移动 IPv6 路由优化安全方案

黄志彬,洪佩琳
HUANG Zhi-bin,HONG Pei-lin

中国科学技术大学 信息网络实验室,合肥 230027
Laboratory of Information Networks,University of Science & Technology of China,Hefei 230027,China
E-mail:zhibin@mail.ustc.edu.cn

HUANG Zhi-bin,HONG Pei-lin.Proposal of route optimization security in mobile IPv6.Computer Engineering and Applications,2009,45(6):120-123.

Abstract: Mobile IPv6 provides mobility support for the IPv6 Internet.Route optimization eliminates the triangular routing problem existing between the mobile node and correspondent node in mobile IP.However,mobile IPv6 brings some security threats at the same time,a great part of the threats are about the authorization and authentication problem of binding update in route optimization.Some security threats still exist in the return routability protocol and CGA-based protocol,the CAM-DH protocol is improved,a new enhanced protocol is proposed,the security is improved,and the computation and message exchange performance is optimized.

Key words: mobile IPv6;route optimization;return routability;Cryptographically Generated Addresses (CGA);Child-proof Authentication for MIPv6-Diffie-Hellman(CAM-DH)

摘 要:移动 IPv6 为 IPv6 网络提供移动性支持,移动 IPv6 路由优化消除了移动 IP 中移动节点和通信对端存在的三角路由问题。但同时,移动 IPv6 也引入了一些安全上的威胁,其中有很大一部分是关于路由优化中的绑定更新的授权和认证问题。传统的返回可路由机制和 CGA 生成家乡地址的方法仍然存在安全上的问题,在 CAM-DH 协议的基础上进行改进,提出了一种新的增强方案,提高了安全性,优化了计算负载和报文交换性能。

关键词:移动 IPv6;路由优化;返回可路由机制;CGA 地址;CAM-DH 协议
DOI:10.3778/j.issn.1002-8331.2009.06.034 **文章编号**:1002-8331(2009)06-0120-04 **文献标识码**:A **中图分类号**:TP393

1 引言

移动 IPv6 协议为 IPv6 网络提供了移动性支持,采用移动 IPv6 协议的移动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。IETF 在移动 IPv6 协议的标准文档 RFC3775 中[1],实现了对移动IPv6 协议操作的标准化。

在移动 IP 中,移动节点(Mobile Node,MN)同时拥有家乡地址(Home Address,HoA)和转交地址(Care-of Address,CoA)。MN 在他的家乡网络拥有一个家乡地址,当 MN 移动到外地网络时,会分配到一个新地址作为 MN 的转交地址。为了能够同通信对端(Correspondent Node,CN)继续保持通信,MN 把这个转交地址和 MN 的家乡地址进行绑定,并向 MN 的家乡代理(Home Agent,HA)发送绑定更新(Binding Update,BU)报文,家乡代理在绑定缓存(Binding Cache)中记录这个绑定关系。CN 向 MN 的家乡地址发送报文,这些报文将被送往 MN 的家乡链路,家乡代理截获这些报文,封装好通过隧道发送给 MN。这样,CN 和 MN 之间形成了一个“三角路由”。

移动 IPv6 支持的路由优化很好地解决了三角路由问题。MN 向 CN 发送绑定更新报文,将自己当前所用的转交地址告诉 CN。CN 在自己的绑定缓存中记录 MN 的家乡地址和转交地址的绑定关系。CN 就可以直接向 MN 的转交地址发送报文,而不用经过 HA,从而避免了三角路由的问题。虽然移动 IPv6 路由优化为通信提供了更短的路径,减少了 MN 和 HA、家乡链路之间的拥塞情况,但它同时也增加了 MN 向 CN 发送 BU 的数量,未认证的或者恶意的 BU 报文引入了多种恶意攻击,增大了移动 IPv6 中存在的安全威胁[2]。

现有的解决移动 IPv6 路由优化安全问题的方法主要是返回可路由(Return Routability,RR)机制和 CGA(Cryptographically Generated Addresses)[3]生成家乡地址的方法。CAM-DH 协议(Child-proof Authentication for MIPv6-Diffie-Hellman)[4]是一种采用 CGA 生成家乡地址的路由优化安全方案,它比 RR 机制提供了更可靠的安全保护,但仍然存在一些安全上的漏洞,攻击者可以伪造转交地址与通信对端联系,从而发起数据重定向或泛洪攻击。本文在 CAM-DH 协议的基础上进行改进,提出了一种新的增强方案,提高了安全性,并对其计算负载和报文交换性能作了优化。

作者简介:黄志彬(1983-),硕士,主要研究方向:高速因特网与网络安全;洪佩琳(1961-),教授,博士生导师,主要研究方向:信息通信网和信息安全。
收稿日期:2008-01-17 **修回日期**:2008-04-18

2 移动 IPv6 路由优化安全

新协议的导入往往会引入新的安全问题，移动 IPv6 安全研究的基本目标是能够达到与 IPv4 协议一致的安全性[5]。移动 IPv6 中的大部分威胁是与发送给 MN 或者 CN 的绑定更新相关的,通过伪造绑定更新报文,攻击者可以将数据重定向到它自己或者其他节点上并阻止受害者继续接受数据。如果攻击者向通信双方发送伪造的绑定更新报文,伪装成对方,就能使自己成为 MN 和 CN 的中间人;如果攻击者向受害者发送大量的绑定更新报文,受害者要对这些绑定更新进行处理或者建立绑定缓存条目,从而会很快耗尽受害节点的 CPU 或者内存资源,形成了对受害节点的拒绝服务攻击。

本文使用的符号意义如表 1 所示。

表 1 符号意义说明表

符号	说明
MAC(k,m)	报文校验码,k 是一个对称密钥,m 是变长的报文
$m\|n$	串接符号,将 m 和 n 串接起来
Hash(m)	对消息 m 的哈希运算
First(m,n)	对 n 取前 m 位
P_X	节点 X 的公钥
S_X	节点 X 的私钥
P_X(message)	使用公钥 P_X 对 message 进行加密
S_X(message)	使用私钥 S_X 对 message 进行数字签名

2.1 RR 机制和 CGA 生成家乡地址方法

RFC3775 中采用 RR 机制保护路由优化安全,RR 机制通过探测移动节点是否能够通过家乡地址 HoA 和转交地址 CoA 接收到测试报文的方式来验证绑定更新的合法性。RR 机制具有很好的可用性,能够抵御反射攻击、DoS 攻击、重放攻击等等。如果没有对绑定更新报文进行认证,任意节点都能够伪造绑定更新报文对正在通信的两个节点进行会话劫持,RR 机制把攻击者的范围缩小到 MN 和 CN 之间的两条路径上。但是,RR 机制也存在着弱点,不能完全防范伪造地址的攻击:攻击者如果能够监听到某部分测试消息,就可以通过伪造家乡地址或者转交地址,接收另一部分测试消息,生成绑定更新密钥,构造一个合法的绑定更新报文发送给通信对端,这样,攻击者就能够伪装成其他身份与通信对端进行联系。

CGA 地址是一种在接口标志符部分包含一个哈希值的地址。使用 CGA 地址的网络节点首先产生一对公私钥对,然后生成关于公钥的哈希值，并以此值的后 64 位作为自己地址的接口标志符部分,从而生成一个和公钥绑定起来的地址。节点用私钥对将要发出的数据包进行数字签名,并将签名数据和公钥附在数据包后,接受到此数据包的节点首先验证数据包的源地址和发送者提供的公钥的绑定关系,然后利用公钥对数据包中的签名进行认证,只有这两次认证均通过后,才真正接受此数据包。

面临移动 IPv6 协议中家乡地址被盗用而导致的通信劫持等安全威胁，人们想到了使用 CGA 方法来产生移动节点的家乡地址。移动节点 MN 拥有一个 CGA 形式的家乡地址。MN 在发送给 HA 的 BU 报文中附上了使用私钥产生的对 BU 数据包的数字签名。HA 收到 BU 后，将采用公钥对数字签名进行认证,如果通过认证就回送一个 BA 报文,成功建立关于 MN 的绑定。CAM-DH[4]和 SUCV[6]都是基于 CGA 地址提出的路由优化安全协议。

使用 CGA 生成家乡地址，恶意节点可以通过侦听 MN 发出的 BU 报文而得到 MN 的家乡地址和公钥,可是无法得到私钥,从而无法生成正确的数字签名,恶意节点发出的假造的 BU 报文无法通过 HA 对其中的数字签名的认证而最终被抛弃。

2.2 CAM-DH 协议

CAM-DH 协议结合了 RR 机制和 CGA 生成家乡地址的特点,利用 CGA 生成家乡地址,并且 CN 分别向 MN 的家乡链路和直接路径发送消息,MN 只有同时收到这两个消息才可以生成绑定更新密钥。CAM-DH 采用 D-H 密钥交换协商绑定更新密钥,以牺牲了一部分性能为代价,比 RR 机制提供了更可靠的安全保护。

CAM-DH 的过程如图 1 所示，包含了 5 个消息。消息 1 中,MN 告诉 CN 自己的家乡地址 HoA 和新的转交地址 CoA。然后,CN 向 MN 的家乡地址发送消息 2:$\{r_h,j,g^i\}$，其中 r_h=MAC(K_{CN},$HoA|N_j|0$),这个消息将经过 HA 转发,从 MN 的家乡链路到达。同时,CN 直接向 MN 发送消息 4:$\{r_c,j\}$，其中 r_c=MAC(K_{CN},$CoA|N_j|1$)。MN 从两个路径接收到消息后,生成绑定更新密钥,向 CN 发送绑定更新报文(消息 5),其中包含绑定更新密钥生成的 MAC 值及 MN 的私钥生成的签名,CN 对绑定更新报文进行校验,验证这个报文的可靠性。

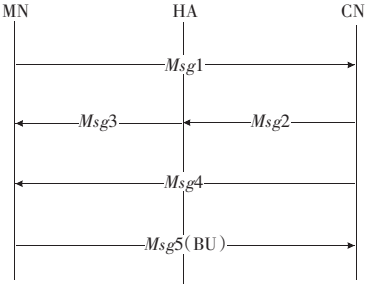

图 1 CAM-DH 报文交换过程

CAM-DH 中包含了一些优化措施,HA 可以拦截 CN 发送给 MN 家乡链路的消息，并代替 MN 进行一部分复杂的计算,再将计算结果通过 HA 和 MN 之间的安全隧道发送给 MN,MN 根据收到的消息生成绑定更新密钥。

但是,CAM-DH 协议也存在着一个问题:攻击者可以产生自己的公私钥对,构造一个合法的家乡地址,攻击者采用这个家乡地址与通信对端建立通信,然后,攻击者伪造一个绑定更新报文,将自己的转交地址伪装为受害者地址,通信对端会接受这个合法的绑定更新。于是,数据就会被重定向到受害者处,攻击者可以通过与多个通信对端发送数据,形成对受害者的泛洪攻击。

2.3 两次哈希的 CGA 地址

在 CAM-DH 协议中，采用的 CGA 方法是一次哈希完成的,这种方法存在漏洞,可能遭受暴力破解,即攻击者采用自己生成的公钥进行哈希计算,直到找到合适的参数使得生成的结果与 CGA 地址一致,这样,攻击者就可以伪装成该 CGA 地址。

RFC3972 中提出了一种新的 CGA 地址计算方法，地址生成过程如图 2 所示,其中采用了两个哈希值代替原来的一个哈希值。增加第二个哈希值 Hash2 的目的是增加 CGA 地址生成的复杂度,同时也增加了暴力破解 CGA 地址的难度。

两次哈希的 CGA 地址包含一个安全参数(Security Parameter,Sec)用于检验其抵御暴力破解的强度,安全参数为一个 3 bit

的无符号型整数,位于接口标志符的最左边 3 位。每个 CGA 地址与一个 CGA 参数(CGA Parameters,CGAP)相关联,CGA 参数中包含了公钥和 modifier、子网前缀、Collision Count、扩展域等其他参数,两个哈希值 Hash1 和 Hash2 都是由这个参数计算出来的,其他节点可以通过 CGA 地址和 CGA 参数来对地址进行验证。

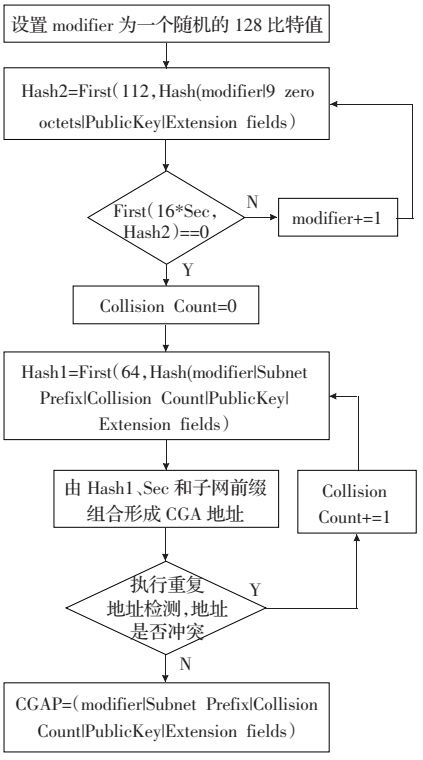

图 2　两次哈希的 CGA 地址生成过程

文献[7]中采用了两次哈希的 CGA 地址代替 CAM-DH 中的 CGA 地址,对 CAM-DH 协议进行改进,提高了 CAM-DH 协议抵御暴力破解的能力。

3　改进方案

通过以上对安全性的分析，可以看到,RR 机制和 CGA 生成家乡地址的方法仍然存在安全上的漏洞,不能完全解决移动 IPv6 路由优化中存在的安全问题。RR 机制和 CGA 生成家乡地址存在一个攻击者伪造地址的共同问题,前者可以伪造家乡地址或者转交地址,而后者只能伪造转交地址。本文在 CAM-DH 的基础上提出了一种改进方案，利用 CGA 生成家乡地址和转交地址，相当于在家乡地址和转交地址之间建立了绑定关系，并且用 HA 代替 MN 同 CN 进行 D-H 密钥交换,可以有效地保护移动 IPv6 路由优化中的安全。

3.1　改进方案流程

本方案包括 HA 和 MN 协商对称密钥 K_{ex}、CN 和 MN 协商绑定更新密钥 K_{BU} 两个阶段(如图 3 所示),下面作具体介绍。

首先,MN 需要采用 CGA 生成家乡地址 HoA 和转交地址 CoA。MN 自己生成公私钥对 P_{MN}/S_{MN},家乡地址 HoA 和转交地址 CoA 的主机标识部分都是通过公钥 P_{MN} 经过两次哈希获得。

MN 向 HA 发送消息 1:$\{HoA, CGAP_H\}$,HA 响应该消息,生成一个 K_{ex} 用于保护 HA 和 MN 之间消息的交换,HA 将 K_{ex} 用 MN 的公钥加密后,发送消息 2:$P_{MN}(K_{ex})$给 MN。MN 用自己的

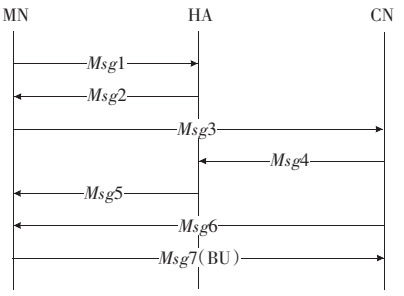

图 3　改进方案报文交换过程

私钥解密后,得到 K_{ex}。消息 1 和消息 2 构成了第一个阶段,HA 和 MN 通过 MN 的公钥交换了一个对称密钥 K_{ex} 用于保护第二阶段的消息。

消息 3~消息 7 是 MN 和 CN 之间协商绑定更新密钥,发起绑定更新的过程。

在消息 3 中,MN 直接向 CN 发送$\{HoA, CoA, CGAP_H, CGAP_C\}$,包含了 MN 的家乡地址和转交地址、CGA 参数。$CGAP_H$ 和 $CGAP_C$ 分别表示家乡地址 HoA 和转交地址 CoA 对应的 CGA 参数,CN 可以通过相应的 CGA 地址和 CGA 参数来对地址进行验证。

CN 接收到消息 3 后，利用 CGA 参数和 CGA 地址的子网标志符生成接口标志符,与 CGA 地址的接口标志符进行比较,从而实现对 CGA 地址的验证。这里,采用同一个公私钥对生成家乡地址和转交地址,因此 $CGAP_H$ 和 $CGAP_C$ 中的公钥应该是相同的,CN 也要对二者进行比较。

CN 对 MN 的家乡地址和转交地址都进行验证后，向 MN 的家乡地址发送消息 4:$\{r_h, j, g^x\}$,其中 r_h=MAC(K_{CN},HoA|N_j|0)。这个消息经过 HA 时会被 HA 拦截,经过处理后发送消息 5 给 MN:{CN,MAC(K_{ex},K_h),g^x,j},其中 K_h=Hash($g^{xy}|r_h$)。K_h 经过第一阶段交换的对称密钥的加密，避免被家乡链路的其他节点窃听。

CN 向 MN 家乡地址发送消息 4 的同时，向 MN 的转交地址发送消息 6:$\{r_c, j\}$,其中 r_c=MAC(K_{CN},$CoA|N_j$|1)。

MN 接收到 HA 发送的消息 5 和 CN 发送的消息 6 后,就可以根据收到的信息计算绑定更新密钥 K_{BU}=Hash($K_h|r_c$)。然后,MN 向 CN 发送绑定更新报文(消息 7):$\{T_0, HoA, CoA, i, MAC(K_{BU}, T_0|HoA|CoA|i), g^x, S_{MN}(TypeTag|g^x|HoA), CGAP_C, MAC(K_3, T_0|\cdots CGAP_C), j\}$,其中 K_3=Hash($r_h|r_c$)、K_{BU}=Hash($K_h|r_c$)。绑定更新报文中带有 K_{BU} 生成的一个内部 MAC 值、MN 的私钥所生成的签名以及 K_3 生成的外部 MAC 值。

CN 接收到绑定更新报文，首先计算 K_3 对外部 MAC 值进行校验,当校验符合后,才验证签名、计算 K_{BU} 并对内部 MAC 值进行校验。这样,CN 就能够防范发送大量伪造 BU 报文的 DoS 攻击，只有整个报文通过校验,CN 上才会建立绑定缓存,保存状态信息。

3.2　安全性能分析

本文提出的改进方案比 RR 机制和 CGA 生成家乡地址的方法提供了更高的安全保护,接下去的部分对本方案进行安全性上的分析。

3.2.1　伪造地址

一方面,通过 CGA 生成家乡地址和转交地址,相当于在家乡地址 HoA、转交地址 CoA 和公钥 P_{MN} 之间建立了一个绑定关系;另一方面,CN 向 MN 的家乡地址和转交地址两条路径发送

报文,验证了转交地址的存在,从而解决了 RR 机制和用 CGA 生成家乡地址方法中伪造地址的安全问题。攻击者采用自己的公私钥对生成家乡地址,伪造自己的转交地址为想要攻击的主机地址,这个伪造的消息 3 在 CN 端无法通过第一轮校验,CN 可以轻易将这个报文丢弃,避免了进行较复杂的密钥运算。

3.2.2 DoS 攻击

在本方案中,CN 端会收到两个报文消息 3 和消息 7。收到消息 3 后,CN 要先对 MN 的家乡地址和转交地址进行验证后才进行 D-H 值的计算。收到消息 7 后,CN 要先计算 K_3 进行报文的校验,然后才进行绑定更新密钥的计算。只有对通过简单验证的报文,CN 才会进行较复杂的运算,能够在很大程度上防范耗尽 CPU 资源的 DoS 攻击。CN 在接收绑定更新报文、生成绑定更新密钥之前,不会保存状态信息,因此,也能够防范耗尽内存资源的 DoS 攻击。

3.2.3 两次哈希的 CGA 方法

本方案中结合了文献[7]中的部分思想,采用 RFC3972 中的两次哈希的 CGA 地址生成方法,可以通过调整 CGA 参数中的 Sec 值,增加地址生成的复杂度,同时也增加了暴力破解的难度。CAM-DH 中暴力破解的算法复杂度是 $O(2^{62})$,文献[7]中暴力破解的算法复杂度为 $O(2^{59+12*Sec})$,本方案采用了基于 RFC3972 的两次哈希的 CGA 地址生成方法,暴力破解需要的运算复杂度增加为 $O(2^{59+16*Sec})$。

3.3 性能分析

3.3.1 计算开销分析

大部分情况下,移动节点受到功率、能量等的限制,性能并不高。在 CAM-DH 协议中,MN 上需要进行 D-H 密钥交换的计算以及使用私钥签名绑定更新报文两个较复杂的操作。本方案将 D-H 密钥计算放到 HA 上,与 CAM-DH 协议相比,节省了 D-H 值的计算以及 D-H 密钥生成的开销。

在 CAM-DH 中,HA 也可以代替 MN 进行 D-H 密钥的计算,但是 HA 计算的密钥需要通过建立安全隧道发送给 MN。采用 IPSec 建立安全隧道需要较大的通信开销和处理工作量,部署起来也相对复杂。本方案中,HA 和 MN 之间预先通过公私钥交换了一个对称密钥,HA 采用这个对称密钥 K_{ex} 对产生的密钥进行加密,再发送给 MN,MN 通过解密获得这个密钥。这种方法利用了 CGA 地址的公私钥对,而不需要 MN 和 HA 之间的安全隧道,节省了 MN 和 HA 之间建立 IPSec 安全隧道的开销,便于部署。当 CN 也是一个移动节点时,CN 可以将这些计算也放到自己的 HA 上,减小 CN 上的计算开销。

3.3.2 报文交换的优化

消息 1~消息 7 发送绑定更新报文是本方案的完整过程。MN 选择一个家乡代理后,可以用消息 1 和消息 2 协商一个对称密钥。消息 3 到消息 7 是 MN 与一个新的 CN 交换绑定更新密钥的过程。在 MN 较频繁的发生切换的情况下,MN 切换到新的子网下,采用 CGA 方法配置新的转交地址后,MN 和 CN 间只需要交换消息 3、6、7 即可,减少了报文交换的延时。

在不同的应用下,g^x 和 g^y 可以重复使用,通过改变 r_c 和 j 的值来改变采用的密钥。这样,不需要频繁的计算 g^x 和 g^y,节省了节点上的运算开销。在对切换速度要求比较高的场合下,为了保持同原有通信对端的联系,MN 上保存 K_h 值不变,CN 直接向 MN 发送消息 6,带上新的 r_c 和 j,MN 计算新的 $K_{BU}=\mathrm{Hash}(K_h|rc)$,向 CN 发送新的绑定更新报文,可以有效地提高切换的效率。

4 结束语

移动 IPv6 为主机在 IPv6 网络下提供了移动性支持,其中,移动 IPv6 路由优化是移动 IPv6 的重要特性,移动 IPv6 路由优化提高了系统通信的效率,但它同时也给整个系统引入了新的安全问题。本文先介绍了目前主要的两种解决方法:RR 机制和采用 CGA 生成家乡地址的方法,并对它们进行了简单的分析。由于这两种方法仍然存在一定的缺陷,在一种 CGA 生成家乡地址方法——CAM-DH 协议的基础上进行了改进,提出了新的增强方案,提高了路由优化过程的安全性,同时减少了 MN 上的计算开销,对报文的交换过程进行了优化。

参考文献:

[1] Johson D,Perkins C.RFC 3775 Mobility support in IPv6[S].IETF,2004.

[2] Ren K,Lou W,Zeng K,et al.Routing optimization security in mobile IPv6[J].Computer Networks,2006.

[3] Aura T.RFC 3972 Cryptographically Generated Address (CGA)[S].IETF,2005.

[4] Roe M,Aura T,O'Shea G,et al.Authentication of mobile IPv6 binding updates and acknowledgments[S].IETF,2002.

[5] Elgoarany K,Eltoweissy M.Security in mobile IPv6:a survey,Information Security[S].2007.

[6] Montenegro G,Castelluccia C.SUCV Identifiers and addresses[S].IETF,2002.

[7] Lee Y H,You I S,Rhee S S.Improving CAM-DH protocol for mobile nodes with constraint computational power[C]//Proc of the 8th International Conference on Knowledge-based Intelligent Information,2004.

(上接 100 页)

[6] Tuck N,Sherwood T,Calder B,et al.Deterministic memory-efficient string matching algorithms for intrusion detection[C]//Proceedings of the IEEE Infocom Conference,Hong Kong,China,March 2004.

[7] Tan L,Sherwood T.A high throughput string matching architecture for intrusion detection and prevention[C]//Proceedings 32nd Annual International Symposium on Computer Architecture(LISA),2005.

[8] 廖明涛,张德运,李金库.基于网络处理器的高效中英文多模式匹配算法[J].计算机工程,2007,33(5):38-40.