文章编号:1001 - 9081(2005)12 - 2911 - 03

移动 IPv6 动态家乡代理地址发现的安全性研究

李 刚
(中国科学技术大学 电子工程与信息科学系,安徽 合肥 230027)
(garth@mail.ustc.edu.cn)

摘 要:分析了动态家乡代理地址发现过程的安全特性,提出了一个对此过程进行安全保护的方案。该方案通过移动节点和家乡代理之间的双向认证和对家乡代理地址列表进行加密传输的方法,对动态家乡代理地址发现过程提供了安全保护,使该过程能够抵御恶意节点的拒绝服务攻击和对家乡链路信息的窃取。对这一方案的性能进行了评估,并在移动 IPv6 示范网络中进行了实现。

关键词:移动 IPv6;动态家乡代理地址发现;任播地址;IPsec
中图分类号: TP393.17 **文献标识码**:A

Research on the security of mobile IPv6 dynamic home address discovery

LI Gang
(*Department of Electronic Engineering and Information Science, University of Science and Technology of China, Hefei Anhui* 230027, *China*)

Abstract: The security feature of DHAAD(Dynamic Home Agent Address Discovery) procedure was analyzed, and a solution was proposed to protect it. The solution authenticated the bi-directional DHAAD messages between mobile node and home Agent, and encrypted the home Agent address list in the message from home Agent to mobile node. The solution can protect the DHAAD procedure against Denial-of-Service attack and the theft of information on home link. Then the evaluation of the solution was given, and it was realized in the Mobile IPv6 demonstration network.

Key words: mobile IPv6; Dynamic Home Agent Address Discovery(DHAAD); anycast address; IPsec

0 引言

移动 IPv6 技术[1]使节点在不同的接入网之间移动时,能够沿用同一个 IPv6 地址,同时保持不中断的网络连接和应用服务。移动 IPv6 技术通信灵活且支持 IPv6。

移动 IPv6 通信的安全保障是其大规模部署和应用的前提。目前主要使用 IPsec 来保护移动 IPv6 通信:首先在移动节点和家乡代理之间建立 IPsec 安全关联,随后用此安全关联来保护移动 IPv6 的通信。IPsec 安全关联的两端只能是全局单播的 IPv6 地址。在动态家乡代理地址发现(Dynamic Home Agent Address Discovery,DHAAD)过程中,移动节点需要和家乡代理任播地址进行通信,而移动节点无法和任播地址之间建立安全关联。因此 DHAAD 过程无法使用通常的 IPsec 方法进行保护。

文献[2]对 DHAAD 过程提出了基于单向认证的安全保护方案,但没有完成对参与 DHAAD 过程的双方的双向认证,也没有实现对家乡代理地址列表的加密传输。本文在分析 DHAAD 过程的安全特性的基础上,提出一种使用双向认证和内容加密的安全保护方案(Bi-directional Authentication and Content Encryption,BACE)。采用这一方案的动态家乡代理地址发现过程能够抵御恶意节点利用 DHAAD 过程进行的拒绝服务攻击,防止恶意节点通过侦听数据包而窃取家乡链路的信息。

1 移动 IPv6 协议简介

使用移动 IPv6 协议进行通信的移动节点(MN)一般具有两个 IPv6 地址,一个是具有家乡链路前缀的家乡地址,其他节点将通过家乡地址来向该移动节点寻址。一个是移动到外地时,在外地的接入网络中通过无状态地址自动配置等机制而获得的转交地址。

处于外地链路的 MN 必须通过位于家乡链路上的一个家乡代理(HA)的帮助才能使用移动 IPv6 通信。如图 1 所示,处于外地链路的 MN 拥有了转交地址后,将向位于家乡链路的家乡代理发送绑定更新(BU)报文,HA 回送绑定应答(BA)消息给 MN,这一过程称之为家乡注册过程。家乡注册成功后,HA 将别的节点(CN)发往 MN 的家乡地址的数据包经过 HA-MN 隧道转发到 MN 的转交地址。同时 MN 将通过与 CN 之间的一系列消息交换而在 CN 上建立 MN 的家乡地址和转交地址之间的绑定。此后 MN 和 CN 之间可以直接采用路由优化方式进行通信。

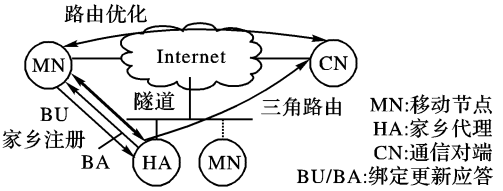

图 1 移动 IPv6 的通信原理

文献[3]描述了采用 IPsec 保护移动 IPv6 通信报文的具体方法。处于外地链路的移动节点在家乡注册过程之前,先向家乡代理发起建立 IPsec 安全关联的过程,随后的家乡注册过程以及与家乡代理之间的其他通信均由这个安全关联保护。IPsec 安全关联的建立是通过移动节点和家乡代理之间

收稿日期:2005 - 06 - 22;**修订日期**:2005 - 08 - 25
作者简介:李刚(1978 -),男,江苏淮安人,硕士研究生,主要研究方向:下一代 Internet 网络技术、移动 IPv6 技术.

的 Internet 密钥交换(IKE)[4]来实现的。

2 DHAAD 过程的安全分析

2.1 DHAAD 过程描述

在实际的移动 IPv6 应用中,在外地启动的移动节点可能并不知道自己的家乡代理地址,或者自身保存的家乡代理地址已经过期了,或者移动节点所使用的家乡代理在通信中发生了变化(比如家乡代理死机或重新启动等)。在这些情况下,移动节点需要一个能够自动获得可用的家乡代理的机制。移动 IPv6 动态家乡代理地址发现过程正是为了满足这种需求而设计。

DHAAD 过程如图 2 所示。移动节点在不知道可用的家乡代理地址的时候,向家乡链路发送 DHAAD 请求报文,报文的目的地址是家乡链路上的家乡代理任播地址。家乡链路上第一个收到 DHAAD 请求报文的家乡代理将拦截此报文,并回送一个包含家乡链路上所有可用的家乡代理的地址的 DHAAD 应答报文。移动节点收到 DHAAD 应答报文后,将按照一定的选择策略,从应答报文中包含的家乡代理地址列表中选择一个家乡代理地址尝试进行家乡注册过程,如果成功,则进行家乡注册,移动节点随后便可以启动移动 IPv6 通信;如果失败,则从家乡代理地址列表中再选出一个进行家乡注册过程。如果对家乡代理地址列表中的家乡代理地址的家乡注册过程均告失败,移动节点便重新发起 DHAAD 过程。

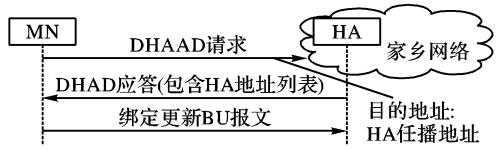

图 2 DHAAD 过程描述

2.2 DHAAD 过程的安全漏洞

从上节的过程描述可见,参与 DHAAD 过程的双方缺乏进行身份认证的机制。恶意节点可以轻易的伪装成移动节点或家乡代理。如果恶意节点伪装成家乡代理,则可以利用 DHAAD 过程对移动节点进行拒绝服务(DoS)攻击。

如图 3 所示,处于移动节点和家乡链路之间的恶意节点侦听到 MN 发出的报文后,便可以向 MN 发送包含虚假的家乡代理(HA)地址列表的 DHAAD 应答报文。MN 收到恶意节点发来的 DHAAD 应答报文后,便向报文中包含的 HA 地址逐一进行家乡注册过程。

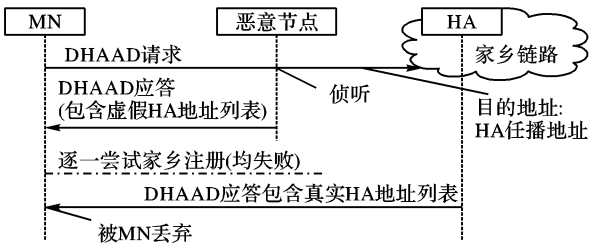

图 3 移动节点受到的 DoS 攻击

如果 MN 采用 IPsec 来保护和 HA 之间的通信,那么 MN 不会成功地向虚假的 HA 地址进行家乡注册,但是 MN 将为尝试向这些虚假的 HA 地址进行家乡注册而耗费时间和资源。当 DHAAD 请求报文发送到家乡链路后,第一个收到此报文的 HA 将向 MN 发送包含真实 HA 地址列表的 DHAAD 应答报文。而 MN 在发出 DHAAD 请求报文后只会对所收到的第一个 DHAAD 应答报文进行处理,因此,如果 MN 先收到假造的 DHAAD 应答报文,HA 发来的真实的 DHAAD 应答报文将被 MN 丢弃。

由此可见,恶意节点不需要拦截 MN 发出的 DHAAD 请求报文,而只需要侦听到这一报文,随后立刻发送虚假的应答报文给 MN,MN 就不得不向虚假的 HA 地址进行家乡注册过程。MN 尝试完所有虚假的 HA 地址后,将重新发出 DHAAD 请求,恶意节点可以不断地侦听 MN 发出的 DHAAD 请求报文,并构造出虚假的 DHAAD 应答报文,先于家乡链路而发送给 MN。这样 MN 将重复进行无用的家乡注册过程,而无法联系上真实的家乡代理,从而无法启用移动 IPv6 通信。恶意节点通过这种方式,阻止 MN 进行移动 IPv6 通信,从而实现了对 MN 的 DoS 攻击。

同时当恶意节点伪装成 MN 时,向家乡代理任播地址发出 DHAAD 请求报文,便可以轻易地收到包含家乡链路上的所有的 HA 地址信息的 DHAAD 应答报文。或者恶意节点可以侦听家乡链路发往合法的移动节点的 DHAAD 应答报文。由于 DHAAD 应答报文中的 HA 地址信息是明文传输的,这样的操作造成了家乡链路上重要信息的泄漏。恶意节点可以利用这些信息对家乡链路进行进一步的攻击。

3 BACE 方案

本文在分析 DHAAD 过程的特点的基础上,提出了一个基于双向认证和内容加密的安全保护方案 BACE。其中双向认证指的是移动节点和家乡代理都能够证实对方的身份,内容加密指的是对 DHAAD 应答报文所传输的家乡代理地址列表进行加密传输。

3.1 方案的前提条件

BACE 方案要求 MN 已经预先和家乡链路上的所有的 HA 共享了某些密钥信息,即一个预共享密钥 pre-shared key (PSK)。HA 和 MN 都可以利用 MN 的身份标识(MN-NAI)在自身的数据库中找到对应的 PSK。此 PSK 在本方案中用于 MN 和 HA 之间进行双方认证。同时,在需要对 HA 地址列表进行加密时,如果 MN 和 HA 协商使用对称密钥加密方法,MN 和 HA 上需要预先存储用于加密 HA 地址列表的密钥信息 eKey。

3.2 方案的报文格式

本方案对 DHAAD 过程中交换的报文(请求和应答报文)的格式进行了修改和扩充。图 4 描述了本方案的报文格式。

DHAAD请求报文

类型(144)	代码(0)	校验和
序列号(id)	E	保留
MN-NAI选项		
认证选项		

DHAAD应答报文

类型(144)	代码(0)	校验和
序列号(id)	E	保留
HA-NAI选项		
MN-NAI选项		
认证选项		
HA地址列表		

图 4 BACE 方案的报文格式

DHAAD 请求报文和应答报文的 ICMPv6 类型值分别为 144 和 145。MN-NAI 和 HA-NAI 选项分别携带 MN 和 HA 的身份标识[5]。本文使用两个报文的“保留”域中的第一个比特(称为 E 比特)来标识是否对 HA 地址列表进行加密。

3.3 方案的操作流程

1)MN 利用自己的身份标识 MN-NAI、转交地址(CoA)、随机生成的 DHAAD 会话序列号 id、和预共享密钥 PSK,计算

出一个哈希值:HASH_REQ,公式(1)是 HASH_REQ 的计算公式。然后构造 DHAAD 请求报文,报文的源地址是 MN 的转交地址,目的地址是家乡代理任播地址,报文中的认证选项内容即为 HASH_REQ。如果 MN 希望 HA 将 HA 地址列表加密后传输,便设置 E 比特为 1。然后 MN 发出此请求报文。

HASH_REQ = First(96, HMAC_SHA1(PSK | id | MN-NAI | CoA)　　(1)

其中:HMAC_SHA1 是一种基于密钥进行认证的单向哈希函数; First(96, x)表示取 x 的前 96 位。

2)位于家乡链路上的某个 HA 收到 DHAAD 请求报文后,首先根据报文中的 MN-NAI 寻找与之对应的 PSK,随后根据公式(1)重新计算哈希值 HASH_REQ,如果计算结果与报文中的认证选项的内容一致,则通过对 MN 的身份验证。

如果 DHAAD 请求报文中的'E'位为 1,HA 便根据 MN-NAI 找出对应的密钥 eKey,并使用 eKey 将自身搜集的 HA 地址列表加密成密文,此密文将放置在 DHAAD 应答报文的 HA 地址列表域中。

3)HA 产生自己的身份验证值。HA 使用自身地址、MN-NAI、HA-NAI、DHAAD 请求报文中的 id、加密后的 HA 地址列和 PSK,计算出另一个哈希值:HASH_REP,计算公式如公式(2)所示。然后构造一个 DHAAD 应答报文,包含值为 HASH_REP 的认证选项和加密后的 HA 地址列表。报文中的'E'比特置 1,以告知 MN 其中的 HA 地址列表是加密的。然后 HA 将此应答报文发送给 MN。

HASH_REP = First(96, HMAC_SHA1(PSK | id | MN-NAI | HA-NAI | IP_HA | HA_List)　　(2)

其中:IP_HA 是接收到 MN 的 DHAAD 请求报文的家乡代理地址; HA_List 是家乡链路上可用的家乡代理地址列表,如果第 2)步中采用加密传输,则这里的 HA_List 是加密的地址列表。

4)MN 收到 DHAAD 应答报文后,首先验证 HA 的身份,即根据公式(2)重新计算 HASH_REP,如果得出与应答报文中的认证选项相同的值,则通过对 HA 的认证。

如果 MN 发出的 DHAAD 请求报文中的 E 比特置 1,而且收到的 DHAAD 应答报文中的 E 比特也为 1,则认为 HA 已经将 HA 地址列表加密传输。MN 使用与 MN-NAI 相应的密钥 eKey 对 HA 地址列表进行解密。

5)经过上述步骤,MN 已经安全地得到了合法的 HA 发来的 HA 地址列表。随后 MN 从列表中逐一选择 HA 地址,进行家乡注册过程。

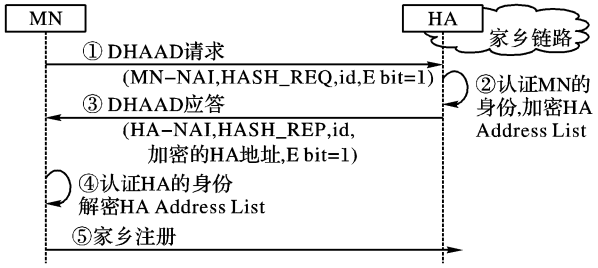

图 5　BACE 方案的操作流程

4　方案的实现和性能评估

本文提出的 BACE 方案已经在实验室的移动 IPv6 示范网中实现。图 6 显示了本文实现的方案抵御恶意节点对家乡链路攻击的情况。为了简单起见,家乡链路上的 HA 同时作为家乡链路和核心网之间的路由器。MN 和 HA 在 DHAAD 过程中通过预先共享的密钥完成了双向认证。处于核心网中的恶意节点向家乡链路发出的 DHAAD 请求报文因无法通过 HA 对恶意节点的身份认证而被丢弃。并且由于 HA 地址列表是加密传输,恶意节点即使侦听到 DHAAD 应答报文后,也因不知道密钥而无法解密出家乡链路上的 HA 地址信息。

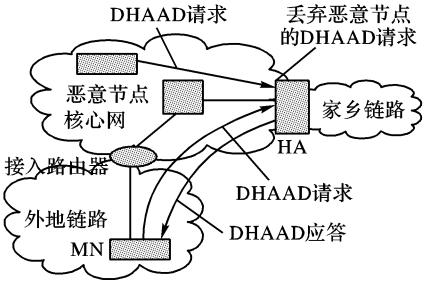

图 6　BACE 方案的实现

同时,本文也模拟了恶意节点对 MN 进行的 DoS 攻击。恶意节点将因为不知道 MN 与家乡链路预先共享的 PSK 而无法得出合法的身份验证值 HASH_REP,MN 收到恶意节点发来的假造的 DHAAD 应答报文后,将因为通不过对 HA 的身份验证而丢弃假造的应答报文,并且继续等待由家乡链路发来的真实的 DHAAD 应答报文。因此,本方案可以有效地防御恶意节点对移动节点的 DoS 攻击。

本方案通过 MN 和 HA 之间的双向认证,以及可选的 HA 地址列表的加密功能,实现了对 DHAAD 过程的安全保护。同时,本方案的实现简单,只需要对现有的移动 IPv6 网络部署和移动 IPv6 协议功能模块进行较小的改动,就可以对 DHAAD 过程进行安全保护。

5　结语

动态家乡代理地址发现过程的安全保护是移动 IPv6 协议中需要特殊考虑的问题。本文在对动态家乡代理地址发现过程的安全性进行分析的基础上,提出了基于双向认证和内容加密的 BACE 方案。本方案能够有效地抵抗恶意节点对移动节点的拒绝服务攻击,并且能够防止家乡链路的信息泄漏。

本方案作为移动 IPv6 协议的安全扩展,应用于大规模的移动 IPv6 部署中,可以加强对移动 IPv6 通信的安全保护,提高移动 IPv6 系统的稳定性和安全性。

参考文献:

[1] JOHNSON D, PERKINS C, ARKKO J. Mobility Support in IPv 6, RFC3775[S]. 2004.

[2] SUN Q, MU L, HASSAN M, *et al*. Security Issues in Dynamic Home Agent Address Discovery[EB/OL]. http://www.watersprings.org/pub/id/draft-sun-mipv6-dhaadsecurity-00.txt, 2004 - 11.

[3] ARKKO J, DEVARAPALLI V, DUPONT F. Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents. RFC3776[S]. 2004.

[4] HARKINS D, CARREL D. The Internet Key Exchange (IKE), RFC2409[S]. 1998.

[5] PATEL A, LEUNG K, AKHTAR H. Network Access Identifier Option for Mobile IPv6[EB/OL]. http://www.watersprings.org/pub/id/draft-ietf-mip6-nai-option-00.txt, 2004.