International Journal of Research and Development in Applied Science and Engineering (IJRDASE)
ISSN: 2454-6844

Arp Security using Asymmetric Key and Invite Accept Protocol

Pankaj Verma
Computer Network,
BBD University, Lucknow, India
pankajverma90444@gmail.com

Dileep Gupta
Computer Science & Engg.,
BBD University, Lucknow, India
dileep,gupta.in@gmail.com

Abstract--In this thesis, we used Invite-Accept Protocol for securing the message from the malicious users. There will be a Blocking Server which sends the Request message to all active users over the Network at a regular period of T time. All the users who will be interested in joining the Network for secure communication will send the Accept message to the Server for the approval of the Invite message. Server will store their IP-MAC pair to its database table. Than Client will send Request message for the MAC address of the requested client to the Server for the communication to the other client over the same network. Server will verify the IP-MAC pair of the requested clients and if matched than they will be allowed otherwise its IP-MAC Address will be stored in the Blocking Address Database Table. The allowed user will than send direct message to the desired client. These protocol is made for reduce the action of the adversary that can cause the loss of message, arbitrarily modify the field of sent message and replay old message. The graph shows the packet drop which implies that forged messages is directly proportional to the packet drop. There will be a possibility to reduce the complexity of the protocol so that the program will run more fluently.

Keywords-- ARP, MAC, LLC, Key.

1. Introduction

The Address Resolution Protocol (ARP) is a data link layer protocol, which resolves any given logical Address (IP Address) to its corresponding physical address (MAC Address) . Address resolution is the process where network layer addresses are resolved into data link layer addresses, to permit data to be sent one hop at a time across an internetwork.

The Address Resolution Protocol (ARP) is the protocol used by the Internet Protocol (IP), specifically IPv4, to map IP network addresses to the hardware addresses used by the Data Link Layer Protocol. The protocol operates below the network layer as a part of the interface between the OSI Network and OSI Link Layer. It is used when IPv4 is used over Ethernet. The term address resolution refers to the process of finding address of a computer in a network. The address is "Resolved" using a protocol in which a piece of information is sent by a client process executing on the local computer to a server process executing on a remote computer. The information received by the server allows the server to uniquely identify the network system for which the address was required and therefore to provide the required address. The address resolution procedure is completed when the client receives a response from the server containing the required address.

An Ethernet network uses two hardware addresses which identify the source and destination of each frame sent by the Ethernet. The hardware address is also known as Medium Access Control (MAC). Each computer Network Interface Card (NIC) is allocated a globally unique 6 byte link address when the factory manufactures the card (stored in a PROM). This is the normal link source address used by an interface. A computer sends all packets which it creates with its own hardware source link address, and receives all packets which match the same hardware address in the destination field or one (or more) pre-selected broadcast/multicast addresses.

The Ethernet address is a link layer address and is dependent on the interface card which is used. IP operates at the network layer and is not concerned with the link addresses of individual nodes which are to be used .The address resolution protocol (ARP) is therefore used to translate between the two types of address. The ARP client and server processes operate on all computers using IP over Ethernet. The processes are normally implemented as part of the software driver that drives the network interface card.

ARP is used for converting a network address (e.g. an IPv4 address) to a physical address like an Ethernet address (also named a MAC address).

The data link layer or layer 2 is the second layer of the seven-layer OSI model of computer networking. This layer is the protocol layer that transfers data between adjacent network nodes in a wide area network (WAN) or between nodes on the same local area network (LAN) segment. The data link layer provides the functional and procedural means to transfer data between network entities and might provide the means to detect and possibly correct errors that may occur in the physical layer. The data link layer has two sub layers: *logical link control* (LLC) and *media access control* (MAC).

ARP is the stateless protocol(a stateless protocol is a communications protocol that treats each request as an independent transaction that is unrelated to any previous request so that the communication consists of independent pairs of request and response), was designed to map Internet Protocol Address (IP) to their associated MAC Address. This is done by mapping a 32 bit IP address to an associated 48 bit MAC Address.

2. Related Work:

ES-ARP An Efficient and Secure Address Resolution Protocol by Md. Ataullah [4] they proposed a stateful protocol, by storing the information of the request frame in

the ARP cache.They did not discussed about how to protect from the message replay .In this both ARP request and reply were broadcasted. All the host except the source host will store the entries in the ARP cache while the broadcast of both ARP Request and Reply. Due to this ARP Cache will be crouded and slow processing will occur. The method used is by storing the ARP Cache value and comparing it with each request. The Mechanism used are Stateful protocol and broadcasts both ARP request and reply.

Gouda and Huang [5] proposed A Secure Address Resolution Protocol, in which a secure server is connected to the Ethernet and communications with the server take place using invite-accept and request-reply protocols. All ARP requests and replies occur between a host and the server, and replies are authenticated using shared pair keys. The drawback is that if server fails due do system failure or other reason, there is no backup for this. They have secured Authentication process, Authorization process, Confidentiality but they have not discussed about the Non-Repudiation process and if the server fails the whole system will be interrupted. There is no backup given for that server. In this Secure Server resolves queries.

Ahmed M. AbdelSalam[3] proposed An Automated approach for Preventing ARP Spoofing Attack using Static ARP entries, in which he uses three different messages that is Register Message which is a unicast message sent from the client contains IP address, MAC address and hashed authentication key. Update message send from server to all clients which indicates that a new user has entered in the network. Third is the Registered response message which is a unicast message sent from the server to the new user contains all the static ARP entries of users successfully registered at the server.But they did not described how the hash code matching is done.

Jun Kim proposed “Method of Defending Against A Spoofing Attack By Using A Blocking Server” [6] The present invention relates to a method of defending against a spoofing attack using a blocking server, blocking server first store the IP –MAC pair in the allowed address database and after that when any malicious activity found about that client than its access is denied and its IP and MAC address pair is stored at blocked address database . They did not discussed about prevention from different ARP attacks. The Mechanism used is to store the IP-MAC pair at their tables and wait for any intruder to perform any type of Attack.

Bruschi et al. [7] proposed a secure address resolution protocol (SARP), which uses asymmetric key cryptography to authenticate the hosts in a local area network (LAN).In SARP, each host uses an invite–accept protocol to periodically register its IP–MAC pairs in a secure server.IP–MAC pairs are hashed by a message digest algorithm. This approach, however, requires medication of the ARP protocol as the sender needs to sign each ARP message with its private key, and the receiver needs to verify the signature with the sender’s public key. The Mechanism used is the Signed ARP replies.

.Limmaneewichid and Lilakiatsakun [8] proposed an ARP authentication scheme based on ARP authentication trailer, named P-ARP, which consists of a magic number, nonce and the authentication data produced by the HMAC hash function. In order to hide the target IP address in an APR request message, additional operation such as hash function must be performed to create nonce and HMAC values. In addition, this approach is ineffective against ARP DoS attacks.

Lootah et al. [10] implemented a secure IP–MAC address mapping in which an ARP reply is generated with an attached signature when a request is issued. A ticket is appended as a variable length Payload. This approach uses a local ticket agent (LTA), a key management server, to issue a public key to obtain the IP–MAC from the ticket. This approach is backward compatible with existing ARP, but it is susceptible to replay attacks.

3. Methodology:

For enhancing the security in the current paper I have used the concept of Invite – Accept protocol [5] with the help of asymmetric key.

The security parameters used are

Timeout to counter message loss

If a process in blocking server sends a message and does not receive a reply for this message for a relatively long time, the process will expire and new timeout will generate. This will also identify those clients which are active over the Ethernet and are eager to communicate with other clients.

Nonce to counter message replay

Before a process (in s or h[i]) sends a message, by inserting this nonce value to message digest and also with the message which will be send to h[i]. The sending process attaches to the message a unique integer nc, called the message nonce. When the receiving process receives the message it decrypts the message with its private key (RSA), if it is correct than matching of nc in the digest and other nc is done, if the value matches than it is justified that the message is not altered. When the sending process receives the reply and checks that the message nonce is the same as that in the original message, it concludes correctly that neither the original nor the reply were replaced by earlier messages by the adversary.

Public and Private key Certificate concept

The nonce value at the server will be encrypted by the public key of the requested client, so that only the desired client can decrypt with its private key. By this if any adversary captures the packet he will not able to decrypt the encrypted message as he will not have the required private key for decryption.

Blocking server and Administrator server (Two servers for Backup)

All type of sending and receiving message is done by blocking server. If any adversary found will be stored at the blocked address database and if the requested client genuine than its IP-MAC pair is stored at allowed address database. If the blocking server fails due to system failure or any other

reason than the backup database (stores both the databases) can be used for recovery from the Administrator server.

Working procedure for Blocking Server, Administrator server and Clients are:-

Step 1- Blocking server will send an Invite message to all the available clients at an interval of T time.
Step 2- The invite message contains a message digest and a nonce value. That message digest consist of the message nonce which is encrypted with the public key of that client h[i] that message nonce will be same as used outside the message digest.
Step 3- At the same time if any message received at the server this may be the Accept message send by the older client or the request message of the new client. The older client message will be processed and the new client message will be stored in the queue for the processing after the Time T.
Step 4- When the invite message is send to the client the Valid counter will be incremented by plus one . This will give an idea for how many request message is send and after T interval the client with incremented value will be considered as inactive.
Step 5- The valid counter and the nonce value is stored at Administrator Server Table in front of IP-MAC Address pair.
Step 6- When Client receives the invite message, First he decrypt with the private key public key pair. If the message is correct than the message will be decrypted otherwise the message is discarded. Second compare the nonce value with the encrypted nonce value for checking of message replay and message modification.
Step 7- When the message is genuine than Client will send Accept message which consist of nonce value, IP address of Client, MAC address of Client and message digest consist of nonce value encrypted with public key of Server.
Step 8- When server receives the accept message, he will compare the received IP-MAC with the stored IP-MAC pair, stored nonce value with received nonce value, encrypted message digest is decrypted with the private key of server.
Step 9- If the digest is decrypted than the message is authentic. This means that the received message is from authenticate user. This complete the process of Authentication.
Step 10- Client send request message to server with destination IP Address encrypted with the Public key of the server.
Step 11-Server reply by giving Destination IP-MAC Pair and Public key of destination Client encrypted with the Public key of the Client.
Step 12- Client decrypt the message and store the data and send the message to the client by encrypting with the Public key (PKI) of the client.

4. Result and Discussion:

In this paper we are describing the working of Server Client communication with the help of derived algorithm developed using the MATLAB R2010a based programming language. The algorithm develops a MANET system of sensor nodes distributed randomly in the area of field width 60x60 m^2. Which consists of 9 cells and each cell consist of a single router. All the nodes shown is of Circular shape, Blocking Server with yellow star, Administrating Server with Green star and 9 Router with square boxes colored with black color Fig 1 . The position of nodes changes at every round as the system is dynamic in nature and the position of the nodes changes at every round.

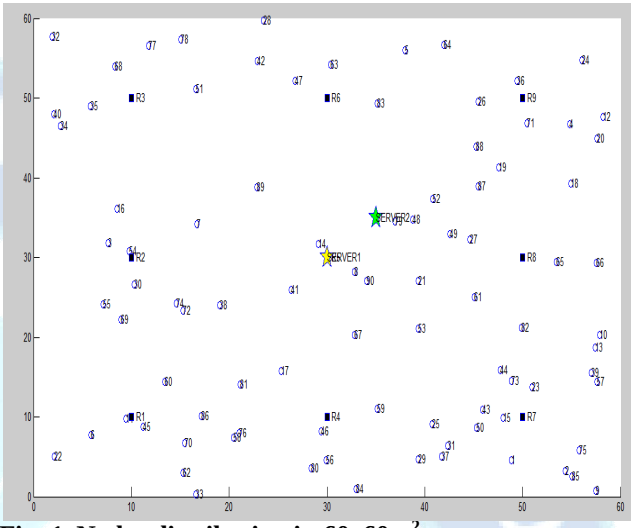

Fig. 1. Nodes distribution in 60x60m^2

When we calculate the complexity of the proposed algorithm, we get that due to inclusion of security the complexity of the proposed algorithm will increase with compared to the base paper used.
The Complexity of Proposed Algorithm is:

$O(n) = n(n+1) + n + n(n+1) + n + n$

$O(n) = n^2 + n + n + n^2 + n + n + n$

$O(n) = O(n^2)$

Note: Highest Degree is taken.

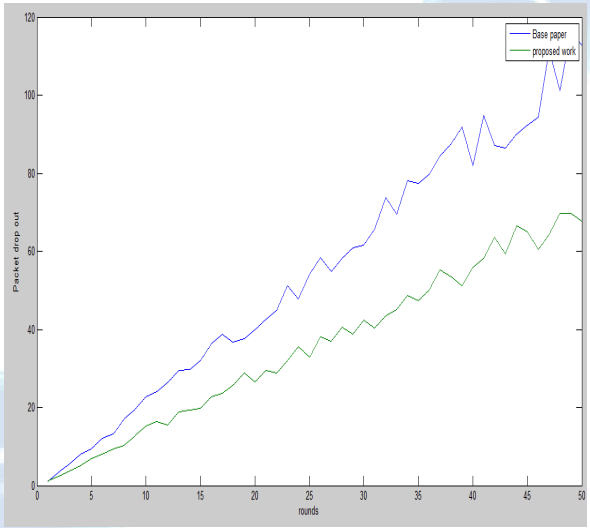

Fig. 2. Packet Drop

This graph shows that in Base Paper the Packet drop will increase after a period of T time as the Blocking Server Database and Allowed Server Database Table stores more data with respect to time and the comparison time will also increase. But in Proposed System the packet drop will depend on many factures such as non availability of client, not interested in communication etc. and there are many

parameters by which comparison of data can be done to reduce time.

5. Conclusion:

In this paper we proposed the secure network between server and clients by using allowed address database, blocked address database and with the help of Invite-Accept Protocol. As ARP has various attacking threats such as MIMA, DOS etc. This makes ARP vulnerable and reduces the guaranty for giving the security to the message send. In this paper the proposed algorithm will try to secure the data by increasing the authentication with the help of nonce value which will be stored at the server database and be given to the clients for authentication purpose. It also fulfill the Integrity of the message as if any intruder changes the value of nonce the received digest value to the client will not match with the calculated digest value and hence proof that the message tempering has been done. Another security which is given was to reduce message replay by frequently sending fresh request value to the active clients by which each time new nonce value would be send. For securing the server a backup server named as Administrating server are introduced so that at the time of failure of the server it acts as the backup for it. Due to high security the complexity of the system has been increased due to which run time will be effected which is calculated with respect to packet loss but security features has been increased more with respect to the previous paper.

References

[1] Weiwei Lang "ARP deception and its prevention" in International Conference on Computer Science and Intelligent Communication (CSIC 2015).

[2] S.Venkatramulu "Various Solutions for Address Resolution Protocol Spoofing Attacks" International Journal of Scientific and Research Publications, Volume 3, Issue 7, July 2013 1 ISSN 2250-3153.

[3] Ahmed M.AbdelSalam "An Automated approach for Preventing ARP Spoofing Attack using Static ARP Entries" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 1, 2014.

[4] Md. Ataullah "ES-ARP: an Efficient and Secure Address Resolution Protocol" 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science 978-1- 4673-1515- 9 2012 IEEE

[5] Gouda,M.G., Huang, C.T.: 'A secure address resolution protocol', Comput.Netw.: Int. J. Comput. Telecommun. Netw., 2003, 41, (1), pp. 57–71

[6] Jun Kim 'Method of Defending Against A Spoofing Attack By Using A Blocking Server' Internation Journal of Network Security Vol.8 No.2 PP.107-118 Mar 2009

[7] Bruschi, D., Ornaghi, A., Rosti, E.: 'S-ARP: a secure address resolution protocol'. Proc. 19th Annual Computer Security Applications Conf.(ACSAC2003), Las Vegas, NV, USA, December 2003, pp. 66–74

[8] Limmaneewichid, P., Lilakiatsakun, W.: 'P-ARP: A novel enhanced authentication scheme for securing ARP'. Proc. 2011 Int. Conf. on Telecommunication Technology and Applications, May 2011,pp. 83–87

[9] Mohamed Al-Hemairy "Towards More Sophisticated ARP Spoofing Detection / Prevention Systems in LAN Networks" 978-1-4244-5757-1/10 ©2009 IEEE