The Research on ARP Protocol Based Authentication Mechanism

Yongzhen Li[1] and Jing Li[2]
[1]School of Yanbian University, Yanji 133002, China
[2]School of Yanbian University, Yanji 133002, China

***Abstract*—ARP protocol is one of the basic agreement in TCP/IP network protocol, but ARP protocol is not safe, because it does not verify the source of the ARP packet is legal or not, in this case lead to variety ARP attack in the local area network (LAN) with the lack of authentication mechanism in ARP protocol, like man-in-middle attack, flooding attack, IP address conflict attack, gateway attack and so on. In this paper, in light of the present condition of the ARP protocol is easy to be attacked, Design authentication mechanism about regulate the request-reply sequence of ARP message and application it in ARP protocol. The simulation result of OPNET indicates new protocol can defense variety of ARP attack effectively in the case of small cost.**

Keywords-ARP protocol;authentication mechanism; ARP attack

I. Introduction

Because of the rapid development of computer networks, every aspect of people have brought great convenience. At the same time, network security has become increasingly prominent problem, variety of network attack means emerge in endlessly, the security and privacy of internet subject to a serious challenge. Security issues have seriously hampered the development of the network, and impede the normal operation of the network. Although security issues of network has received increasingly attention, we are continuously strengthen defense against external threats at the same time, but internal LAN security has become a problem cannot be ignored[1-2]. Since the first ARP virus was found in 2005,by the year 2007,the report CERNET pointed out that the ARP virus is still one of the most serious threat. At present, ARP virus is harmful viruses in the top 5. According to data released of the 360 Internet security center shows, there are 4.97% of user in the average daily suffer from ARP attack, ARP attacks have greatly threaten the security of LAN users[3].

II. ARP protocol and the ARP Attack

A. ARP Protocol

ARP (Address Resolution Protocol), belongs to the link layer protocol, is used to transform the computer's network address (32-bit IP address) into a physical address (48-bit MAC address) [4]. The way of transforming data frames from one host to another host on the LAN is determined by 48-bit Ethernet address (hardware address). To send data, the system kernel must know the hardware address of the destination, and the role of ARP protocol is helping target host use its IP address to obtain the corresponding hardware address.The packet of ARP protocol contains two formats: ARP request packet and ARP reply packet[5]. Packet format as shown in figure 1.

6 Byte	6 Byte	2 Byte	2 Byte	2 Byte	1 Byte	1 Byte	2 Byte	6 Byte	4 Byte	6 Byte	4 Byte
Ethernet destination address	The Ethernet source address	The frame type	Hardware types	Protocol type	The length of MAC	Protocol address length	OP	The sender Ethernet address	The sender IP address	Objective to Ethernet address	The destination IP address

First Part of Ethernet | 28 Byte of ARP request/reply

FIGURE I. ARP PACKET FORMAT

B. ARP Attack

Don’t verify the source’s legality of ARP packets is a big flaw at the beginning of designing ARP protocol. That means when the host receives an ARP reply packet, it does not verify whether it has sent a corresponding ARP requests or verify the credibility of the ARP reply packet. Instead, it directly use the correspondence between MAC address and IP address in the reply packet to replace the corresponding information in original ARP cache table, and the achievement of ARP attack takes advantage of it[6]. Because of lacking certification in the ARP protocol, there are various ARP attacks on LAN such as middle attack, flooding attack, IP address conflict attack, gateway attacks. This article will focus on ARP middleman attacks.

MITM (middle attack) is one of ARP attack that will bring the greatest damage. Before starting to transmit data, if the host does not have the matched mapping relations of IP-MAC , the host will broadcast ARP request and there is no certification in the process. So any host who is in the same subnet can respond to a fake ARP reply packet, the host will trust this reply packet and write mapping relationship of IP-MAC. if an attacker wants to modify the mapping relations between the attacker and someone being attacked, the data transmission between host are exposed to the attacker, while the normal host are unaware of this.

III. AUTHENTICATION MECHANISM OF ARP

As can be seen from the address resolution process, ARP protocol is very simple and efficient, but insecurity, mainly manifested in the following four points:

1) ARP relationship mapping table on host base on dynamic update cache, but there is a time limit on cache refresh, the attacker can modify the cache before it refreshed[7].

2) ARP request packets on the LAN is a broadcast transmission, an attacker can by pretending to be a real host for ARP reply, to intercept real host communication data, finish the attack[8].

3) A host in Ethernet can send any fake ARP reply message.ARP protocol is a stateless protocol, based on an Ethernet on all hosts are trusted, it does not check the packet is legitimate, also do not check if they send ARP request accordingly ,if the destination IP address from reply packet as same as owns, the host will respond, and according to the packet information store or update the ARP table, this is the root cause of ARP attack[9].

4) ARP reply packet lack of authentication mechanism, because of the protocol is considered at the beginning of the design that the LAN communication between all hosts are fully trusted, and consideration of the data transmission speed, so there is not take any security measures in the data link layer, and no corresponding certification in ARP reply[10].

On the above four defects, this paper designed two method to improve the security of protocol. The total design flow chart as shown in Figure 2.

a) ARP attack defense mechanism based on the authentication, to regulate the order of ARP packets, stipulate host must send ARP request firstly, if host receive a corresponding reply packet, the reply packet is considered legitimate; If host do not send ARP request, but received the reply packets from other hosts, the reply packet is considered illegal.

b) *IP - MAC integrity detection based on MD5, the two host must detect bidirectional IP - MAC integrity for the first connection, to calculate MD5 value through the IP-MAC with shared key and add to the packet, received packet host calculate and compare with it. If two md5 value are equal, packet is considered legitimate, otherwise packet is considered illegal*

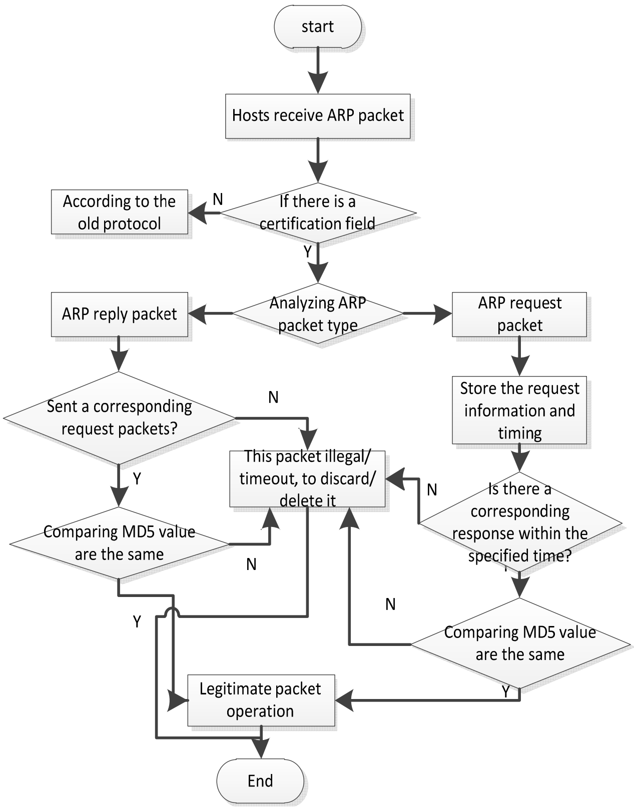

start
Hosts receive ARP packet
According to the old protocol
N
If there is a certification field
Y
ARP reply packet
Analyzing ARP packet type
ARP request packet
Sent a corresponding request packets?
N
Store the request information and timing
This packet illegal/ timeout, to discard/ delete it
Y
N
Is there a corresponding response within the specified time?
Comparing MD5 value are the same
N
N
Y
Comparing MD5 value are the same
Legitimate packet operation
Y
End

FIGURE II. THE TOTAL DESIGN FLOW CHART

IV. The Simulation Experiment of New ARP Protocol

In this paper, taken OPNET as the simulation experiment of new ARP protocol, compared with the old agreement to test efficacy and safety. Simulation experiment have LAN A and LAN B is connected through a router, each LAN is connected by the switch. Network topology is as follows:

A. *A.The Efficiency Test*

Figures 3is the simulation results about Network delay. The figure shows the new protocol slightly delayed compared to the older protocol, but they are in the normal range among 1ms-30ms,hosts simply cannot perceive the difference.

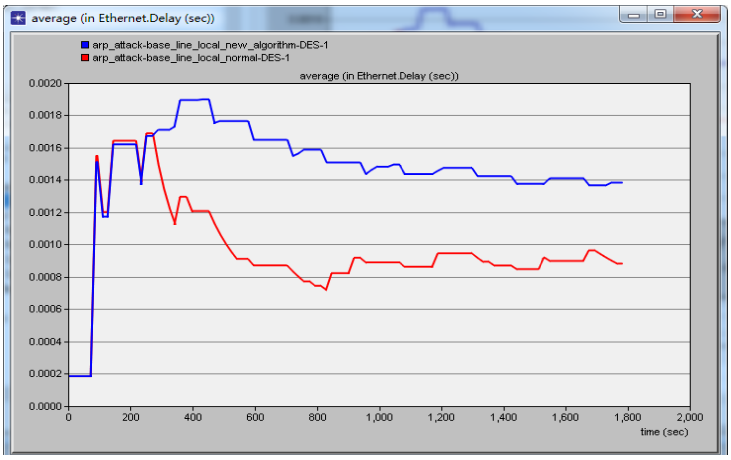
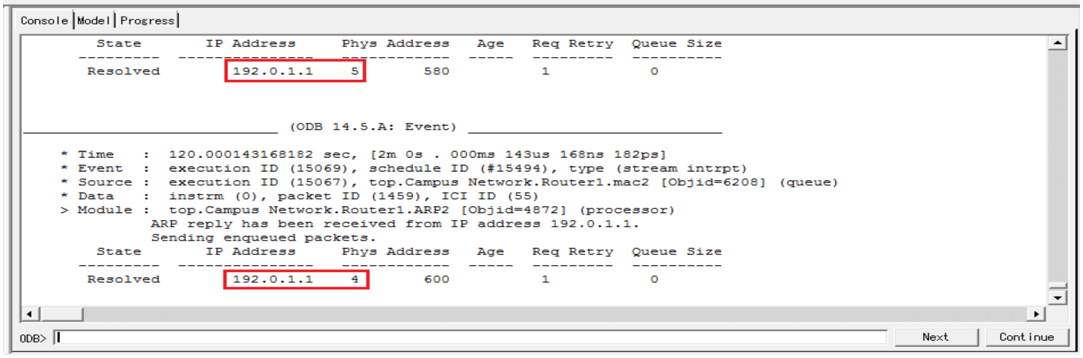


FIGURE III. NETWORK DELAY

B. *B.The Security Test*

Set the B2 node for ARP attack host, attack the router when the network simulation proceeds to 120s. Specifically send a wrong IP-MAC mapping relations reply packet to the router, to see whether to change the ARP table of the router. Figure 4 is a simulation result of the old protocol, can be seen in 120.00014sec, IP address of the server's physical address 192.0.1.1 from the previous 5 becomes 4,resulting in network access to the server's data packet is sent to the physical address of B2 node in which an attacker. Figure 5 is a simulation result of the new protocol, can be seen after the attack, IP address for server 192.0.1.1 physical address has not been tampered with. Simulation results show that the new protocol can effectively prevent such ARP attack, improved security compared to the old protocol.

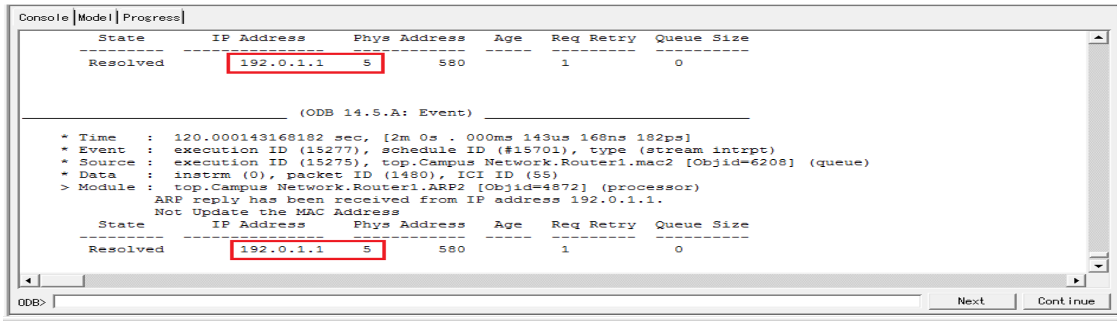


```
        State          IP Address        Phys Address    Age    Req Retry   Queue Size
      ---------    ----------------    ------------    -----    ---------   ----------
       Resolved          192.0.1.1        5         580              1            0


_____________________________ (ODB 14.5.A: Event) ______________________________

     * Time    :  120.000143168182 sec, [2m 0s . 000ms 143us 168ns 182ps]
     * Event   :  execution ID (15069), schedule ID (#15494), type (stream intrpt)
     * Source  :  execution ID (15067), top.Campus Network.Router1.mac2 [Objid=6208] (queue)
     * Data    :  instrm (0), packet ID (1459), ICI ID (55)
     > Module  :  top.Campus Network.Router1.ARP2 [Objid=4872] (processor)
                ARP reply has been received from IP address 192.0.1.1.
                Sending enqueued packets.
        State          IP Address        Phys Address    Age    Req Retry   Queue Size
      ---------    ----------------    ------------    -----    ---------   ----------
       Resolved          192.0.1.1        4         600              1            0
```

FIGURE IV. ARP CACHE FORM OF OLD PROTOCOL UNDER ATTACK



```
        State          IP Address        Phys Address    Age    Req Retry   Queue Size
      ---------    ----------------    ------------    -----    ---------   ----------
       Resolved          192.0.1.1        5         580              1            0


_____________________________ (ODB 14.5.A: Event) ______________________________

     * Time    :  120.000143168182 sec, [2m 0s . 000ms 143us 168ns 182ps]
     * Event   :  execution ID (15277), schedule ID (#15701), type (stream intrpt)
     * Source  :  execution ID (15275), top.Campus Network.Router1.mac2 [Objid=6208] (queue)
     * Data    :  instrm (0), packet ID (1480), ICI ID (55)
     > Module  :  top.Campus Network.Router1.ARP2 [Objid=4872] (processor)
                ARP reply has been received from IP address 192.0.1.1.
                Not Update the MAC Address
        State          IP Address        Phys Address    Age    Req Retry   Queue Size
      ---------    ----------------    ------------    -----    ---------   ----------
       Resolved          192.0.1.1        5         580              1            0
```

FIGURE V. ARP CACHE FORM OFNEWPROTOCOL UNDER ATTACK

V. Conclusion

In this paper, based on the analysis of the old ARP protocol, designeda new ARP protocol based on the authentication mechanism. The new agreement mainly includes:①The order of ARP packets is regulated, avoid to trust protocol with no reply packet authentication. ②To detect integrity mapping relations of IP-MAC, avoid the ARP spoofing attack. Simulation results show s, the new protocol more effective than the old protocol to prevent part of ARP attack, improved the security of the ARP protocol, in the case of spending a small amount of cost. Currently, although to prevent the ARP spoofing attack but cannot stop the flow of attack packets in the network, and author will makes a deeper research in the future.

References

[1] Zhu zhebo:The research and implementation of ARP attack prevention technology(D, Nanjing University of Science and Technology, China 2013).p.1-7.

[2] Guo weixin, Liu xu.MITM Attack Detection Method Based on ARP Cache Overtime. Computer Engineering. Vol. 34 (2008) , p.133-135.

[3] Cui beiliang,Yang xiaojian. On protection againstARP attack w ithin campus network. Journal of Nanjing University of Technology. Vol. 5(2005) ,p.78-81.

[4] Zhang yuqing.The attack and defense technology of network. Tsinghua University Publisher. Vol. 1(2011) ,p.102-109.

[5] Duan dongyan.On the analysis of ARP cheating network monitoring technology and prevention. Science & Technology Information. Vol. 20(2010) ,p.235-238.

[6] V Goyal, R Tripathy.An Efficient Solution to the ARP Cache Poisoning Problem Information Security and Privacy. ACISP. Australasian,2005,p.40-51.

[7] Guo li. Analysis and research based on ARP spoofing monitor exchange network technical (D, Shandong qufu normal university, China 2006). P.28-31.

[8] Gong jingwen. Research of Internet based Remote Intelligent Elevator Monitoring System (D, Wuhan University of Technology, China 2006). P.28-31.

[9] V Ramachandran, S Nandi.Detecting ARP Spoofing:An Active Technique.ICISS. India, 2005, p.239-250.

[10] Zhang huangli, The Study and Implementation of Positive Defence Police with ARP Attack(D, Chongqing University, China 2010). P.5-10.