An Innovative Method for Detection and Prevention Against ARP Spoofing in MANET

Shradha Shukla
Computer Science & Engg. Deptt.
GGCT, Jabalpur
R.G.P.V. Bhopal (M.P.), India

Indresh Yadav
Computer Science & Engg. Deptt.
GGCT, Jabalpur
R.G.P.V. Bhopal (M.P.), India

Abstract- Network Security is always foremost and big issue in wired and wireless network. Wireless network, whether it is infrastructure mode or mobile adhoc mode, breaks the barriers of wired network and are easily accessible to everyone but everything is at a cost, the cost is in the form of increased susceptibilities and vulnerabilities of network. Using static ARP entries is considered the most effective way to prevent ARP spoofing. Yet, ARP spoofing mitigation methods depending on static ARP have major drawbacks. In this paper, we propose a scalable technique to prevent ARP spoofing attacks, which automatically configures static ARP entries. Among this Address Resolution Protocol (ARP) is responsible for the agreement to host the target of 32-bit IP address into the corresponding 48-bit MAC (Media Access Control) address, so as to ensure smooth communication.The technique operates in both static, DHCP and MANET based addressing schemes, and Scalability of the technique allows protecting of a large number of users without any overhead on the administrator. Performance study of the technique has been conducted using a real network. The measurement results have shown that the client needs no more than one millisecond to register itself for a protected ARP cache. The results also shown that the server can a block any attacker in just few microsecond under heavy traffic.

Keywords: layer two attacks; ARP spoofing; Static ARP entries, MAC address, Spoof detection, Port security

I. INTRODUCTION

Generally ARP is responsible for the agreement to host the target of 32-bit IP address into the corresponding 48-bit MAC address, so as to ensure smooth communication. The ARP is a network layer protocol of the Open Systems Interconnection (OSI) that is used by hosts on a LAN to dynamically mapping an IP address (logical address) to a MAC address (physical machine address). However, the current state of IP address management can be said to be extremely inefficient. Mobile ad-hoc networks are more prone towards spoofing attacks. In identity-based spoofing attacks, an attacker can forge its identity to masquerade as another device or even create multiple illegitimate identities in the networks by masquerading as an authorized wireless access point (AP) or an authorized client [1]. An attacker can launch denial of- service (DoS) attacks, bypass access control mechanisms, or falsely advertise

services to wireless clients. Therefore, identity-based attacks will have a serious impact to the normal operation of wireless and sensor networks.

1.1. IP SPOOFING

Internet Protocol (IP) is the protocol used for transmitting messages over the Internet [3]; it is a network protocol operating at layer 3 of the Open Systems Interconnection (OSI) model. IP spoofing is the act of manipulated the headers in a transmitted message to mask a hackers true identity so that the message could appear as though it is from a trusted source. IP spoofing is used to gain unauthorized access to a computer. The attacker forwards packets to a computer with a source address indicating that the packet is coming from a trusted port or system.

1.2. ARP SPOOFING

ARP Spoofing involves constructing forged ARP request and reply packets. By sending forged ARP replies, a target computer could be convinced to send frames destined for computer A to instead go to computer B". This referred to as ARP poisoning. Generally ARP is responsible for the agreement to host the target of 32-bit IP address into the corresponding 48-bit MAC address, so as to ensure smooth communication. The ARP is a network layer protocol of the Open Systems Interconnection (OSI) that is used by hosts on a LAN to dynamically mapping an IP address (logical address) to a MAC address (physical machine address). However, the current state of IP address management can be said to be extremely inefficient.

1.3 WEB SPOOFING

Web Spoofing is an attack that allows someone to view and modify all web pages sent to a victim's

machine. They can observe any information that is entered into forms by the victim. This can be of particular danger due to the nature of information entered into forms, such as addresses, credit card numbers, bank account numbers, and the passwords that access these accounts.

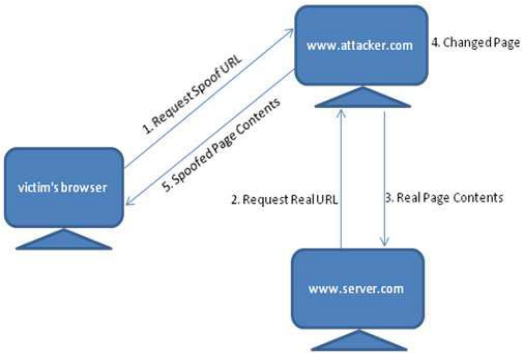

Fig.1. Working of WEB Spoofing

1.5. DNS SPOOFING

A DNS spoofing attack can be defined as the successful insertion of incorrect resolution information by a host that has no authority to provide that information. In DNS spoofing an attacker may insert IP address information that will redirect a customer from a legitimate website or mail server to one under the attacker's control thereby capturing customer information through common man-in the-middle mechanisms.

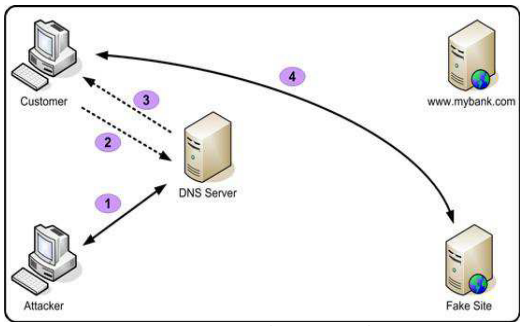

Fig.2. Working of DNS Spoofing

However, authentication requires additional infrastructural overhead and computational power associated with distributing and maintaining cryptographic keys. A different approach is proposed, where in the physical property associated with each wireless node is used to assess the presence of adversaries in the wireless network. This method is hard to falsify, and not reliant on cryptography as the basis for detecting spoofing attacks. This approach enables to detect and localize multiple adversaries in the network, with high detection rate and minimal infrastructure. In a large-scale wireless network, multiple adversaries may masquerade as the same identity and collaborate to launch malicious attacks. Therefore, the problem can be divided into 2 folds such as:

i. Detect the presence of spoofing attacks,

ii. Determine the number of attackers, and localize multiple adversaries. The identification and localization can be done in the following ways:

II. PRINCIPLE OF ARP SPOOFING

ARP protocol is based on the mutually trust, it is a stateless protocol. The request way of ARP is by broadcasting, each host that does not receive the request can send out ARP response package randomly, when ARP buffer without authentication mechanism received the ARP response it will dynamic updating the cache directly, the above all provide the spoofing condition. Among this various attacks e.g. ARP spoofing attacks, man in middle attack are threatening the security of our campus network, which causing confusion within the network. Disturbed information of one network to another network illegally. Now various points of view i.e. impacting network connection, ARP spoofing attack [19, 20] is divided into two types:

i. Cheating gateway

By forging a series of IP address and the corresponding error MAC address, and sent the forged ARP packets to gateway with certain frequency, and then the correct address information stored in gateways be refreshed by the wrong address information. As a result, the gateway will send the data to the wrong MAC address, so the normal host cannot receive the message and not access the Internet. This ARP communication provides a chance for ARP cheat.

ii. Cheating the host of the internal network

The cheater fake gateway, and make the target host refresh its ARP cache list, by this way the cheater can intercepted the target host' information which send to the gateway. Hence ARP spoofing allows an attacker for DNS poisoning. DNS server returns the IP address of the corresponding DNS address to the client browser [18]. Now this section discuss about principles of ARP spoofing attack with two types, now next section of this paper discuss about consequences of various attack e.g. man in middle attack being performed over a network by an unauthentic user. The task of determining the MAC (Media Access Control) address for the data to be sent on network is the responsibility of ARP. ARP is used by the IP network layer to map IP addresses to hardware addresses at data link layer.

2.1 WORKING OF ADDRESS RESOLUTION PROTOCOL (ARP)

Step 1: When a source device wants to communicate with another device, source device

checks its Address Resolution Protocol (ARP) cache to find it already has a resolved MAC Address of the destination device. If it is there, it will use that MAC Address for communication.

Step 2: If ARP resolution is not there in local cache, the source machine will generate an Address Resolution Protocol (ARP) request message, it puts its own data link layer address as the Sender Hardware Address and its own IPv4 Address as the Sender Protocol Address. It fills the destination IPv4 Address as the Target Protocol Address. The Target Hardware Address will be left blank, since the machine is trying to find that.

Step 3: The source broadcast the Address Resolution Protocol (ARP) request message to the local network.

Step 4: The message is received by each device on the LAN since it is a broadcast. Each device compare the Target Protocol Address (IPv4 Address of the machine to which the source is trying to communicate) with its own Protocol Address (IPv4 Address). Those who do not match will drop the packet without any action.

Step 5: When the targeted device checks the Target Protocol Address, it will find a match and will generate an Address Resolution Protocol (ARP) reply message. It takes the Sender Hardware Address and the Sender Protocol Address fields from the Address Resolution Protocol (ARP) request message and uses these values for the Targeted Hardware Address and Targeted Protocol Address of the reply message.

Step 6: The destination device will update its Address Resolution Protocol (ARP) cache, since it need to contact the sender machine soon.

Step 7: Destination device send the Address Resolution Protocol (ARP) reply message and it will NOT be a broadcast, but a unicast.

Step 8: The source machine will process the Address Resolution Protocol (ARP) reply from destination, it store the Sender Hardware Address as the layer 2 address of the destination.

Step 9: The source machine will update its Address Resolution Protocol (ARP) cache with the Sender Hardware Address and Sender Protocol Address it received from the Address Resolution Protocol (ARP) reply message.

You have learned Address Resolution Protocol (ARP), Address Resolution Protocol (ARP) Message Format and how Address Resolution Protocol (ARP) operates in a LAN.

ARP does not maintain the states of its own and hence does not check whether the upcoming ARP reply was actually requested or not, before updating the corresponding pairing in the ARP cache of the system. So, the attacker sends the bogus replies to the communicating systems, thereby making the changes favourable to attacker, in the pairing of IP and MAC addresses. By doing this the information starts going through the attacker's machine, without coming into notice of actual hosts. In order to minimize the number of ARP requests that are being broadcast, operating systems maintain a cache of ARP replies from different hosts. When a host receives any ARP reply, it will normally update its ARP cache with the new IP/MAC association entry. Since ARP is known to be stateless protocol, most operating systems generally will update their cache if a reply is received, regardless of fact whether they sent out any actual requet or not.

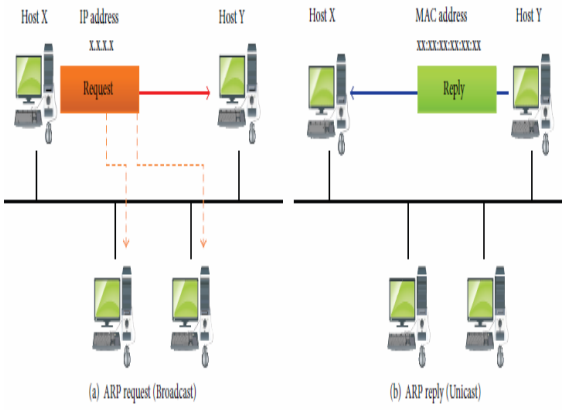

Figure 1: ARP request/reply protocol.

2.2 ARP SPOOFING

ARP spoofing or ARP cache poisoning, a method of attacking an Ethernet LAN by updating the target computer's ARP cache with both a forged ARP request and reply packets in an effort to change the Layer 2 Ethernet MAC address (i.e., the address of the network card) to one that the attacker can monitor. The result of ARP cache poisoning is that the IP traffic intended for one host is diverted to a different host. There is much different kind of attacks that could be implemented to poison the respective ARP caches of two communicating devices. These are like man-in-the-middle attack, sniffing, cloning, connection hijack, denial of service, smart IP spoofing etc. Encrypted connections are also not secure. Such attacks can also be performed on SSL (Secure Socket Layer)

also. It has also become easy due to easy availability of different exploits online and that too are free of cost.

ARP Spoofing is a hacking technique to send fake ARP request or ARP reply, ARP spoofing problem comes from the way the ARP protocol works [5]. Since the ARP protocol is a stateless protocol that receives and processes ARP replies without issuing ARP request [6], the ARP cache can be infected with records that contain wrong mappings of IP-MAC addresses. ARP spoofing can be used to launch one of two different attack categories [7]: Denial of Service (DoS) attacks or Man in the Middle (MITM) attacks.

Several solutions have been proposed to mitigate the ARP spoofing, but each has its limitations [7]. The solutions have been classified into five different categories [8]:

i. Modifying ARP using cryptographic techniques- These solutions add some cryptographic features to the ARP protocol, but will not be compatible with the standard ARP and affect the protocol performance.
ii. Kernel-based patching - The technique adds a patch to the operating system kernel in order to prevent ARP spoofing attacks, but the problem is that not all operating systems can be patched and it may become incompatible with the standard ARP protocol.
iii. Securing switch Ports- Use the switch port security or Dynamic ARP inspection (DAI) option to prevent ARP spoofing. However its ability of preventing ARP spoofing easily, the cost of implementing such solution may not be acceptable by most of the organizations.
iv. ARP spoof detection & protection software- Programs or tools developed to prevent ARP spoofing attacks, but the experimental results have shown there ineffectiveness in protection.
v. Manually configuring static ARP entries- The most basic and effective way to prevent ARP spoofing [1] [6] [9] is adding static ARP entries at each host. However this solution cannot be easily managed and cannot scale well specially in organizations that have large number of users and require a heavy workload on the network administrator.

III. Background and Related Work

As mentioned previously, solutions attempting to prevent ARP spoofing attack using the static ARP cache entries are very efficient. Yet this category of solutions has some major problems [7] [8]:
i. Overhead required for manual configuration of static entries
ii. Limited scalability for large networks
iii. Ability to work in static and DHCP based networks.
In the following, we will survey several methods belonging to this category along with their drawbacks.
The DAPS (Dynamic ARP spoof Protection System) technique suggested in [8] is a solution to ARP spoofing that snoops DHCP packets and use them as vaccines. Yet this technique doesn't scale well for those networks that use static IP addressing scheme and also vaccines will be invalid if DHCP starvation attack occurs.
In [12], the NIDPS (Network Intrusion Detection and Prevention System) technique is suggested have a server collecting IP-MAC mappings from users using small agents. These mappings will be then used as static ARP entries to correct any wrong mapping detected. However, agents aren't authenticated to the server. Moreover, it detects only attacks from its LAN segment. Also, the server examines every packet going in or out the LAN segment. Finally, it waits for the attack to occur and then try to solve it.
Xiangning et al. [13] has proposed a technique that expands the snort pre-processors plug-ins by adding an ARP detection module. The proposed technique doesn't scale well in large networks due to the need of manual configuration of the static mappings at the server. It also doesn't work in DHCP based networks.
A solution to ARP spoofing using a server is proposed in [14]. The server will get mappings for the network users from the DHCP server. It replies also to ARP requests. Unfortunately, this solution works only in DHCP networks. Also, it is not compatible with the standard ARP. Moreover, if DHCP starvation occurs, all the server information will be invalid.
Ai-zeng Qian [15] proposed a technique to prevent ARP spoofing by using static ARP entries but the technique still doesn't work with dynamic networks using DHCP addressing. The administrator must assign all IP addresses along with their MAC to the server so it will be not visible for large scale network.
A method is suggested in [16] to solve ARP spoofing problem using snort IDS and static ARP entries. Yet, it still needs the administrator to add the static mappings manually. Also, it works only in static networks.

IV. Proposed Method

The proposed technique is a client-server protocol that prevents ARP spoofing by automatically configuring static ARP entries. The protocol works in both static, DHCP, wireless and MANET networks. Moreover, it can work in large-scale networks without any overhead on the administrator. In addition, the technique doesn't

require special hardware to be deployed, as any host can work as ARP server.
The protocol proposed defines three different messages:
1. Register Message**:** is unicast message sent from the client to the server. It contains its IP and MAC address. Also it includes a hashed authentication key.
2. Update Message: is a broadcast notification message sent from the server to all users in the network indicating that a new user has entered the network. It also contains the IP and MAC address of that new user.
3. Register Response Message**:** is a unicast message sent from the server to the new user. It contains all static ARP entries of users successfully registered at the server.

The protocol also defines two different entities:
a) ARP Client**:** is software installed on user's machines. It fulfils the following:
i. Automatically get the IP and MAC address of the user and use them to send register message to the server.
ii. Receive update and register response messages from the server.
iii. Verify that update or register response messages received are coming from a trusted server.
iv. Use the IP and MAC pairs received in the update or register response message to add static ARP entries to the user ARP cache.

b) ARP Server**:** is server software that can be installed on any device in the network. It can also be installed on a dedicated server, and has the following functions:
i. Receive register messages from the ARP clients.
ii. Verify that the message is coming from a trusted user.
iii. Make use of the IP and MAC pairs encapsulated within the register message to create a list of trusted users in the network.
iv. Send broadcast update message to notify them that a new user has come to the network.
v. Send register response message to the new users.
vi. Take the proper action regarding users who try to violate the protocol security rules.
The proposed protocol defines two different algorithms for the client and server in order to prevent the ARP spoofing attack

4.1 CLIENT ALGORITHM

The client algorithm described in Algorithm 1 adds static entry for the server in the client ARP cache to avoid the rogue server threat. Furthermore, it obtains the user IP and MAC address automatically to make the user has no opportunity to send fake information to the server.

The algorithm checks the source IP address of the received message to be sure that it is coming from the trusted server. It only accepts the IP and MAC addresses encapsulated in the message if the key is correct.

In order to work in MANET networks where IP and MAC mappings are frequently changing, the algorithm searches for the MAC encapsulated in the message. If matched map is found, it will be changed to the new mapping. Otherwise a new mapping will be added. Finally if any of the conditions are not met, the algorithm will discard the message and return to listen for another message from the server.

4.2 SERVER ALGORITHM

The server algorithm, described in Algorithm 2, listens to incoming register messages from the clients, checks the hash code to be sure that the message is coming from a trusted host. Users are given only three trials to send the correct hash code. If it fails to send the correct hash code within the three trials, the server will block this user. The blocking action depends on the addressing scheme being used, for MANET networks, the MAC address of the user will be added to MANET deny list. Hence, it will not be able to obtain IP configuration from the MANET server again, for static networks, the server will prevent traffic from this user to reach the server by obstructing its IP address. If the key is correct and the number of wrong trials doesn't reach the threshold, the server will search its ARP cache for matching between MAC address encapsulated in the register message received and MAC address in ARP cache. This gives the algorithm the ability to work with MANET based networks. In turn, it prevents an intruder having the hash code to spoof all ARP cache entries. As a matter of fact, it can only spoof one at a time. If it tries to spoof another one the old spoofed entry will be deleted. User who has successfully registered at the server will receive a register response message contains the IP and MAC addresses of all successfully registered users to add them as static ARP entries. Moreover, all other users will receive an update message contains IP and MAC address of the new user to add it as a static entry in their ARP cache. Using the client and server algorithms, every user in the network will have its ARP cache filled with static ARP entries for all other users in the network. Hence, it will not suffer from the ARP spoofing problem again. And everything is done automatically without any overload on the administrator; this gives the algorithm a greater scalability.

4.3 PRINCIPLE OF WINPCAP

Generally winpcap (windows Packet capture) is a network layer access tool to access system under the windows platform, which provides the following functions:

a) To capture the raw datagram, including datagram sent/received by or to the hosts in the sharing network and as well as the exchange of between;

b) To filter some special datagram in accordance with the user defined rules before sent to the application process.

c) To send original datagram on the network.

d) To collect statistics in the network communication process.

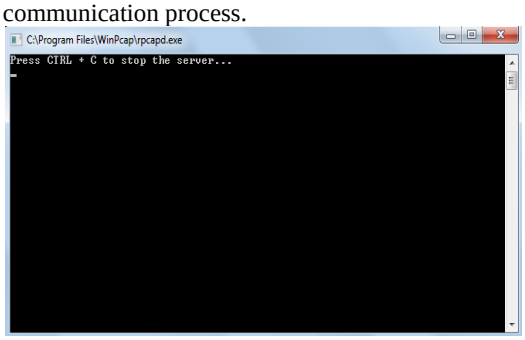

Fig 4.1Initialization of Winpcap Services

Hence this section discusses various defence mechanisms against ARP spoofing attack using winpcap. Now next section discuss about network monitoring using sniffer tread (winpcap).

4.4 NIGHTHAWK ATTACKER

Nighthawk is an experimental implementation of ARP/ND spoofing, password sniffing and simple SSL stripping for Windows.It requires WinPcap and .NET Framework 4 (Client profile) and works best on windows platform.

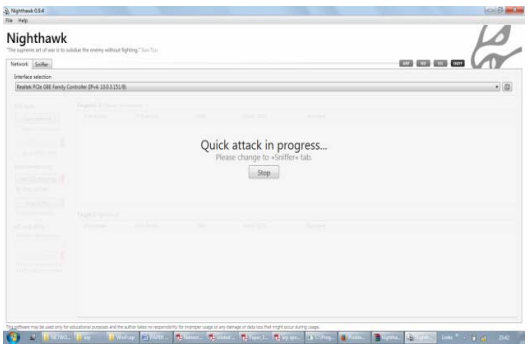

Fig 4.2 Nighthawk Attacker for ARP Spoofing Attack

4.5 ARP ATTACK DETECTION AND PREVENTION

We have implemented a ARP detection and prevention mechanism based on .NET framework.

Detection-

Active checking of host-level: Another preventive measure of ARP deception detection is to arrange host to send ARP request packet about its own IP address while starting system or periodically [2,17]. If could receive another ARP response, report ARP deception to the host user or administrator.

b) Passive detection of host-level: Checking whether the target address matches with IP address of the local web application, we can know whether the message sent to own. If yes, we need to send an ARP response. Once the operating systems was interrupted, checking whether the sender's IP address correspondent with its own IP address, and if same, indicates that it is ARP deception [4,7].

c) Network-level detection: To detect network level through periodic polling. Through regular review of the ARP high-speed cache, it will be able to detect these correspondence changes between IP Address in high-speed cache of these machines and hardware address [1, 9].

d) Server-class detection: In order to establish its authenticity, when the server has received the ARP response, it will regenerate a RARP request from the MAC address given by the response message according to Reverse ARP (RARP), and, which asked the question: "If you are the owner of the MAC address, please reply to your IP address".

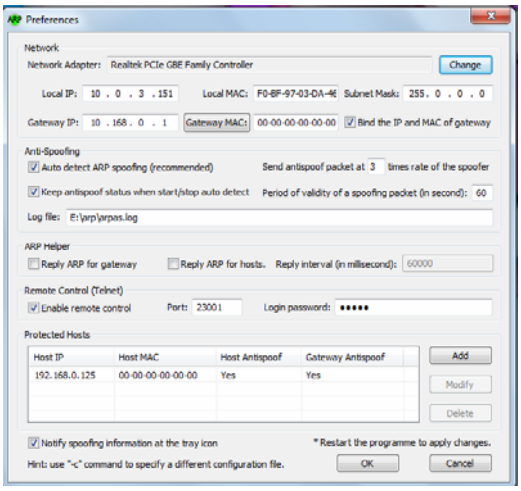

Fig 4.3 ARP Spoofing Identification and Prevention System

Prevention-

According to ARP response packet theory, relevant source address corresponding to its target MAC address in these two protocols should be the same As per the principle of actualization of TCP/IP protocol stack, upper layer protocol sends data packet to its corresponding lower layer protocol and the lower layer seals that data packet as the data of his own; when receiving data packets, every layer only handles protocol of its own. After handling this, it hands the data parts to upper layer protocol. But now during this process, cross-layer

verification cannot be done. Now check relevant items in data packet when system sends or receives ARP response data packet over a network. So whether relevant source MAC address and target MAC address match or not to verified in the ARP data packet; link layer head information.Now if it does not match the information of host computer, directly block data packet and prompt the user. This check can effectively prevent users from other users'ARP virus attack and avoid users ARP virus attacking other users.This ARP communication provides a chance for ARPcheat [12].Check rules are as follows:

a) ARP response packet sent: Check whether source MAC address in ARP packet totally matches displayed destination MAC address in link layer head information. Discard it, if not; check whether destination IP address in ARP packet totally matches destination MAC address in link layer head information [12,15]. If not, Directly discard it; check whether source MAC address in ARP data packet is the MAC address of this host, if not, discard it directly; check whether source IP address is the IP address of host, if not, directly discard it. On the basis of Host blocking attack, Host sends ARPresponse data packet to gateway and informs the gateway the address avoiding gateway being cheated [2].

b) TheARP response packet received*:* check whether source MAC address in ARP packet totally matches source MAC address in link layer head information [8]. Discard it, if not; check whether destination MAC address in ARP packet totally matches destination MAC address in link layer head information. If not, Directly discard it; check whether destination IP address is the IP address of host, if not, directly discard it.

V. CONCLUSION

In this paper, a solution to the problem of ARP spoofing has been proposed; the solution is an automatic and scalable method of configuring static ARP entries instead of manually configuring. The solution solves the main problems related to this category of solutions Usage of static entries, automation, scalability, manageability, prevention, and cost are the main features of the proposed method. The proposed method has defined two separate algorithms, one for the client, and the other for the server. Experimental evaluation was conducted on the LAN network. The response time metric is used to evaluate the system. Also different types of traffic workloads were used during the measuring the response to show the effect volume of traffic on the response time values. The results prove how fast and accurate the proposed algorithm is since any new user needs less than one millisecond to be safe from ARP problem for heavy workloads.

REFERENCES

[1] Yafeng Xu and Shuwen Sun , "The study on the college campus network ARP deception defense," 2010 2nd International Conference on Future Computer and Communication (ICFCC), 3(1), pp. 465-467, May 2010.

[2] R. W. Stevens. TCP/IP Illustrated, Volume 1: The Protocols. Addison–Wesley Professional Computing Series, January 1994.

[3] D. Plummer. An Ethernet address resolution protocol, Nov. 1982. RFC 826.

[4] Mohamed Al-Hemairy, Saad Amin, and Zouheir Trabelsi, "Towards More Sophisticated ARP Spoofing Detection/ Prevention Systems in LAN Networks," 2009 International Conference on the Current Trends in Information Technology (CTIT), pp.1-6, December 2009.

[5] Hu Xiangdong, Gao Zhan, and Li Wei "Research on the Switched LAN Monitor Mechanism and its Implementation Method based on ARP spoofing," International Conference on Management and Service Science.(MASS '09), pp. 1-4, Sept. 2009.

[6] Marco Antônio Carnut and João J. C. Gondim, "ARP spoofing detection on switched ethernet networks: a feasibility study," 5th Symposium on

Security in Informatics held at Brazilian Air Force Technology Institute, November 2003.

[7] Cristina L. Abad and Rafael I. Bonilla, "An Analysis on the Schemes for Detecting and Preventing ARP Cache Poisoning Attacks," 27th International Conference on Distributed Computing Systems Workshops, 2007. (ICDCSW '07), page(s): 60, June 2007.

[8] Somnuk Puangpronpitag and Narongrit Masusai, "An Efficient and Feasible Solution to ARP Spoof Problem," 6th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology, 2009. (ECTI-CON 2009), 3(1), pp. 910—913, May 2009.

[9] S. Whalen, "An introduction to ARP spoofing," 2600: The Hacker Quarterly, 18(3), 2001, (accessed 13-9-2012). [Online].:http://servv89pn0aj.sn.sourcedns.com/gbpprorg/2600/arp spoofing intro.pdf

[10] http://technet.microsoft.com/en-us/library/cc958841.aspx. ARP Cache, (accessed May 8, 2013).

[11] Zouheir Trabelsi and Wassim El-Hajj, "Preventing ARP Attacks using a Fuzzy-Based Stateful ARP Cache," IEEE International Conference on Communications.(ICC '07), pp. 1355 -1360, June 2007.

[12] Dr. S. G. Bhirud and Vijay Katkar, "Light Weight Approach for IP-ARP Spoofing Detection

and Prevention," 2011 Second Asian Himalayas International Conference on Internet (AH-ICI), page(s):1-5, November 2011.

[13] Xiangning HOU, Zhiping JIANG, and Xinli TIAN, "The detection and prevention for ARP Spoofing based on Snort," 2010 I

[14] Andre P. Ortega, Xavier E. Marcos, Luis D. Chiang and Cristina L. Abad, " Preventing ARP cache poisoning attacks: A proof of concept using OpenWrt," Latin American Network Operations and Management Symposium. (LANOMS), pp. 1-9, Oct. 2009.

[15] Ai-zeng Qian, "The Automatic Prevention and Control Research of ARP Deception and Implementation," 2009 WRI World Congress on Computer Science and Information Engineering, , 2(1), pp. 555-558, April 2009.

[16] Boughrara, A.; Mammar, S., "Implementation of a SNORT's output Plug-In in reaction to ARP Spoofing's attack," 2012 6th International Conference on Sciences of Electronics Technologies of Information and Telecommunications (SETIT), pp.643,647, 21-24 March 2012

[17] R. K. Jain, “The Art of Computer Systems Performance Analysis: Techniques for Experimental Design, Measurement, Simulation, and Modeling,” Prince Hall, April 1991.

[18]. Ferdous A. Barbhuiya, Santosh Biswas, NeminathHubballi,”A Host Based DES Approach for Detecting ARPSpoofing”, IEEE, 2011.

[19]. TAO Jun, LIN Hui, “IDSV: Intrusion Detection Algorithm based on Statistics Variance Method in User Transmission Behavior”, International Conference on Computational and Information Sciences, 2010.

[20]. JanghunBae, SeongjinAhn, “Network Access Control and Management using ARP Spoofing in Various Windows Environment”, IEEE, 2011.