第 34 卷 第 6 期 计 算 机 工 程 2008 年 3 月
Vol.34 No.6 Computer Engineering March 2008
·安全技术· 文章编号：1000—3428(2008)06—0167—03 文献标识码：A 中图分类号：TP393.08

基于 CGA 技术的移动 IPv6 绑定更新安全机制

曹 昉，杜学绘，钱雁斌
（解放军信息工程大学电子技术学院，郑州 450004）

摘 要：为解决移动 IPv6 路由优化过程当中绑定更新消息的安全问题，结合返回路径可达协议和 CAM 协议的优点，提出一种基于加密生成地址(CGA)技术的绑定更新安全机制。该机制在没有部署 PKI 的环境下，利用 CGA 技术实现了跨信任域的 2 个节点基于地址的身份认证，可有效防止攻击者伪造、篡改绑定更新消息，解决路由优化过程中存在的反射式攻击问题。

关键词：路由优化；绑定更新；移动 IPv6；返回路径可达；加密生成地址

Security Mechanism of Mobile IPv6 Binding Update Based on CGA

CAO Fang, DU Xue-hui, QIAN Yan-bin
（Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004）

【Abstract】 In order to solve the security issues of the binding update message in the IPv6 route optimization process, this paper presents a new security mechanism based on Cryptographically Generated Addresses(CGA) through the analysis of the Return Routability Procedure (RRP) and CAM protocols. Security analysis proves that the mechanism can authenticate the nodes based on IPv6 address without PKI infrastructure, and prevent the forged binding update messages and the reflecting attack.

【Key words】 route optimization; binding update; mobile IPv6; Return Routability Procedure(RRP); Cryptographically Generated Addresses(CGA)

移动IPv6 协议在通信对端和移动节点之间的通信过程中采用了路由优化策略[1]。该策略的基本思想是移动节点通过发送绑定更新消息的方法，向通信对端声明其家乡地址与外地转交地址之间的映射关系。当通信对端向移动节点发送数据时，则根据该映射关系将数据直接发往移动节点的外地转交地址。路由优化策略解决了移动IPv4 中的“三角路由问题”，有效提高了数据传输的效率，减少了家乡链路和家乡代理的负载。但是，如果不对路由优化策略提供必要的安全措施予以保护，将会为IPv6 网络体系带来巨大的安全隐患。根据文献[2]针对路由优化策略的攻击主要源于对绑定更新消息的篡改和伪造。因此，在没有完善的PKI环境下，如何对通信对端和移动节点之间的绑定更新消息进行认证和加密，成为一个亟待解决的问题。

1 已有的绑定更新安全机制

1.1 RRP 协议

返回路径可达(Return Routability Procedure, RRP)[1]采用协商绑定更新管理密钥的方法，保护绑定更新消息的安全。根据文献[1]，该协议采用 3 个安全措施：(1)协议中的消息禁止使用家乡地址扩展域，配合地址过滤的方法防止攻击者对消息进行伪造；(2)通信对端将授权信息分为两部分，通过不同路径发送给移动节点，实现了对移动节点的可达性探测；(3)通信对端只在接收到绑定更新消息后，才计算绑定更新管理密钥，对消息摘要进行验证，并且不储存移动节点的任何信息，以防止拒绝访问式攻击。但是该协议只限制了攻击者发起攻击的时间和位置，不能对绑定更新消息进行有效认证，同时也没有实现消息的安全传输，无法完全解决路由优化的安全问题。

1.2 CAM 协议

CAM(Child-proof Authentication for MIPv6)[3]使用地址绑定公钥的方法计算出移动节点的家乡地址，即

家乡地址=单播地址前缀+网络前缀+用户标识

其中，用户标识为移动节点拥有公钥的散列值。该协议通过散列计算建立了地址与公钥的绑定关系，实现了通信对端对绑定更新消息签名的验证，防止了攻击者发送伪造的绑定更新消息。但其中仍然存在安全隐患，表现在 2 个方面：

(1)以公钥和调整参数作为输入的散列计算过于简单，易于找出其碰撞值，进而伪造出违法的地址与公钥的绑定关系；

(2)无法确认移动节点的真实位置，攻击者可以通过合法的移动节点身份对网络中任意节点发起反射式攻击[2]。

2 基于 CGA 技术的绑定更新安全机制

由文献[2]可以得出，路由优化主要的安全威胁来自于伪造、篡改、重放绑定更新消息以及针对通信对端的拒绝服务式攻击。本文方案采用 SEND 协议(Secure Neighbor Discovery Protocol)中的加密生成地址(Cryptographically Generated Addresses, CGA)技术实现通信对端和移动节点跨信任域的认证，并使用验证后的公钥对授权信息进行加密，防止攻击者对消息进行伪造和篡改。在此基础上通过使用可达性测试的思想对移动节点的实际位置进行探测，确定移动节点在其声称的位置上，有效解决了反射式攻击。同时采用即时生成绑定更新管理密钥的方法，防止攻击者发起拒绝访问式攻击。

2.1 绑定更新安全机制的认证体系

本文提出的绑定更新安全机制依靠CGA技术建立公钥与地址的绑定关系，来验证移动节点提供的公钥是否有效，并使用该公钥验证消息签名，实现通信对端对移动节点基于地

作者简介：曹 昉(1980－)，男，硕士研究生，主研方向：网络安全；杜学绘、钱雁斌，博士研究生

收稿日期：2007-05-20 **E-mail：**caofang66@sina.com

址的跨信任域认证。绑定关系的建立需要一个重要的数据结构——CGA数据结构(CGA Parameters data structure)，如 图 1 所示[4]。其中，修正值字段为 128 b随机数，用于提高CGA类型地址生成的安全性；子网前缀字段为 64 b；冲撞值字段为 8 b的无符号整型数，可能为 0, 1 或 2，其值随CGA类型地址生成时，DAD(Duplicate Address Detection)协议探测到的地址冲突次数的增加而增加；公钥字段为地址拥有者使用的公钥，长度可变；扩展域字段为可选项，长度可变。

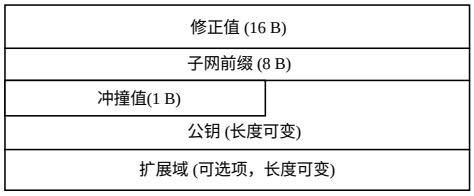

图 1　CGA 数据结构

移动节点根据该 CGA 数据结构计算出其家乡地址，当移动节点移动到新的链路上后，根据同样的方法得到外地转交地址。CGA 地址生成步骤如图 2 所示。

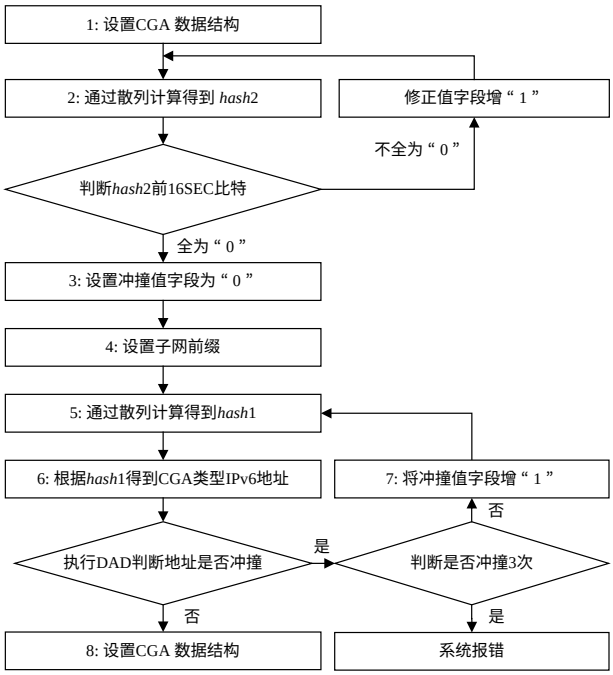

图 2　CGA 类型地址生成步骤

移动节点设置 CGA 数据结构各字段值，其中，修正值字段为 128 b 的随机数；子网前缀字段和冲撞值字段设置为 0；公钥字段设置为移动节点拥有的公钥；扩展域字段不使用。将生成的 CGA 数据结构作为输入值进行 SHA-1 散列计算，取结果的前 112 b 为 *hash*2，并判断 *hash*2 前 16SEC 位是否全部为 0，“否”则对修正值字段增 1 并返回第 2 步，“是”则将 CGA 数据结构的冲撞值设置为 0。将子网前缀字段设置为所在子网的网络前缀，然后进行 SHA-1 散列计算，取结果的前 64 b 作为 *hash*1，并按照格式得到用户标识(用 SEC 覆盖 *hash*1 前 3b，并将 u, g 两位，即第 6 位、第 7 位置 1)。连接子网前缀和用户标识得到 128 b 的 IPv6 地址，同时执行 DAD，如果发现地址冲突，则对冲撞值字段增 1，并返回到第 5 步，连续冲突 3 次则报错并退出。如果未发现地址冲突，则按照 CGA 数据结构的格式顺序写入最终的修正值、子网前缀、冲撞值、公钥、扩展域。

当通信对端收到消息后，根据消息中的 CGA 数据结构验证消息中源地址与其公钥的绑定关系，验证步骤如图 3 所示。

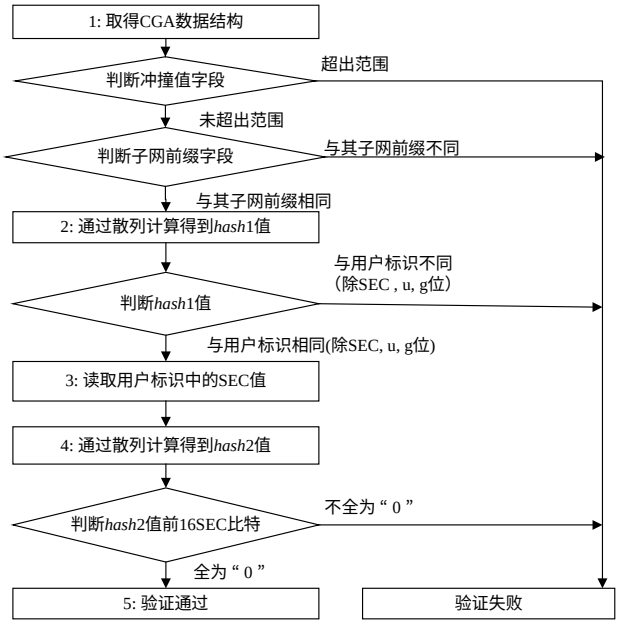

图 3　CGA 类型地址验证过程

取得 CGA 数据结构，判断其冲撞值字段是否为 0, 1 或 2。如果超出这个范围，则验证失败并退出，如果没有超出则继续判断子网前缀字段中的值是否与移动节点所在子网的网络前缀相同，不同则验证失败，相同则将该 CGA 数据结构作为输入进行 SHA-1 散列计算，取结果的前 64 b 为 *hash*1。判断该 *hash*1 与消息源地址的用户标识部分(除 SEC 与 u 位、g 位)是否完全相同，如果不同则验证失败，相同则将 CGA 数据结构的子网前缀字段和冲撞值字段置 0，并作为输入进行 SHA-1 散列计算，取结果的前 112 b 为 *hash*2。取出消息源地址中的 SEC 值(用户标识部分的前 3 b)，判断 *hash*2 前 16SEC 位是否全为 0，“是”则验证成功，“否”则验证失败。

2.2　绑定更新安全机制的消息传递

本文提出的绑定更新安全机制分为 3 个过程：绑定更新的发起，绑定更新的授权以及绑定更新消息的传递。消息传递过程如图 4 所示，其中，MN 为移动节点；HA 为该移动节点的家乡代理；CN 为通信对端。

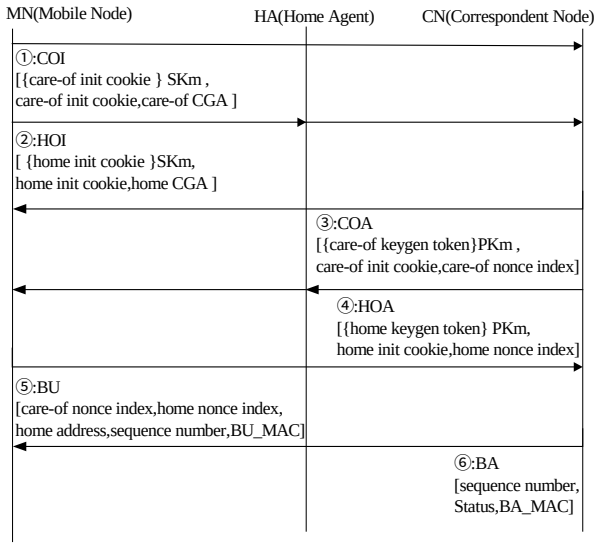

图 4　绑定更新安全机制消息传递过程

过程描述如下：

(1)绑定更新的发起

MN 通过消息①、消息②向 CN 发起绑定更新,消息①直接发送给 CN，消息②通过隧道由 HA 转发给 CN。其中，care-of init cookie 与 home init cookie 为随机数，用于匹配 CN 发送回来的授权消息；care-of CGA 与 home CGA 用于公钥和地址绑定关系的验证。CN 接收到消息后，进行 CGA 类型地址验证，通过后使用 CGA 数据结构中 Public key 字段的公钥 PKm 对 home init cookie 及 care-of init cookie 进行验签，如果签名正确则进行绑定更新的授权。

(2)绑定更新的授权

CN 通过消息③、消息④对 MN 进行授权，消息③直接发送给 MN，消息④由 HA 转发给 MN。其中，

care-of keygen token=First(64, HMAC_SHA1(Kcn, (care-of address| nonce|1)))

home keygen token=First(64, HMA_SHA1 (Kcn, (home address|nonce|0)))

其中，Kcn 为 CN 私有的密钥；nonce 为 CN 每间隔一段时间产生的随机数，使用 nonce index 进行标识，每个 nonce 有一定的有效时间。MN 接收到消息③和消息④后，使用其自身的私钥 SKm 对消息中的加密消息进行解密，得到 home keygen token 和 care-of keygen token，计算绑定更新管理密钥：

Kbm=SHA1(home keygen token|care-of keygen token)

(3)绑定更新消息的传递

绑定更新消息的传递过程中，MN 向 CN 发送带有地址映射关系的消息⑤，CN 向 MN 应答消息⑥。其中，

BU_MAC=First(96, HMAC_SHA1(Kbm, (care-of nonce index|home nonce index| care-of address|home address |correspondent node addres|sequence number)))

BA_MAC=First(96, HMAC_SHA1(Kbm, (care-of address| correspondent node address | status | sequence number)))

其中，sequence number 为 16 b，作为消息⑤、消息⑥的匹配标识，另外也用于防重放攻击。CN 接收到消息⑤后，根据 home nonce index, care-of nonce index 指示的 nonce 及 Kcn，重新生成 care-of keygen token 与 home keygen token，从而得到 Kbm 验证 BU_MAC。如果验证成功 CN，则建立绑定更新条目，并返回消息⑥给 MN，完成整个绑定更新过程。如果通信对端再次接收到该绑定更新消息，则判断新收到消息的 sequence number 是否大于已接收消息的 sequence number，大于则根据新的绑定更新消息覆盖原有的绑定，小于等于则抛弃新收到的绑定更新消息。

3 安全性分析与比较

本安全机制使用 CGA 技术生成移动节点的家乡地址和外地转交地址。攻击者要伪造绑定更新消息的源地址，就必须在 COI 和 HOI 消息中伪造该地址合法拥有者的 CGA 数据结构，并使用与该数据结构中公钥字段相应的私钥对发起消息中的 cookie 进行签名。而该私钥为合法地址拥有者所私有，攻击者难以获取，因此，无法伪造 COI 和 HOI 消息中的源地址。通信对端验证通过 COI 和 HOI 中 CGA 类型的源地址后，对消息中的签名信息进行验签，如果验签成功，说明该公钥的拥有者为源地址的拥有者，实现了对移动节点基于地址的身份认证。通信对端使用该公钥对密钥生成令牌 home keygen token 与 care-of keygen token 进行加密传输。攻击者截获该消息后，难以取得相应的私钥，无法计算出 Kbm，从而防止了攻击者对绑定更新消息的篡改和伪造。

移动节点发起绑定更新时，需要使用其家乡地址和外地转交地址分别发送 COI 和 HOI 消息给通信对端，对移动节点进行可达性测试。攻击者如果利用自身的家乡地址绑定一个攻击对象的地址，将数据包重定向到攻击对象所在的位置，就需要以攻击对象的身份伪造 COI 消息。由于外地转交地址也采用 CGA 技术，攻击者无法伪造消息中的源地址，因此通信对端收到 COI 和 HOI 消息，就能够确认移动节点一定移动到其声称的位置，防止了反射式攻击。

与 RRP 相比，本安全机制采用了 CGA 技术防止攻击者对消息源地址的伪造，并使用公钥对密钥生成令牌进行加密传输。而 RRP 协议采用地址过滤机制来防止攻击者对消息源地址的伪造，由于实际的网络拓扑结构灵活复杂，该安全机制没有基于密码学的 CGA 技术有效。另外，RRP 协议采用了明文方式传输通信对端的授权信息，易于被攻击者利用并发起攻击。

与CAM协议相比，本安全机制提供了可达性测试，能防止了反射式攻击。在CAM协议中，通信对端无法根据绑定更新请求消息判断出请求者的实际位置，易受反射式攻击。CAM与本安全机制都使用了基于密码学的地址认证机制，但是CGA技术能够根据SEC的指示进行多轮的散列计算，相比CAM协议，攻击者进行强力攻击的算法复杂度从$O(2^{64})$增加到$O(2^{59+12SEC})$，具有更高的安全性。本安全机制采用nonce和sequence number相结合的方法防止对绑定更新消息的重放攻击。如果绑定更新消息中nonce index指示的nonce超过其有效时间，说明该绑定更新消息已经失效，通信对端抛弃该消息。如果消息中的nonce index指示的nonce没有超过其有效时间，但移动节点又发生了移动，则通信对端通过判断sequence number的值确定消息的有效性，这比CAM使用时间戳的方法更为有效、灵活。

4 结束语

本文通过分析 RRP 和 CAM 协议，提出了一种基于 CGA 技术的绑定更新安全机制，能够实现节点间跨信任域的身份认证。在此基础上完成消息的加密，解决了路由优化过程中绑定更新消息的安全传输问题，同时通过可达性测试的方法，防止了反射式攻击。但是，本安全机制对移动节点计算能力要求过高，需要进一步的深入研究。

参考文献

[1] Johnson D, Perkins C. Mobility Support in IPv6[S]. IETF RFC 3775, 2004-06.

[2] Nikander P, Aura T, Montenegro G. Mobile IP Version 6 Route Optimization Security Design Background[S]. IETF RFC 4225, 2005-12.

[3] O'Shea G, Roe M. Child-proof Authentication for MIPv6 (CAM)[J]. ACM SIGCOMM Computer Communications Review, 2001, 31(2): 4-8.

[4] Aura T. Cryptographically Generated Addresses(CGA)[S]. IETF RFC 3972, 2005-03.