the BMMV algorithm and voting concept. As demonstrated, VB-ARP can efficiently and accurately detect ARP attacks by identifying malicious MAC addresses that differ from legitimate ones. Also, the detection is done without any false positive or negative, and computational complexity is O(n). Moreover, it is able to prevent attackers and keep the validation of the cache table. We plan to extend our schemes to detect other types of ARP spoofing (i.e., DDoS and hijacking attacks). Also, we will adapt our scheme to run on all platforms to be general schemes against all kinds of ARP attacks.

REFERENCES

[1] M. B. Muzammil, M. Bilal, S. Ajmal, S. C. Shongwe, and Y. Y. Ghadi, "Unveiling vulnerabilities of web attacks considering man in the middle attack and session hijacking," *IEEE Access*, 2024.
[2] M. M. Inuwa and R. Das, "A comparative analysis of various machine learning methods for anomaly detection in cyber attacks on iot networks," *Internet of Things*, vol. 26, p. 101162, 2024.

TABLE II
COMPARISON BETWEEN VB-ARP AND RELATED SCHEMES

Scheme	Ref. [30]	Ref. [31]	Ref. [25]	VB-ARP
Static/Dynamic entries	yes	yes	yes	Yes
Single point of failure	yes	No	yes	No
Defense against gratuitous ARP	N/A	N/A	N/A	Yes
Drawbacks	Modify ARP, DHCP protocols, and key Distributer	Modify ICMP packets	ARP and ICMP protocols	Install VB-ARP paltform

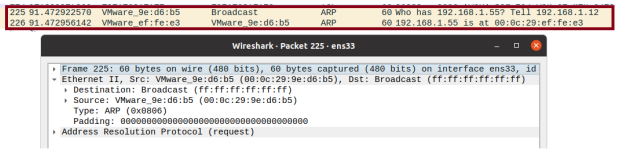

Fig. 6. Spy broadcast

[3] R. Goenka, M. Chawla, and N. Tiwari, "A comprehensive survey of phishing: mediums, intended targets, attack and defence techniques and a novel taxonomy," *International Journal of Information Security*, vol. 23, no. 2, pp. 819–848, 2024.

[4] E. Alalwany and I. Mahgoub, "Security and trust management in the internet of vehicles (iov): Challenges and machine learning solutions," *Sensors*, vol. 24, no. 2, p. 368, 2024.

[5] M. Conti, N. Dragoni, and V. Lesyk, "A Survey of Man In The Middle Attacks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2027–2051, 2016.

[6] M. Lehto, "Cyber-attacks against critical infrastructure," in *Cyber Security: Critical Infrastructure Protection*, pp. 3–42, Springer, 2022.

[7] S. Morsy and D. Nashat, "D-ARP: An Efficient Scheme to Detect and Prevent ARP Spoofing," *IEEE Access*, 2022.

[8] M. R. F. Eslava, J. C. H. Lozada, M. H. Bolaños, and J. S. Gutiérrez, "Firewall system for the internet of things," in *International Congress of Telematics and Computing*, pp. 73–85, Springer, 2023.

[9] C. P. David, "An ethernet address resolution protocol," *RFC 826*, 1982.

[10] S. Bhirud and V. Katkar, "Light weight approach for IP-ARP spoofing detection and prevention," in *2011 Second Asian Himalayas International Conference on Internet (AH-ICI)*, pp. 1–5, IEEE, 2011.

[11] B. Prabadevi and N. Jeyanthi, "Security solution for ARP cache poisoning attacks in large data centre networks," *Cybernetics and Information Technologies*, vol. 17, no. 4, pp. 69–86, 2017.

[12] H. Xi, "Research and application of ARP protocol vulnerability attack and defense technology based on trusted network," in *AIP Conference Proceedings*, vol. 1820, pp. 090019.1—-090019.7, AIP Publishing LLC, 2017.

[13] B. Prabadevi and N. Jeyanthi, "A framework to mitigate ARP sniffing attacks by cache poisoning," *International Journal of Advanced Intelligence Paradigms*, vol. 10, no. 1-2, pp. 146–159, 2018.

[14] D. Hercog and D. Hercog, "Arp protocol," *Communication Protocols: Principles, Methods and Specifications*, pp. 321–322, 2020.

[15] G. Song, J. Hu, and H. Wang, "A novel frame switching model based on virtual mac in sdn," *International Journal of Information Security*, vol. 22, no. 3, pp. 723–736, 2023.

[16] G. Jinhua and X. Kejian, "ARP spoofing detection algorithm using ICMP protocol," in *2013 International Conference on Computer Communication and Informatics*, pp. 1–6, IEEE, 2013.

[17] N. Saxena and N. S. Chaudhari, "Secure-AKA: An efficient AKA protocol for UMTS networks," *Wireless personal communications*, vol. 78, no. 2, pp. 1345–1373, 2014.

[18] S. Jadhav, A. Thakur, S. Nalbalwar, S. Shah, and S. Chordia, "Detection and mitigation of arp spoofing attack," in *International Conference On Innovative Computing And Communication*, pp. 383–396, Springer, 2023.

[19] M. M. Alani, A. I. Awad, and E. Barka, "Arp-probe: An arp spoofing detector for internet of things networks using explainable deep learning," *Internet of Things*, vol. 23, p. 100861, 2023.

[20] R. S. Boyer and J. S. Moore, "Mjrty—a fast majority vote algorithm," in *Automated reasoning: essays in honor of Woody Bledsoe*, pp. 105–117, Springer, 1991.

[21] Y. Sun, Y. Han, Y. Zhang, M. Chen, S. Yu, and Y. Xu, "Ddos attack detection combining time series-based multi-dimensional sketch and machine learning," in *2022 23rd Asia-Pacific Network Operations and Management Symposium (APNOMS)*, pp. 01–06, 2022.

[22] L. Pike, N. Wegmann, S. Niller, and A. Goodloe, "Copilot: monitoring embedded systems," *Innovations in Systems and Software Engineering*, vol. 9, pp. 235–255, 2013.

[23] S. Jose, T. G. Selvaraj, K. Samuel, J. T. Philip, S. Nanjappan Jothiraj, S. Muthu Swamy Pandian, V. S. Handiru, and E. S. Suviseshamuthu, "Intramuscular emg classifier for detecting myopathy and neuropathy," *International Journal of Imaging Systems and Technology*, vol. 33, no. 2, pp. 659–669, 2023.

[24] S. Y. Nam, S. Djuraev, and M. Park, "Collaborative approach to mitigating ARP poisoning-based Man-in-the-Middle attacks," *Computer Networks*, vol. 57, no. 18, pp. 3866–3884, 2013.

[25] P. Arote and K. V. Arya, "Detection and prevention against ARP poisoning attack using modified ICMP and voting," in *2015 International Conference on Computational Intelligence and Networks*, pp. 136–141, IEEE, 2015.

[26] H. Salim and Z. Li, "A Precise Model to Secure Systems on Ethernet Against Man-In-The-Middle Attack," *IT Professional*, vol. 23, no. 1, pp. 72–85, 2021.

[27] A. Majumdar, S. Raj, and T. Subbulakshmi, "ARP Poisoning Detection and Prevention using Scapy," in *Journal of Physics: Conference Series*, vol. 1911, p. 012022, IOP Publishing, 2021.

[28] H. I. Nasser and M. A. Hussain, "Provably curb man-in-the-middle attack-based arp spoofing in a local network," *Bulletin of Electrical Engineering and Informatics*, vol. 11, no. 4, pp. 2280–2291, 2022.

[29] F. Mvah, V. Kengne Tchendji, C. Tayou Djamegni, A. H. Anwar, D. K. Tosh, and C. Kamhoua, "Gatebasep: game theory-based security protocol against arp spoofing attacks in software-defined networks," *International Journal of Information Security*, vol. 23, no. 1, pp. 373–387, 2024.

[30] D. Bruschi, A. Ornaghi, and E. Rosti, "S-ARP: a secure address resolution protocol," in *19th Annual Computer Security Applications Conference, 2003. Proceedings.*, pp. 66–74, IEEE, 2003.

[31] S. Singh and D. Singh, "ARP Poisoning Detection and Prevention Mechanism using Voting and ICMP Packets," *Indian Journal of Science and Technology*, vol. 11, no. 22, pp. 1–9, 2018.

Sabah M.Morsy Sabah Mahmoud Mohammed Morsy received a Master's degree in network security from the Faculty of Science, Assiut University, Egypt. Since 2022, Sabah has worked as an Assistant Lecturer in the faculty of Computers and information technology at the Egyptian E-learning University. Her research interests include network security, intrusion detection, and Information Security.

Dalia Nashat Dalia Nashat received the Ph.D. degree in networks security from Tohoku University, Japan, in 2010. She was an Assistant Professor in computer science with the Faculty of Science, Assuit University, Assuit, Egypt, from 2010 to 2020, where she is currently an Associate Professor with the Department of Information Technology, Faculty of Computers and Information. She was an Assistant Professor with Taif University, Saudi Arabia, from 2011 to 2014. Her research interests include networks security, intrusion detection, and signal processing.