A Study on Various Schemes for Detection and Prevention of ARP Based Attacks

D Francis Xavier Christopher[a]**, C. Divya**[b]

[a]Director, School of Computer Studies, Rathnavel Subramaniam College of Arts and Science, Coimbatore, Tamilnadu, India

[b]Research Scholar, School of Computer Studies, Rathnavel Subramaniam College of Arts and Science, Coimbatore, Tamilnadu, India

Abstract

Address resolution protocol (ARP) is considered as the essential protocol for the computer communications due to frequent usage in individual as well as organization levels. Though efficient during regular scenarios, the design of ARP has not been designated to tackle malicious hosts. Considering the adverse circumstances, many researchers have developed strategies to improve the effectiveness of ARP by detecting and preventing the malicious attacks including spoofing, Man in the middle (MITM) and Denial of service (DoS) attacks. This paper discusses about the ARP poisoning attacks and focuses on reviewing various mechanisms developed for attack detection and prevention with specified analysis to their advantages. Different attack detection and mitigation methods are evaluated and compared on the basis of important parameters. This study helps in understanding the strategy employed for ARP attack detection and mitigation and developing a framework for improvement.

KEYWORDS— Network Security, Address resolution protocol, spoofing, Man in the middle attack, Denial of service, ARP poisoning

INTRODUCTION

Network security begins with approval of access to information in a network, usually with a username and a password. Network security comprises of the arrangements and approaches received by a network manager to avert and monitor unapproved access, changes in system, or denial of a PC network and network resources [29]. It has turned out to be more important to PC clients, and associations. If this approved, a firewall powers access to strategies, for example, what administrations are permitted for network clients can be accessed. This unapproved access to system may neglect to check potentially harmful data like PC worms or Trojans being transmitted over the network. Anti-virus programming or an intrusion detection system (IDS) can help in identifying the malware [20]. However inconsistency in communications between hosts increases the security issues. There is a significant absence of security techniques that can be effectively actualized in the network innovation. There exists a communication gap between the engineers of security innovation and designers of networks.

Network configuration is a generated procedure that is relies upon the Open Systems Interface (OSI) model [7]. The OSI has a few points of interest when outlining network security. It offers modularity, ease of use, flexibility, and standardization of protocols. The protocols of various layers can be effortlessly joined to make stacks which permit measured improvement. Rather than secure network configuration is certainly not an all-around developed process. There is no approach to deal with the multi-objective nature of security requirements. While considering about network security, it ought to be underscored that the total network is secure, instead of considering only the computers at the end of the communication chain to avoid attacks in hosts [24]. A programmer will focus on the communication channel, get the information, and decode it and reinsert a copy message. While building up a protected network, the essentials should be considered are confidentiality and integrity. However the variety of attacks is still increasing by passing time [17].

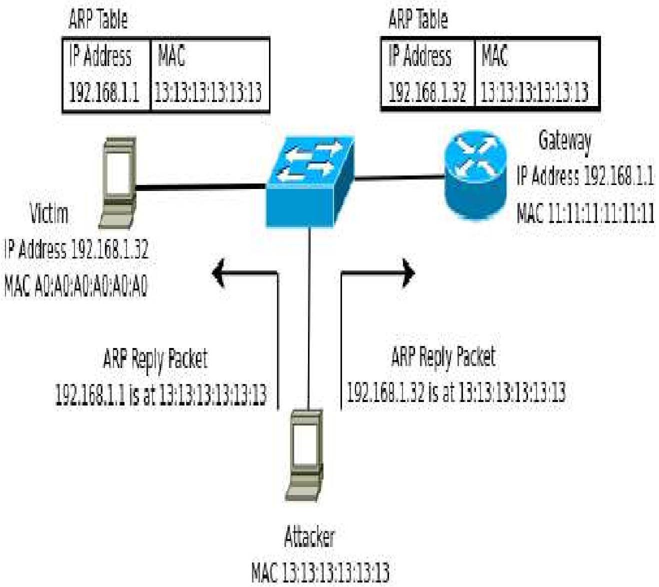

Fig.1. ARP Spoofing/Cache poisoning

The fundamental class of attacks is categorized as active and passive attacks which include spoofing, modification, wormhole, fabrication, denial of services, sinkhole, Sybil, eavesdropping, black hole, rushing attacks, etc. ARP is a broadly utilized communications protocol for determining Internet layer addresses into link layer addresses. ARP spoofing or ARP cache poisoning [23] is a procedure by which an attacker sends spoofed ARP messages onto a LAN. Figure 1 demonstrates the ARP spoofing or ARP cache poisoning attack (Source: [1]).

The fundamental principle behind ARP spoofing is to misuse the absence of authentication in the ARP protocols by sending spoofed ARP messages onto the LAN. ARP spoofing attacks can be initiated from a traded off host on the LAN or from an attacker's machine that is associated specifically to the objective LAN. Mostly, the objective of the attack is to relate the attacker's host MAC address with the IP address of an objective host, so any activity implied for the objective host will be sent to the attacker's host [35].Regularly the attack is utilized as an opening for different attacks, for example, denial of service, man in the middle, or session hijacking attacks. The attacker may assess the packets (spying), while at the same time sending the traffic to the genuine default destination to avoid discovery, alter the information before sending it (man-in-the-middle attack), or dispatch a denial-of-service attack by causing a few or the majority of the packets on the network to be dropped. The attack can only be utilized on networks that employ ARP, and are bound to require the attacker to increase guide access to the LAN to be attacked. There are a few methodologies to mitigate ARP spoofing like utilizing ARP entries and prevention software or securing the operating system [4], [15]. However most strategies fail when the attack gets stronger and hence most prominent methods are sought to be developed. This article aims at reviewing some of the ARP detection and prevention mechanism developed over the years by different scientists and researchers to provide an understanding of these attacks and effective scope for development.

I. ARP SPOOFING ATTACK DETECTION AND PREVENTION MECHANISMS

As discussed above, ARP spoofing is responsible for the cause of many attacks. The research for detecting and preventing against such attacks is a long process exceeding about three decades. There have been various research models that tend to analyze, detect and mitigate ARP spoofing effects. However the ever changing environments and attacks initialization strategies have made it look like the research to find the efficient method is never ending. The varying features of ARP spoofing makes it comfortable for the attackers to avert the prevention mechanisms once they become familiar. Many research works like Zheng and Chenzhong[31], Bruschi et al, [5], Carnutand Gondim[16], Koo et al, [14], etc. have been undertaken to provide secured defense mechanism against ARP spoofing. Some of the most prominent methods developed for this purpose over the years are reviewed in this section in hope of tracing the basic vulnerabilities and perfect mitigation approach for ARP based attacks.

1. Spoofed ARP packets detection in switched LAN networks :Trabelsiand Shuaib[34] developed an efficient mechanism for detecting malicious hosts that performs the ARP spoofing attacks. This mechanism consists of sending first spoofed ARP packets to the network's hosts and then, analyses the collected responses packets to efficiently and accurately identify the spoofing attacks. The mechanism does not degrade the network performance when injecting packets into to the network, since the number of injected packets is relatively very limited. However the major setback of this approach is that the false positive/negative ratio is significantly higher when the hosts use personal firewalls to filter the incoming and outgoing traffic. Lootah et al, [28] introduced a Ticket-based address resolution protocol (TARP) which implements security by distributing centrally issued secure IP/Medium Access Control (MAC) address mapping attestations through existing ARP messages. This model of ARP also reduces cost by as much as two orders of magnitude over existing solutions for security issues in ARP. This model efficiently resolves the lack of authentication and proof of address ownership problems in ARP which has caused a range of serious security vulnerabilities. However this model has not been accepted by the internet community to implementation due to its nature of modifying the ARP features.

2. Research of the ARP spoofing principle and a defensive algorithm: Liu et al, [33] developed a method of ARP cache updating, using switching equipment to control the ARP spoofing attacks. This model has a guard against deception algorithms, to prevent functional efficiency against the ARP attacks. However still this method is not satisfactory and hence requires random algorithms to consider acceding to the future efficiency of algorithms.

3. Principle of and Protection of Man-in-the-middle Attack Based on ARP Spoofing :Haoand Tao [9] analysed the MITM attacks and other ARP spoofing attacks and suggested a protection strategy against them. The solutions suggested are to encrypt the communication data and to bind the switch port such that the attacks can be averted. If a static ARP cache is set and the IP-MAC records are edited manually, the Host will not be able to update the ARP cache even if it receives an ARP response. Thus the MITM can be detected and averted but it cannot be resolved permanently.

4. An analysis on the schemes for detecting and preventing ARP cache poisoning attacks : Neminath et al, [13] developed a discrete event system (DES) approach for detecting and mitigating the ARP spoofing attacks. This approach does not alter the ARP features or any additional constraints while the DES model for the system under normal condition and also under each of the failure conditions. This approach is developed exclusively for network layers as the ARP spoofing in network layer resembles the events of a normal situation and hence it is difficult to trace. Initially, a probe is sent for each ARP request and at least one response is received and selected. Then the possibility of attacks is determined by the spoofed ARP hash tables. However this approach causes more traffic due to probe forwarding for each ARP request which can be reduced only when maintaining separate tables for spoofed and genuine IP-MAC pairs.

5. S-ARP: A secure address resolution protocol : Xing et al, [30] developed a defense mechanism against ARP spoofing attacks using WinPcaP. In this method the process of detection is done by setting filtering rules by filtering mechanisms of the WinPcaP, and the system just captures the ARP packets flowing through the local card, and then sends the packets to the analysis module. The malicious activities are detected at the analysis module. In this module, the IP address of each packet is checked and compared with IP/MAC address connections to trace the adversary. Then the response module sends alerting messages to the systems if the ARP spoofing attacks are identified and the ARP cache table is modified and updated information is stored. This model of ARP spoofing detection seems effective in all LAN connections under adverse situations.

6.The detection and prevention for ARP Spoofing based on Snort :Hou et al, [32] developed an ARP spoofing detection model using Snort. Snort is an open-source, free and lightweight network intrusion detection system which has good expansibility and transplanting ability, and can be used in various environments. However the general Snort has limitation on ARP spoofing detection and hence the authors expanded the Snort pre-processor plug-ins by adding an ARP detection module. This modification significantly improves the ARP spoofing attack detection efficiency of Snort. Though efficient than Snort, this model still lacks dynamic detection mechanism and hence considered to be below par mechanism.

7. An active host-based intrusion detection system for ARP-related attacks and its verification: Barbhuiya et al, [8] developed an active host based intrusion detection system to track the ARP attacks in LAN connections. This host based system works on the adverse environment with constraints like static IP-MAC, modified ARP, variable routes, etc. but has been designed to detect various attack scenarios. This system detects the ARP related attacks namely, malformed packets, response spoofing, request spoofing and denial of service efficiently. However, the major shortcoming of this system is it does not provide diagnosis or prevention methods for which new methods or third-party applications are needed to be employed along with this model.

8. A centralized detection and prevention technique against ARP poisoning : Kumar andTapaswi, [26] developed a centralized system to mitigate ARP spoofing attacks. Along with ARP Central Server (ACS), the centralized system manages and validates the ARP table entries in all hosts to remove the possible inconsistencies. The ACS validates and corrects the poisoned ARP entries of the attacked hosts and hence prevents ARP poisoning in the network. This model allows the backward compatibility to existing networks by utilizing the ARP without new modifications. However, this scheme is susceptible to central point failure, although minor, which will render the network defenceless to ARP poisoning. Similarly, IP exhaustion attack on this system is also untraceable considering the scope of this research scheme.

9. Collaborative approach to mitigating ARP poisoning-based Man-in-the-Middle attacks : Nam et al, [27] proposed and developed a collaborative approach for mitigating the ARP attacks especially the Man-in-the-middle attacks using fairness voting process. This model works on the concept of protecting a node by resolving the mapping processes between IP and MAC addresses through the fair voting method mong the neighboring host nodes. In order to achieve fairness in voting, the uniform transmission capability of the Ethernet connections is employed and found to be better than existing voting schemes. This model is purely efficient as the public key cryptography methods are not required additionally even when the communication is over public Wi-Fi environments. Hong et al, [25] developed a defense mechanism against the ARP spoofing attacks using the cryptography schemes. This mechanism employed does not require changes to the network protocol of ARP or require additional equipment. Instead it utilizes AES and RSA encryption algorithms to improve the attack mitigation. Additionally, this mechanism automatically renews the reliable MAC address information to the ARP table as a static type to protect users from ARP spoofing. However, in contrast to its core concept, a light application of physically separated system with MAC-Agent is utilized for detecting the MAC address variations.

10. IDS for ARP spoofing using LTL based discrete event system framework :Mitra et al, [18] developed an intrusion detection system for ARP spoofing attacks using Linear-time Temporal Logic (LTL) discrete event system framework. This detection system provides a paradigm for stating the system specifications, modelling, detector construction and checking its correctness. It also provides adapted polynomial time complexity in the number of system states as compared to exponential complexity of the other traditional frameworks. It has better detection accuracy than other models due to the fact it does not alter the ARP protocol but improves the message tracking mechanism. However this method creates more congestion to detect the attacker nodes which may be problem when prolonged for each stage of transmission.

11. ARP spoofing detection algorithm using ICMP protocol: Jinhua and Kejian, [10] developed an ARP spoofing detection algorithm using the Internet Control Message Protocol (ICMP) which identifies the malicious hosts. This scheme collects and analyses the ARP packets, and then injects the ICMP echo request packets to probe for malicious host according to its response packets. Firstly, it does a cross layer control to examine the consistency of the source and destination address in Ethernet header and ARP header. Then, it compares the address mappings in valid ARP packets with those in the database and finally, all new ARP packets will be sent to ARP Spoof Detection Module to be re-verified. The advantage of this method is that the time delay between capturing packets and detecting spoofing is minimum than other models.

12. Prevention of ARP spoofing: A probe packet based technique: Pandey[22] developed a probe packet based prevention technique for ARP spoofing. This technique utilized Enhanced Spoofing Detection Engine (E-SDE) for detecting the ARP spoofing along with the genuine IP-MAC associations in the ARP cache of the network host. In this technique, the ARP and ICMP packets are used as probe packets and the attacking model is effectively detected. This technique also has less network traffic than other existing intrusion detection models. However as in most ARP spoofing detection models, when a strong attack is initiated, this model just detects the presence of attack while it fails to map the IP-MAC addresses due to strong opposition.

13. A new detection scheme for ARP spoofing attacks based on routing trace for ubiquitous environments: Song et al, [19] developed Detect Spoofing ARP (DS-ARP) scheme for detecting and mitigating the ARP spoofing attacks. This scheme detects ARP attacks through real-time monitoring of the ARP cache table and a routing trace and protects the hosts from attackers through ARP Link Type Control which changes from dynamic to static. Additionally, it can solve problems such as host impersonation, man-in-the-middle attack, and block of host. Unlike other existing schemes, this proposed scheme does not require an ARP protocol change or a complex encryption algorithm; moreover, it does not cause high system load. However, still the basic weaknesses of ARP prevail when new strategies of attacks are initiated.

An Integrated Approach to ARP Poisoning and its Mitigation using Empirical Paradigm: KaurandMalhotra[11] developed an integrated approach to detect and mitigate the ARP poisoning attacks by employing empirical paradigm. This model utilized tools like NetworkMiner, Cain and Abel and Wireshark for demonstrating the attack scenarios and corresponding attack mitigation. This model of attack mitigation is highly suitable for each kernel of the communication networks while also improve the HTTPS protocols. The limitation of this model is that the detection model using empirical paradigm is much simpler to break by the adversary.

14. Bayes-based ARP attack detection algorithm for cloud centers: Ma et al, [12] developed an intrusion detection model using Bayesian based algorithm to forecast the probability of each possible attacker hosts. Following these footsteps, a detection model is also utilized in order to mitigate the attacker host nodes. Using the SDN technology, the ARP packets are processed and the communication model of entire network is controlled. This process enables the system to distinguish the attackers' features from the normal features and thereby identifies the attacker host node. However the major issue with this model is that the attack nodes are unidentified when the adversary makes the attack features absorbed into normal node features.

15. RTNSS: a routing trace-based network security system for preventing ARP spoofing attacks: Moon et al, [6] designed and developed a routing trace-based network security system (RTNSS) as a detection model which uses monitoring agents to detect the ARP spoofing. The installed monitoring agent monitors the changes in the ARP cache table by the adversary. These changes are made to spoof the host address with a fake address including the IP, MAC address pair. Detection of these spoofing can be performed by the agent through a routing trace and it alerts the main server. Though this method seems to be similar to some existing detection methods, the ARP cache table changes are more accurately sensed in RTNSS and thus the attack detection is significant. Another important aspect is that, unlike existing methodologies, RTNSS incorporates the mechanisms to tackle the effects of structure changes and increased traffic changes due to encryption complexity. However this model fails to handle packet forwarding relay based attack strategy and also the lack of encryption mechanisms increases the security vulnerability of ARP.

16. Securing ARP and DHCP for mitigating link layer attacks: Younes, [21] introduced a security model that applies cryptography based protocols to the communications at data link layer to improve the authentication and data integrity. This model utilizes IPsec and Transport Layer Security (TLS) to provide authentication and data integrity using cryptography for communications at the network and transport layer. This model of intrusion detection can mitigate most of the link layer attacks including the rogue Dynamic Host Configuration Protocol (DHCP) server, DHCP exhaustion, malicious user, host impersonation, ARP Spoofing, man-in-the-middle, and denial of service attacks. Unlike existing models, this model mitigates the DHCP starvation attack using the symmetric key cryptography. However the limitation of this model is that it fails to prevent DoS attacks based on flooding and hence care should be taken.

17. Security Solution for ARP Cache Poisoning Attacks in Large Data Centre Networks : Prabadevi and Jeyanthi, [3] considered the issues in Layer-2 ARP protocols to mitigate the attacks. This model utilized the components to process by decoding the packets, updates the invalid entry made by the user with Timestamp feature and messages being introduced. Utilizing these components, the insecure communication, scalability issues and VM migration issues are mitigated such that the attacks in ARP namely host impersonation, MITM, Distributed DoS are prevented effectively. However this model fails to detect the ARP scanning attacks due to the issues in identifying the neighbor host feature.

18. A framework to mitigate ARP Sniffing attacks by Cache Poisoning: Prabadevi and Jeyanthi, [2] developed another framework for mitigating ARP sniffing attacks by cache poisoning. This method works by comparing the IP-MAC pair in the ARP and Ethernet headers and if any fake entry is suspected, the information is updated in the fake list and a message is sent to the gateway or router to alert it from cache poisoning attacks. This model significantly identifies the ARP based attacks including the scanning attacks but the limitation is that when new attack strategy is undertaken by the adversary hosts, it fails to identify the attack.

The surveying of these research methodologies enlighten the concept of spoofing and enhancements in tackling them over the years. These methodologies form the basic foundation for future research works. A summarized comparison of these reviewed methodologies can further improve the understanding about the prevention strategies, which is provided in the following section.

II. Comparison of Attack Prevention Methodologies

The analysed methods and strategies are compared in terms of unique features, merits and demerits helps in obtaining a clear picture about the detection and prevention mechanisms of ARP cache poisoning and spoofing attacks. Table 1 shows the comparison of these methodologies.

From this comparison, it can be found that over the years, the methods and mechanisms developed for ARP based attack mitigation has been increased in number as well as quality based on the strength of the attack strategies. However, it is fair to say that in spite of tremendous efforts by various researchers, the ARP based attacks have also grown significantly and hosts launch stronger attacks countering the preventive measures. It is also quite understandable that this war between researchers and attackers is tends to continue and hence the scope for developing efficient defense mechanisms that tackle the existing vulnerabilities and limitations. By taking inputs from the past research models, the researchers can up with new efficient methodologies to tackle the ARP based attacks.

TABLE I

Comparison of ARP BASED attack mitigation strategies

S. No.	Authors	Method/ Approach Used	Merits	Demerits
1	Zheng &Chenzhong (2003)	Stateless property based ARP Spoofing detection	Simplest approach without changing the features of ARP	Serious performance degradation with updates in attacks
2	Bruschi et al, (2003)	Secure address resolution protocol (S-ARP)	Strong authentication reduces ARP poisoning occurrence	Single-point failure is not eliminated
3	Carnut&Gondim (2003)	Sniffer based and SNMP packet based detection	Enables both for direct detection and false positive mitigation	Additional strategy for false positive mitigation is used which incurs excess cost
4	Koo et al, (2005)	Network Blocking algorithm	Improved network resource and security management system with higher authentication	Sometimes it fails to detect genuine users due to technical mistakes
5	Trabelsi&Shuaib (2006)	Spoofed ARP packet based detection	Accurate identification without performance degradation due to additional packets flow	High false positive/negative ratio when firewalls are used in attacks
6	Lootah et al, (2007)	Ticket-based address resolution protocol (TARP)	Resolves lack of authentication and proof of address ownership problems in addition to spoof detection	Not commonly accepted by the internet community as it changes ARP features
7	Liu et al, (2008)	ARP cache updating using Switching	Better prevention of ARP attacks through its own	Requires additional algorithms for varying

			feature functionality	attack features
8	Hao& Tao (2009)	Encryption & Binding switch ports	Detects manual update of IP-MAC records and averts malicious hosts	Provides only a temporary solution
9	Neminath et al, (2010)	Discrete event system (DES) approach	Detects the attacks through spoofed ARP hash tables with less false detection	High traffic is generated for probe packets and requires separate cache tables for spoof & genuine IP-MAC addresses.
10	Xing et al, (2010)	WinPcaP based defense mechanism	Detects without altering ARP features and also sends alert messages	Delay in transmission is inevitable
11	Hou et al, (2010)	Snort with ARP detection module	Improved ARP spoofing detection than normal Snort	Lacks dynamic detection mechanism
12	Barbhuiya et al, (2011)	Active host based intrusion detection system	Detects most ARP based attacks	Third party applications are required for prevention of attacks
13	Kumar &Tapaswi, (2012)	Centralized systemwith ARP Central Server	Consistent detection without altering ARP architecture	Susceptible to central point failure and also the IP exhaustion attack is untraceable
14	Nam et al, (2013)	Collaborative approachusing fairness voting	Detects MITM attacks efficiently and does not rely on public key cryptography methods	False detection is possible when the neighbor hosts are already spoofed
15	Hong et al, (2013)	Cryptography based schemes	AES and RSA protects against attacks along with automatic renewal of MAC address details	Additional application is used for detecting MAC address variations which deviates from its core concept
16	Mitra et al, (2013)	LTL discrete event system framework	Attack detection with high accuracy but without altering ARP features and improved message tracking mechanism	More congestion is possible when the attack detection is prolonged over transmission time
17	Jinhua&Kejian, (2013)	ICMP based ARP spoofing detection	Time delay for detection is minimum & detection accuracy is higher	Presence of existing attacks is untraceable
18	Pandey (2013)	Probe packet based technique with E-SDE	Attack detection with less traffic	Fails to map IP-MAC address when strong attack is initiated
19	Song et al, (2014)	DS-ARP	Detects attacks without requiring encryption algorithms or altering ARP and also does not cause high system load	Inefficient when new strategies of attacks are initiated
20	Kaur&Malhotra (2015)	Integrated approach with empirical paradigm	Suitable for HTTP and HTTPS protocols	Simpler to break after certain trails of execution

21	Ma et al, (2016)	Bayesian based algorithm	Centralized control of entire network enhances protection	Attacks are unidentified when attacks features are misinterpreted as normal features
22	Moon et al, (2016)	Routing trace-based network security system (RTNSS)	Detects ARP attacks with effective tackling strategies for structure changes and increased traffic	Lack of encryption and failure to handle packet forwarding relay based attack strategy
23	Younes (2017)	Cryptography based protocols with IPsec and TLS	Prevents ARP spoofing attacks including DHCP starvation attack	Failure to detect flooding based DoS attacks
24	Prabadevi&Jeyanthi, (2017)	Messaging based detection	Effective attack mitigation along with resolving scalability issues and VM migration issues	ARP scanning based attacks are not detected
25	Prabadevi&Jeyanthi, (2018)	IP-MAC comparison based detection	Effectively detects ARP based attacks including scanning attacks	Fails to detect attacks through new strategies

III. Conclusion

This paper provided the survey and analysis of some of the research works based on ARP Spoofing based attack prevention strategies over the recent years. The aim of this paper is to understand the concepts of ARP attacks and analyze the principles of various detection and prevention methodologies. This work would provide us with a clear understanding about the current stage of ARP spoofing detection research and help us to take over the future researches. The illustrated methodologies are compared based on their merits and demerits from which it is found some strategies like DES, TARP, S-ARP and ICMP based models are still in the early research stages. Likewise, the network blocking algorithm, encryption & binding and WinPcaP strategies are mostly prescribed based on the reduced labour work but the adverse effects on performance are still not resolved. Among these methodologies, DS-ARP, Bayesian based algorithm and RTNSS are most efficient ones with better application of attack detection and prevention strategies with broader view of performance maintenance. Based on the analysis results inferred, it can be concluded that there still lot of vulnerabilities in ARP architecture. The major limitations that need instant consideration are a) inability to detect existing attackers and attacks through new strategies, b) higher cost and transmission delay due to high encryption and c) more congestion and loss of information. These limitations must be portrayed while introducing new concepts of prevention methodologies for newly evolving attack strategies in order to satisfy all necessities of an ideal ARP spoof defense model.

References

1. A. Samvedi, S. Owlakand V. K. Chaurasia, “Improved Secure Address Resolution Protocol,” arXiv preprint arXiv:1406.2930, 2014.
2. B. Prabadevi andN. 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.
3. B. Prabadevi andN. 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.

4. C. L.Abadand R. I. Bonilla, “An analysis on the schemes for detecting and preventing ARP cache poisoning attacks,” In Proc. 27th International Conference on Distributed Computing Systems Workshops, ICDCSW'07, IEEE, 2007,pp. 60-60.
5. D. Bruschi, A. OrnaghiandE. Rosti, “S-ARP: a secure address resolution protocol,” In Proc. 19th Annual Computer Security Applications Conference, 2003, pp. 66-74.
6. D. Moon, J. D. Lee, Y. S.Jeongand J. H. Park, “RTNSS: a routing trace-based network security system for preventing ARP spoofing attacks,” The Journal of Supercomputing, vol. 72, no. 5, pp. 1740-1756, 2016.
7. D. Wetteroth, OSI reference model for telecommunications (Vol. 396). New York: McGraw-Hill, 2002.
8. F. A.Barbhuiya,S. BiswasandS. Nandi, “An active host-based intrusion detection system for ARP-related attacks and its verification,” International Journal of Network Security and Its Applications (IJNSA), vol.3, no.3, pp. 163-180, 2011.
9. G. HaoandG. Tao, “Principle of and Protection of Man-in-the-middle Attack Based on ARP Spoofing,” Journal of Information Processing Systems, vol. 5, no. 3, pp. 131-134, 2009.
10. G. JinhuaandX. Kejian, “ARP spoofing detection algorithm using ICMP protocol,” In Proc. International Conference on Computer Communication and Informatics (ICCCI), IEEE, 2013, pp. 1-6.
11. G. KaurandJ. Malhotra, “An Integrated Approach to ARP Poisoning and its Mitigation using Empirical Paradigm,” International Journal of Future Generation Communication and Networking, vol. 8, no. 5, pp. 51-60, 2015.
12. H. Ma, H. Ding, Y. Yang, Z. Mi, J. Y. Yang andZ. Xiong, “Bayes-based ARP attack detection algorithm for cloud centers,” Tsinghua Science and Technology, vol. 21, no. 1, pp. 17-28, 2016.
13. H. Neminath, S.Biswas, S. Roopa, R.Ratti, S. Nandi, F. A. BarbhuiyaandV. Ramachandran, “A DES approach to intrusion detection system for ARP spoofing attacks,” In Proc. 18th Mediterranean Conference on Control and Automation (MED), IEEE, 2010,pp. 695-700.
14. J. Koo, S. Ahn, Y. LimandY. Mun, “Evaluation of network blocking algorithm based on ARP spoofing and its application,” In Proc. International Conference on Computational Science and Its Applications, Springer, Berlin, Heidelberg, 2005, pp. 848-855.
15. J. Singh, G. Kaur andJ. Malhotra, “A Comprehensive Survey of Current Trends and Challenges to mitigate ARP attacks," In Proc. International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO), IEEE, 2015, pp. 1-6.
16. M. CarnutandJ. Gondim, “ARP spoofing detection on switched Ethernet networks: A feasibility study,” In Proc. of the 5th SimposioSegurancaemInformatica, 2003.
17. M. Conti, N. DragoniandV. Lesyk, “A survey of man in the middle attacks,” IEEE Communications Surveys and Tutorials, vol. 18, no. 3,pp. 2027-2051, 2016.
18. M. Mitra, P. Banerjee, F. A. Barbhuiya, S.BiswasandS. Nandi, “IDS for ARP spoofing using LTL based discrete event system framework,” Networking Science, vol. 2, no. 3-4, pp. 114-134, 2013.
19. M. S. Song, J. D. Lee, Y. S.Jeong, H. Y. Jeongand J. H. Park, “DS-ARP: a new detection scheme for ARP spoofing attacks based on routing trace for ubiquitous environments,” The Scientific World Journal, vol. 2014, Article ID 264654, 7 pages, 2014.

20. O. Depren, M. Topallar, E. Anarimand M. K. Ciliz, "An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks," Expert systems with Applications, vol. 29, no.4, pp. 713-722, 2005.
21. O. S. Younes, "Securing ARP and DHCP for mitigating link layer attacks," Sādhanā, vol. 42, no. 12, pp. 2041-2053, 2017.
22. P. Pandey, "Prevention of ARP spoofing: A probe packet based technique," InProc. IEEE 3rd International Advance Computing Conference (IACC), 2013, pp. 147-153.
23. R. Wagner, "Address resolution protocol spoofing and man-in-the-middle attacks," The SANS Institute, 2001.
24. S. H. Weingart, "Physical security devices for computer subsystems: A survey of attacks and defenses," In Proc. International Workshop on Cryptographic Hardware and Embedded Systems, Springer, Berlin, Heidelberg,2000, pp. 302-317.
25. S. Hong, M. Oh andS. Lee, "Design and implementation of an efficient defense mechanism against ARP spoofing attacks using AES and RSA," Mathematical and Computer Modelling, vol. 58, no. 1-2, pp. 254-260, 2013.
26. S. Kumar andS. Tapaswi, "A centralized detection and prevention technique against ARP poisoning. In Proc. International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), IEEE, 2012, pp. 259-264.
27. S. Nam, S. Djuraev andM. Park, "Collaborative approach to mitigating ARP poisoning-based Man-in-the-Middle attacks," Computer Networks, vol. 57, no. 18, pp. 3866-3884, 2013.
28. W. Lootah, W. Enck andP. McDaniel, "TARP: Ticket-based address resolution protocol," Computer Networks, vol. 51, no. 15, pp. 4322-4337, 2007.
29. W. Stallings, Network Security Essentials: Applications and Standards, 4/e. Pearson Education India, 2000.
30. W. Xing, Y. ZhaoandT. Li, "Research on the defense against ARP spoofing attacks based on Winpcap," In Proc. Second International Workshop on Education Technology and Computer Science (ETCS), 2010, vol. 1, pp. 762-765.
31. W. Zhengand L. I. Chenzhong, "AN Algorithm against Attacks Based on ARP Spoofing," Journal of Southern Yangtze University (Natural Science Edition), vol. 2, no. 6, pp. 167-1696, 2003.
32. X. Hou, Z. JiangandX. Tian, "The detection and prevention for ARP Spoofing based on Snort," In Proc. International Conference on Computer Application and System Modeling (ICCASM), 2010, vol. 5, pp. V5-137.
33. Y. Liu, K. Dong, L. Dong andB. Li, "Research of the ARP spoofing principle and a defensive algorithm,"International Journal of Communications, vol. 4, no. 1, pp. 143-147, 2008.
34. Z. TrabelsiandK. Shuaib, "Spoofed ARP packets detection in switched LAN networks," In Proc. International Conference on E-Business and Telecommunication Networks, Springer, Berlin, Heidelberg, 2006, pp. 81-91.
35. Z. TrabelsiandW. El-Hajj, "On investigating ARP spoofing security solutions," International Journal of Internet Protocol Technology, vol. 5, no. 1-2, pp. 92-100, 2010.