doi:10.3772/j.issn.1002-0470.2014.03.005

加入盲确认安全机制的地址解析协议①

宋广佳② 季振洲 王 晖

(哈尔滨工业大学计算机科学与技术学院 哈尔滨 150001)

摘 要 对地址解析协议(ARP)的安全性问题进行了研究,指出协议易受攻击的主要原因是协议假定网络上的节点都是可靠的(实际上欺骗节点是存在的),而且将要解析的地址在网络中广播,也没有对应答报文采取验证措施,从而使欺骗节点可以轻易地发起攻击。针对这种情况,提出了一种加入盲确认(BA)机制的地址解析协议(简称 ARPBA),该协议针对 ARP 应答采用二次盲确认,在确认包隐藏了目标 IP 地址,使欺骗节点无法根据目标 IP 进行欺骗,可有效地过滤掉欺骗主机的应答。通过 OPNET 仿真实验表明,ARPBA 有效降低了局域网丢包率和 ARP 缓存表污染率,具有更强的安全性。

关键词 地址解析,地址解析协议(ARP),网络安全,盲确认,仿真

0 引 言

在网络中仅仅知道目标的 IP 地址是不能进行数据传输的,如果要将数据包发送给目标还必须要知道目标的媒体接入控制(MAC)地址,而由 IP 地址获得对应的 MAC 的解析过程就是地址解析协议(address resolution protocol,ARP)完成的主要功能。ARP 是 Internet 重要的基础协议之一。针对地址解析过程的攻击造成的后果是非常严重的,比如典型的中间人攻击,会造成数据被截取、串改,甚至网络通信中断等严重后果,ARP 攻击是局域网安全的主要威胁[1,2]。

目前国内外对地址解析协议(ARP)的安全性研究主要集中在三个方面:(1)防御与检测技术,即采用技术手段对攻击进行防御或者检测已经发生的攻击,对网络中主机的 < IP,MAC > 进行长期监视与记录,一旦发现主机发送的 ARP 报文中 < IP,MAC > 映射与记录中的不符,则认为存在欺骗[3,4](传统的 < IP,MAC > 绑定与划分 VLAN 方法也可归为此类,但该方法属于被动防御,同时增大了网络复杂度与维护成本);(2)改进协议的方式,主要以采用改变协议过程或者增加协议环节的方法来增强安全性[5,6],比如文献[7]中采用在网络中增加一台 DHCP 服务器,并且扩展了 DHCP 协议使其可以完成地址解析过程,但产生了单点故障问题,增加了组网成本;(3)加密通信的方式,比如使用非对称加密技术对 ARP 报文进行加密,防止 IP 地址盗用[8]。虽然 IPv6 中规定可以用 IPSec 保护邻居发现协议(neighbor discovery protocol,NDP)报文,但没有说明如何使用,为此 IETF 小组提出安全邻居发现(secure neighbor discovery,SEND)协议,使用密码生成地址(cryptographically generated address,CGA)、数字签名、时间戳等方法来加密 ND 消息[9],但加密方式存在密钥管理难的问题[7],而且 SEND 协议固有时间复杂度高[10-12],目前仅停留在实验阶段[13],而且加密通信存在一个逻辑问题,即通信双方在加密通信前双方须互相知道 MAC 地址以便能够交换密钥,而这恰恰是 ARP 要实现的,这一过程如果存在欺骗,那么后续的通信保障则失去了意义。本文针对 ARP 攻击的特点对 ARP 进行了改进,提出了一种加入盲确认机制的地址解析协议(ARP with blind acknowledgement,ARPBA),ARPBA 使用二次盲确认的方法对欺骗应答进行过滤,具有更强的安全性。

1 ARP 欺骗原理

局域网工作的每个主机都有一个 ARP 缓存表,

① 国家自然科学基金(61173024)资助项目。

② 男,1981 年生,博士生;研究方向:IPv6 网络,网络安全,实时系统调度等;E-mail:35059899@qq.com

(收稿日期:2013-05-27)

表中存放每台主机的 IP 与 MAC 地址对应关系,当某主机 A 要向主机 B 发送数据包时,首先会在其 ARP 缓存表中查找有无 B 的 IP 地址,如果有则按其对应的 MAC 地址发送数据包,如果没有找到则进行一次 ARP 广播,请求 B 回答其 MAC 地址,局域网内所有主机都可以接收到 ARP 广播包,但只有 B 会回答一个 ARP 应答包,应答包中包含 B 的 IP 地址与 MAC 地址,A 收到这个应答之后就会更新自己的 ARP 缓存表,然后按照表中的 MAC 地址向 B 发送数据[2]。

ARP 虽然简单、高效,但却存在安全隐患。首先,它假定局域网内的主机都是可信的,但实际情况却是网内可能存在由于病毒或恶意程序而产生的恶意欺骗主机。其次,缺少确认机制,比如主机 A 要与 B 进行通信,在进行 ARP 广播之后,在收到 ARP 应答包时,不会检查自己是否发送过 ARP 请求,或者应答是否是真实的,只要对方的 ARP 包中的 MAC 地址是自己的,A 都会更新自己的 ARP 缓存表,这为局域网的 ARP 欺骗提供了便利条件。一种常见的欺骗方式如图 1 所示。

当主机 A 广播 ARP 请求要求主机 B 回答时,主机 C 不断进行 ARP 应答,谎称自己是主机 B,则 A 收到应答后并不知道这是冒充的报文,则会误更新自己的 ARP 缓存表,将 C 当作 B,并将本应发送给 B 的数据包发送给 C,从而形成了 ARP 欺骗[2]。ARP 协议数据包格式如下:

以太网头部	以太网目的地址 以太网源地址 协议类型
IP数据	ar_hrd ar_pro ar_hln ar_pld ar_op ar_sha ar_spa ar_tha ar_tpa

图 1 ARP 数据包格式

图 1 中几个重要字段的值如下:

ar_hrd:硬件类型,以太网为 1;

ar_pro:协议类型,IP 协议为 0x0806;

ar_op:操作类型,ARP 请求为 1,ARP 应答为 2。

2 加入确认应答机制的 ARP 协议

从逻辑角度来分析,C 之所以能够对 A 造成欺骗,原因之一是 C 知道 A 正在寻找 B,如果 C 不知道 A 寻找的是谁,就很难对 A 造成欺骗。

改进后的协议加入了确认应答机制,并且增加了两种新的 ARP 包:ARP 确认包与 ARP 确认应答包。ARP 确认包的操作类型字段为 3,目标 IP 地址为全 0,ARP 确认应答包操作类型为 4,目标 IP 地址为本机 IP,改进后的 ARP 协议过程如图 2 所示。

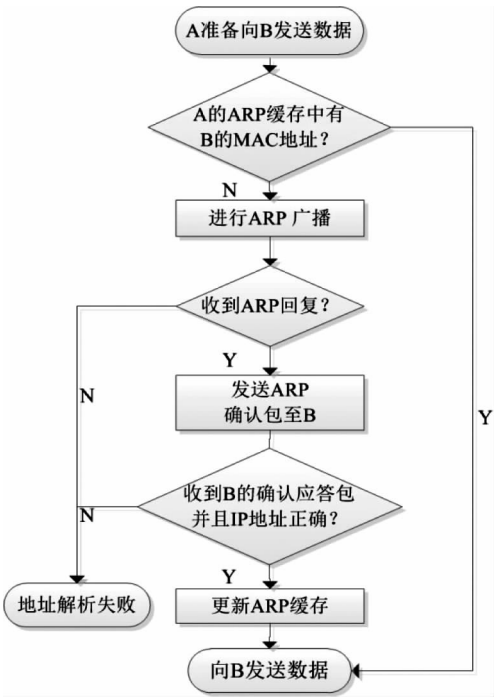

图 2 ARPBA 协议过程

新协议的地址解析过程如下:

当主机 A 要向目的主机发送数据时,首先查找自己的 ARP 缓存表,如果找到了 B 的 IP 地址,则直接按照表中对应的 MAC 地址发送数据,如果没找到,则 A 进行一次 ARP 广播,如果没有收到 ARP reply 则 ARP 失败,否则发送 ARP 确认包,确认包的操作代码为 3,目的 IP 为全零,如果目的主机发送回的确认返回包中的 IP 地址是正确的(即 A 广播时要找的地址)则 A 就更新自己的 ARP 缓存表,然后向应答主机发送数据,如果 IP 地址不对则 ARP 确认失败。

假设局域网有 A,B,C 等多台主机,IP 与 MAC 地址见表 1。

表 1 主机 IP 与 MAC 地址

主机	IP 地址	MAC 地址
A	172.20.0.1	AAAA:AA:AA:AA:AA
B	172.20.0.2	BB:BB:BB:BB:BB:BB
C	172.20.0.3	CC:CC:CC:CC:CC:CC

当 A 要想 B 发送数据时会先查找自己的 ARP 缓存表,如果找到 B 的 IP 地址则直接按照表中对应的 MAC 地址发送数据,如果没有找到,则 A 进行 ARP 广播,包格式见图 3 中主机 A 的 ARP 广播包。

广播包	应答包
FF:FF:FF:FF:FF:FF	FF:FF:FF:FF:FF:FF
AA:AA:AA:AA:AA:AA	CC:CC:CC:CC:CC:CC
0x0806	0x0806
1	1
0x0800	0x0800
6	6
4	4
1	2
AA:AA:AA:AA:AA:AA	CC:CC:CC:CC:CC:CC
172.20.0.1	172.20.0.2
00:00:00:00:00:00	AA:AA:AA:AA:AA:AA
172.20.0.2	172.20.0.1

图 3　ARP 广播包与应答包

确认包	确认应答包
FF:FF:FF:FF:FF:FF	FF:FF:FF:FF:FF:FF
AA:AA:AA:AA:AA:AA	CC:CC:CC:CC:CC:CC
0x0806	0x0806
1	1
0x0800	0x0800
6	6
4	4
3	4
AA:AA:AA:AA:AA:AA	CC:CC:CC:CC:CC:CC
172.20.0.1	172.20.0.2
CC:CC:CC:CC:CC:CC	AA:AA:AA:AA:AA:AA
0.0.0.0	172.20.0.1

图 4　确认包与确认应答包

如果广播之后收到了应答,是 C 冒充的,C 应答包见图 3 中主机 C 的 ARP 应答包。A 会发出 ARP 确认,包中操作类型为 3,目的 IP 地址为全零,格式见图 4 中左侧 ARP 确认包。如果 C 为欺骗主机,在收到 ARP 确认包后不知道确认返回包应填入的 IP 地址,而 A 只有在收到正确的确认返回包后才会更新自己的 ARP 缓存表,即使 C 保存了 A 在一段时间内发出的 ARP 请求,但却无法知道 A 要对哪一次请求进行确认,因此无法进行欺骗。我们把这种确认方式称作盲确认,改进后的协议则叫做 ARPBA。

3　实验与分析

实验采用模拟局域网的方式,拓扑图为星型结构,中间一个交换节点,外围 16 个节点,其中 15 个为普通节点,1 个为欺骗节点。

节点内部模型包含两个发包源,一个为 ARP 发包源,完成 ARP 包的发送,为模拟操作系统,节点每隔 1 秒进行一个 ARP 轮询,另一个为业务数据包源节点内部处理模块的有限状态机见图 5。两个发包源数据分布分别采用黑龙江中医药大学核心交换机(华为 9306)30 天多播流量统计及平均流量统计,数据采集软件为 SolarWinds orion network performance monitor,数据见图 6 与图 7。

共进行了 2 次实验,分别模拟 ARP 协议与 ARPBA 协议,实验测试在局域网有一台 ARP 欺骗主机情况下节点的丢包率与 ARP 缓存表污染率。丢包率为目标机收到的包数与源主机向其发送的总包数的比值,污染率为 ARP 表中错误条目与 ARP 表总条目比值。

图 8 与图 9 分别是 ARP 与 ARPBA 的丢包率情况,通过对比可发现 ARPBA 的丢包率明显低于 ARP 丢包率,因为在 ARP 协议中,只要收到欺骗主机发送 ARP 应答包,源主机就会更新 ARP 缓存表,进而造成丢包,而在 ARPBA 中采用了盲确认机制,是欺骗主机的 ARP 应答很难通过确认,即使采用了随机地址进行应答,通过的几率也是非常低的。图 10与图 11 分别是 ARP 与 ARPBA 的 ARP 缓存表污染率,可见在 ARP 缓存表污染率方面,ARPBA 也优于 ARP。

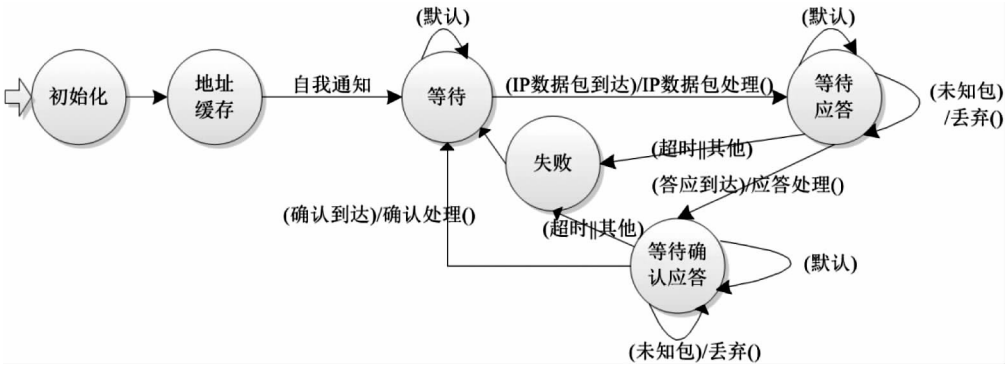

图 5　ARPBA 有限状态机

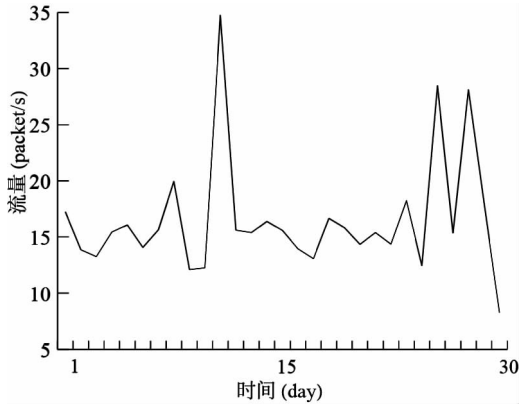

图 6 30 天多播数据流量

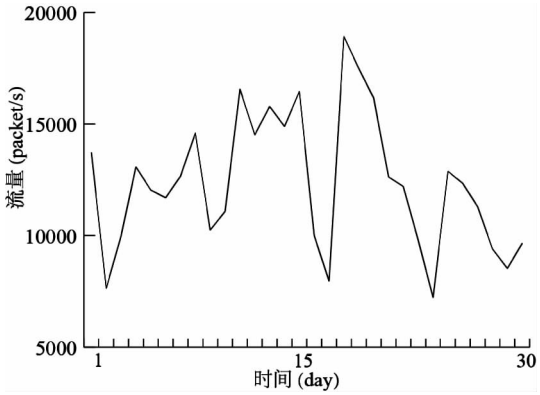

图 7 30 天平均流量

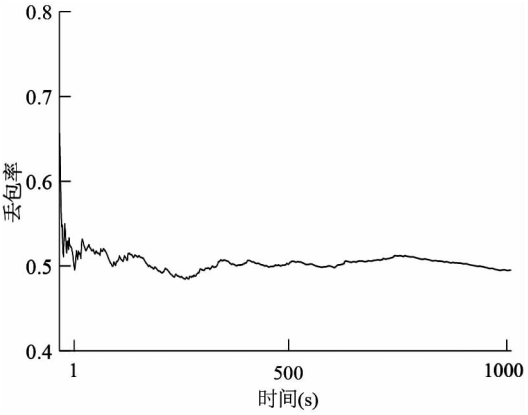

图 8 ARP 丢包率

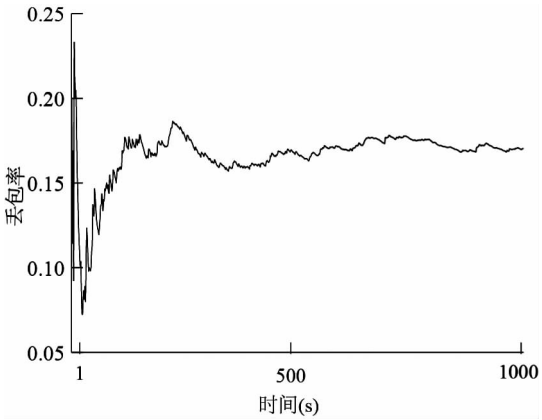

图 9 ARPBA 丢包率

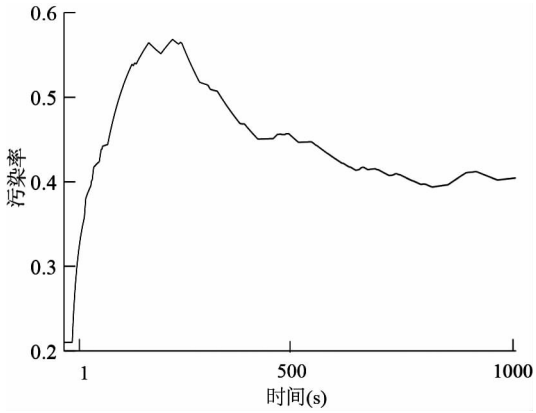

图 10 ARP 缓存表污染率

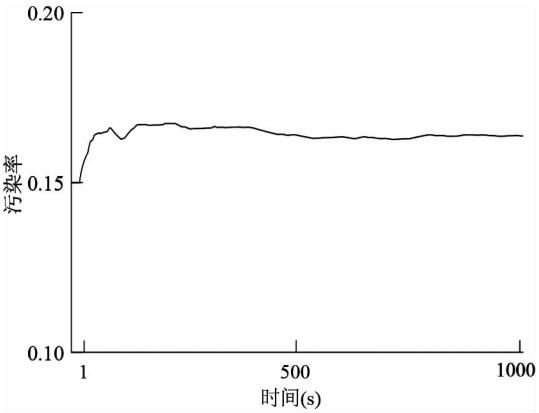

图 11 ARPBA 缓存表污染率

4 结 论

ARP 协议是 Internet 重要的基础协议之一,其主要功能是在数据传输过程中完成由目标 IP 地址到目标 MAC 地址的解析过程,协议的安全性尤为重要,因为地址解析过程安全性一旦失去保障,那么上层协议通信将面临极大威胁。本文通过对 ARP 协议原理与 ARP 攻击方式进行研究,指出协议易受攻击的主要原因是错误地假设网络中所有节点都是可靠的,而现实情况是由于恶意程序及病毒影响,不可信节点是广泛存在的,并且 ARP 将目标解析地址在网络中广播,没有对应答报文采取任何验证措施,使欺骗节点可以轻易发起攻击而不付出任何代价。本文针对性地提出了一种加入确认机制的协议 ARP-BA,此协议对 ARP 应答报文采取逆向盲确认,并在确认包中隐藏了目标 IP 地址,使欺骗节点无法根据目标 IP 伪造应答报文,因此无法通过验证。仿真实验表明,ARPBA 的盲确认机制可以有效过滤掉欺骗主机的伪造 ARP 应答,可有效降低局域网丢包率和地址缓存表污染率,大幅提高了网络安全性。

参考文献

[1] 谢希仁. 计算机网络. 第四版. 北京:电子工业出版社, 2004. 183-185

[2] 秦丰林,段海新,郭汝廷. ARP 欺骗的检测与防范技术综述. 计算机应用研究,2009,26(1):30-33

[3] Nam Seung Yeob, Kim D W, Kim J. Enhangced ARP: preventing ARP poisoning-based Man-In-the-Middle attacks. *IEEE Commnication Letters*, 2010, 14(2): 187-189

[4] M Oh, Y-G Kim, S Hong, et al. ASA: agent-based secure ARP cache management. *IET Communications*, 2012, 6(7): 685-693

[5] 胡清桂. 一种新的 ARP 协议改进方案. 陕西科技大学学报,2011,28(5):81-86

[6] 黄天福,白光伟. 基于改进协议机制的防 ARP 欺骗方法. 计算机工程,2008,34(14):168-170

[7] Biju Issac, Lawan A. Mohanmmed. Secure unicast address resolution protocol (S-UARP) by extending DHCP. In: Proceedings of the 13th IEEE International Conference on Networks Jointly Held with the 7th IEEE Malaysia International Conference on Communications, koala Lumpur, Malaysia, 2005. 363-368

[8] Goyal V, Tripathy R. An efficient solution to the ARP cache poisoning problem. *Lecture Notes in Computer Science*, 2005: 40-51

[9] J Arkko, ED Ericsson, Kempf J. Secure Neighbor Discovery (SEND). http://tools. IETF. org/html/rfc3971: IETF, 2005

[10] Hayoung Oh, Kijoon Chae. An efficient security management in IPv6 network via MCGA. In: Proceedings of the 9th IEEE International Advanced Conference on Communication Technology, Pnoenix Park, Korea, 2007. 1179-1181

[11] Su G X, Wang W D, Gong X Y. A quick CGA generation method. In: Proceedings of the 2th IEEE Internationa Conference on Future Computer and Communication, Wuhan, China, 2010. 769-773

[12] AlSa'deh A, Rafiee H, Meinel C. Stopping time condition for practical IPv6 cryptographically generated addresses. In: Proceedings of the 26th IEEE International Conference on Information Networking, Bali, Indonesia, 2012. 257-262

[13] Rafiee H, AlSa'deh A, Meinel C. Winsend: windows secure neighbor discovery. In: Proceedings of the 4th International Conference on Security of Information and Networks, Sydney, Australia, 2011. 243-246

An address resolution protocol with blind-acknowledgement mechanism

Song GuangJia, Ji ZhenZhou, Wang Hui

(School of Computer Science and Technology, Harbin Institute of Technology, Harbin 150001)

Abstract

The security issues of address resolution protocol (ARP) were studied, and the conclusions were drawn that ARP networks are more easily attacked by deceive nodes because the ARP assumes that all network nodes are reliable (actually not) and it broadcasts the addresses which need resolving in the networks. In order to overcome the above disadvantages, a novel improved ARP with a Blind-Acknowledgement mechanism (ARPBA) was proposed. The protocol uses reverse blind acknowledgement to check ARP replies. Since a destination IP address is hidden in the acknowledgement packet, malicious nodes cannot deceive according to the destination IP. Moreover it can effectively filter out the spoofing replies. The OPNET simulation experiments showed that ARPBA had the stronger security by effectively reducing the LAN packets loss rate and the ARP cache table contamination rate.

Key words: address resolution, address resolution protocol (ARP), network security, blind-acknowledgement, simulation