一种基于代理移动 IPv6 绑定更新的安全策略①

陈华山, 王 熠, 刘宪成

(河海大学 常州校区信息中心, 常州 213022)

摘 要: 随着移动 IPv6 技术的不断发展, 对网络的安全性提出了更高的要求. 针对代理移动 IPv6 绑定更新过程当中的安全问题, 结合返回路径可达过程协议和不对称加密技术, 改进了返回路径可达过程协议, 提出一种基于自动密钥认证的返回路由可达过程绑定更新安全机制. 分析了方案的安全性, 该方案能有效防止攻击者伪造、篡改绑定更新消息, 杜绝移动主机受到拒绝服务攻击等问题, 提高了通信主机绑定更新过程的安全性.

关键词: 代理移动 IPv6; 绑定更新; 返回路由可达; 安全性

Security Strategy Based on the Binding and Update of the Proxy Mobile IPv6

CHEN Hua-Shan, WANG Y, LIU Xian-Cheng

(Information Center of Changzhou Campus, Hohai University, Changzhou 213022, China)

Abstract: With the unceasing development of the mobile IPv6 technology, the users have put forward higher requirements for the security of the network. According to the proxy mobile IPv6 binding update process safety issues, this paper improves the return path process, basing on the Return Routability Procedure and the Asymmetric cryptographic technique. It proposes one kind of security mechanism based on the automatic key authentication. The paper analyses the security of the scheme, which can effectively prevent attackers from forging, tampering the messages, denying the mobile host being attacked by a series of problems, such as the denial of service.

Key words: Proxy Mobile IPv6 (PMIPv6); binding update; Return Routability Procedure (RRP); security

移动IPv6的设计原则是通过构建移动节点的身份标识和位置标识之间的映射关系来实现移动性管理. 移动 Ipv6 延时过长, 无法满足实时业务的需求, 从而出现了快速切换 FMIPv6、层次移动 MIPv6 等一些改进方案. MIPv6, FMIPv6 提供了较为完整的移动性解决方案[1]. 但它们也有不足, 这主要是这些方案要求移动节点参与到信令交互过程中, 对手机、PDA 等终端设备提出了更高的要求. 为此, IETF NETLMM 工作组颁布了一种基于网络的移动性管理协议代理移动 Ipv6. 现在, PMIPv6 成为新一代宽带无线网络建设中实现区域移动管理的技术方案, 已经被无线通信技术标准所采用.

1 代理移动IPv6简介

代理移动IPv6(PMIPv6)是一种解决IPv6移动性需求的方法. 它通过扩展移动 IPv6 协议中移动节点和家乡代理之间的信令消息来支持 IPv6 节点的移动性, 不需要主机的参与. 这种支持移动性的方法并不需要移动节点参与家乡代理的信令消息交互. 网络中的代理移动实体执行与家乡代理之间的信令交互, 代替网络上的移动节点进行移动管理.

PMIPv6 在 MIPv6 的基础上, 引入了本地移动定位点(LMA, Local Mobility Anchor) 和移动访问网关(MAG, Mobile Access Gateway) 的概念[2]. LMA 作为 MN(移动主机)归属网络前缀的拓扑定位点, 负责管理 MN 的绑定与可达性状态. MAG 作为与 MN 实际相连的访问路由器(AR, Access Router) , 负责检测 MN 的到达和离开, 并代替 MN 向 LMA 交换与移动相关的信令消息. 所有的 LMA 与 MAG 都通过有线链路相连, 每个 MAG 都会连接若干个访问点(AP, Access Point), MN

① 基金项目:中央高校基本科研业务费专项资金(2010B23914)

收稿时间:2013-05-24;收到修改稿时间:2013-07-12

以无线方式与 AP 相连从而接入 MAG. 当移动节点进入 PMIPv6 域并连接到某条访问链路时, 该链路上的 MAG 会对 MN 的身份进行验证, 提供基于网络的移动性管理服务.

2 代理移动IPv6绑定更新的过程

当 MN 在 LMA 域(LMD) 内的不同区间移动时, 通过 MAG 与 LMA 来完成区域绑定更新. 当 MN 在不同 LMD 域间移动时, 采用全局移动性管理协议进行家乡绑定更新[3]. PMIPv6 绑定更新的主要流程如图 1 所示.

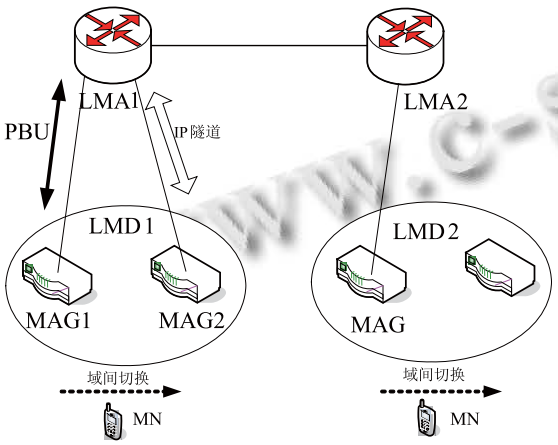

图 1　PMIPv6 绑定更新流程图

(1) 当 MN 进入 PMIPv6 的 LMD1 时, 收到来自 MAG1 包含 LMA 前缀信息的路由通告消息, MN 利用该前缀信息建立代理家乡地址, 并向 MAG 进行连接.

(2) 连接成功后, MAG1 代替 MN 向 LMA1 发送代理绑定更新消息(PBU).

(3) LMA1 对 PBU 进行应答, 若通过检验, LMA 就会为 MN 分配不少于 1 个的归属网络前缀, 并建立一个绑定缓存条目, 同时 LMA 与 MAG 共同建立一条双向隧道用来传输 MN 与通信节点之间的数据分组. 此时 MN 就可以使用分配的 HNP 创建归属地址, MN 在整个域中移动而不需要信令传输. 在 MN 看来整个域就像是一条单独的链路, 对发往或发自 MN 的数据进行转发.

(4) 当 MN 改变了它的接入点后, MAG1 会立刻检测出 MN 断开了与它的连接, 并触发计时器. 超过时间后, LMA 将处理结果通过代理绑定确认报文(PBA)发送给 MAG1, 后者收到后立即拆除先前与 LMA 建立的隧道.

3 代理移动IPv6绑定更新存在的安全问题

在代理移动 IPv6 中, 大多数的潜在威胁都是关于错误绑定的, 这会导致拒绝服务攻击. 还有一些威胁可能会引起截获和冒充攻击. 主要存在的威胁是发送到 MAG 和通信对端的绑定更新的威胁. 如果 MAG 接受这样的欺骗信息, 移动节点可能收不到发送给它数据流, 恶意节点冒充受害节点.

恶意节点在发送的绑定更新中将转交地址设置成受害节点的地址. 如果这种绑定更新被接受了, 恶意节点可以引诱通信对端向受害节点发送大量的数据. 通信对端对恶意节点报文的响应, 将会被发送到受害主机或网络, 这可以引起分布式的拒绝服务攻击. 使用流控制协议也不能防止这种类型的攻击, 因为攻击者可以伪造确认信息. 即使对 TCP 的初始序列号保密也没有用, 因为攻击者可以在自己的地址接收最初的几个片段, 再将数据流重定向给受害者的地址[4].

目前的研究中, 绑定更新主要是 MN 通过 HA 转发 IKEv2 协商消息, 与 CN 建立 IKE SA 和共享密钥, 通过 IPSec 保护 MN 和 CN 间的绑定更新消息. 该方法的绑定更新过程是安全的, 但在 HA 转发 MN 和 CN 消息的过程中增加了绑定更新时延, 容易造成 HA 的拒绝服务. 还有研究是基于身份的数字签名, 该方法解决了 MN 与 CN 之间的身份认证和 BU 的完整性认证问题. 减少了信令传送, 从整体上减小了绑定时延, 提高了网络性能且可对抗假冒和密钥截获等攻击.

综上所述, 代理移动 IPv6 绑定更新过程中可能遭受的攻击主要包括拒绝服务攻击、来自 MN 到 MAG 和通信对端的绑定更新的威胁, 还有就是数据流重定向问题.

4 代理移动IPv6绑定更新的安全策略

对于基于网络的移动管理协议潜在的安全威胁, 特别是代理移动 IPv6 绑定更新存在的安全问题. 目前研究出一些代理移动 IPv6 抵御这些来自绑定更新威胁的安全策略.

4.1 MN 到 MAG 之间绑定更新的安全策略

通过保护移动节点和 LMA 之间移动报文, IPSec ESP 对 BU 和 BA 的完整性提供保护. 使用动态密钥, IPSec 就可以提供抗重播保护. IPSec 不保证数据包的正确顺序, 只保证它们没有被重播, 因为这样, 移动 IPv6 使用了序列号来保证正确的顺序. 使用动态密钥,

IPSec 抗重播保护和移动 IPv6 序列号可以防止这样的攻击. 然而, 因为移动节点和 LMA 之间有安全协议, LMA 总是可以识别有问题的移动节点. 使用一对手动密钥的安全策略, 会与移动节点的新家乡地址的产生或采用新的家乡子网前缀发生冲突, 这是因为 IPSec 安全策略受限于使用的地址[5]. 采用基于证书的自动密钥在一定程度上缓和了这个问题, 还需要保证给定的移动节点不会代替其他的移动节点发送 BU.

4.2 MN 到通信对端绑定更新的安全策略

在代理移动 IPv6 中采用返回路由可达过程(RRP), 可以保护 MN 到通信对端的绑定更新. 在 MN 向通信对端(CN)发出绑定更新(BU)之前, MN 与 CN 需要交换 4 个控制信息,在成功交换了这些信息后,MN 才会向 CN 发出 BU, CN 也会对 MN 发过来的 BU 进行处理. 直到认证的 BU 到达, 通信对端保留关于移动节点的状态. 通过使用由 nonce 和节点密钥构造的密钥标识完成的, 密钥标识可以由通信对端重新构造[6].

返回路径可达过程的主要优势是限制了潜在攻击者对特定路径的接入, 并避免其他位置所发送的伪造的绑定更新, 但是 RRP 在安全特性上还是有一定缺陷. 返回路径可达过程存在中间人攻击的威胁, 如果恶意节点截获 MN 发送过来的消息, 然后用虚假的转交地址伪造新的消息发送给 CN 来进行绑定更新, 由于 CN 没有相应的认证机制, 因此恶意节点可以得到基于虚假转交地址的应答.

5 一种新的代理移动IPv6绑定更新安全方案

代理移动 IPv6 是在移动 IPv6 的基础上提出的, 它引入了 LMA 和 MAG 两个实体, 在一定程度上减轻了移动节点的开销. 在移动节点在不同域中移动时, 并不需要移动节点参与信令交换, 它是通过 LMA 和 MAG 这两个实体来完成, 这也增加了 LMA 和 MAG 这两个实体的工作压力. 但是综合考虑, 随着硬件设备的性能不断提升, 用增加硬件负担来换取网络的安全性, 并且为移动 IPv6 的 QoS(服务质量)提供了安全保证. 代理移动 IPv6 更高的安全性和不需要移动节点参与到网络当中, 是推动移动 IPv6 发展的保证, 也是代理移动 IPv6 的优势所在.

在上述代理移动 IPv6 绑定更新的安全策略分析中, 不管是 MN 到 MAG 之间还是 MN 到通信对端之间都存在一些安全隐患. 通过返回路由可达过程可以保护到通信对端的数据安全, 但是对于冒充移动主机和通信对端进行绑定更新, 返回路由可达过程无法判断移动主机的身份[7]. 对于这种情况, 在返回路由可达过程中引入基于自动密钥认证方法可以保证绑定更新的安全性. 改进的传统返回路由可达过程, 称之为基于自动密钥认证的返回路由可达过程, 它在代理移动 IPv6 的整个绑定更新过程中起到安全保障作用.

基于自动密钥认证的返回路由可达的工作过程是在代理移动 IPv6 会话开始之前, 生成一对新的密钥, 在会话结束后, 密钥取消. 在移动节点通信过程中, 这一对密钥由参与通信的设备使用, 其它第三方不能获取. 它的主要步骤是生成一对临时的公/私钥, 再生成一个 EID=Hash(公开部分), 发起方发送绑定更新和用其私钥签名的 EID 给响应方, 响应方逐一做出回应[8]. 文中提到的安全方案改进, 主要是返回路由可达过程步骤的改进, 基于自动密钥认证的返回路由可达过程的步骤如图 2 所示.

图 2 PMIPv6 的返回路由可达过程流程图

改进了的返回路由可达过程, 增强了移动节点和通信对端的信息安全性. 移动主机向 MAG 发起连接报文, MAG 就会触发到 AAA 服务器, AAA 服务器对移动节点进行认证, 这个步骤是移动节点能进行通讯的初始化条件. 在返回路由可达过程中发送的是本地初

始化测试请求报文, 改进了的返回路由可达过程中间增加本地初始化测试报文的请求和应答. LMA 回复本地初始化测试应答报文, 内容包括特定的认证信息, 建立安全机制, 这样就保证了移动节点在 LMD 域中的安全性.

基于自动密钥认证的 PMIPv6 绑定更新的具体步骤是: MN 直接向 CN 发起绑定更新请求消息, 消息通过隧道由 LMA 转发给 CN. 其中生成 cookie 随机数, 用于匹配 CN 发送回来的授权消息. 生成一对临时的公/私钥, CN 验证公钥和地址绑定关系. CN 接收到消息后, 进行密码验证, 通过后使用数据结构中 Public key 字段的公钥 PKm 对 cookie 进行验签, 如果签名正确则进行绑定更新的授权. 绑定更新的授权 CN 通过响应消息对 MN 进行授权. 其中, Kcn 为 CN 私有的密钥, CN 每间隔一段时间产生 nonce 随机数, 使用 nonce index 进行标识, 每个 nonce 有一定的生命周期. MN 接收到消息后, 使用其自身的私钥 SKm 对消息中的加密消息进行解密, 计算出绑定更新的管理密钥. 在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, CN 向 MN 返回应答消息. CN 接收到消息后, 根据 nonce 和 Kcn, 得到绑定更新管理密钥 Kbm[9]. 如果验证成功, 则建立绑定更新条目, 并返回消息给 MN, 整个绑定更新过程完成. 如果通信对端再次接收到该绑定更新消息, 判断新收到消息的序列号(sequence number)是否大于已接收消息的序列号, 大于就将新的绑定更新消息覆盖原有的绑定, 小于或者等于则丢弃新收到的消息.

6 安全性分析

对返回路由可达过程进行了两个方面的改进, 增加了移动节点的本地初始化测试请求和本地初始化测试应答, 在绑定更新过程中引入了动密钥认证机制, 增强了移动节点绑定更新的安全性. 绑定更新消息的发送经过家乡密钥生成令牌和转交密钥生成令牌加密, 所以绑定更新消息的安全性是可以得到保证. 有效的防范了来自网络的攻击, 保证了协议的安全性. 与其他安全策略相比, 没有增加其他的安全隐患.

移动节点在进行会话前, 先进行 AAA 服务器认证, 然后通信对端使用公钥对密钥生成令牌进行加密传输. 攻击者截获该消息后, 没有相应的私钥, 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. 与传统的 RRP 相比, 改进了的 RRP 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.

该安全策略采用 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 超过其有效时间, 说明已经失效, 通信对端丢弃该消息. 如果通信对端再次接收到该绑定更新消息, 判断新收到消息的序列号是否大于已接收消息的序列号, 大于则绑定, 小于或者等于则丢弃, 该方法比用时间戳的方法更加有效. MN 和 HA 之间存在 SA, 通信过程中 IPSec 提供安全性, 所以在 MN 的私钥生成过程中, MN 和 HA 之间的相互认证与私钥的传输是安全可靠的. 私钥生成过程是在 MN 离开家乡链路后, 向 HA 注册转交地址, 有效避免了密钥被截获. 绑定更新过程中 MN 的身份认证和 BU 的完整性认证依赖于 HA 为 MN 生成的公钥/私钥对. MN 用自己的私钥对 BU 进行签名, CN 用 MN 的公钥进行验证, 保证了 BU 的完整性和合法性, 同时也对 MN 的身份进行了有效认证, 可以杜绝基于主机绑定更新的拒绝服务攻击.

确保绑定更新身份及地址的合法性, 改进了的安全策略有效地防止消息源的伪造, 通过收到消息的序列号确定信息源的可靠性. 协议认证性的分析通过 ProVerif 对网络模型进行查询来完成, 认证包括 CN 对消息信令、MN 身份、转交地址的认证以及 MN 对 CN 身份和地址的认证, 试验输出结果显示正确. 在新的绑定更新机制的认证性过程中, 试验结果表明该绑定更新机制满足认证性, 保证了 MN 在移动网络中绑定更新的安全性.

7 总结和展望

代理移动 IPv6 绑定更新认证过程中使用建立安全联系的 IPSec 来保护代理绑定更新消息与代理绑定确认消息, 这从根本上消除了与假冒移动接入网关或本地移动锚相关的威胁.

通过改进 RRP, 提出了一种基于自动密钥认证的返回路由可达过程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, 并且能完成消息的加密, 解决了绑定更新消息的安全传输问题, 有效控制了拒绝服务攻击. 在研究代理移动 IPv6 的绑定更新安全认证过程中, 它不需要移动节点参与信令交换, 但是也

(下转到 192 页)

取传感器数据, 发送到控制中心 AP, AP 通过串口发送数据给 GPRS 模块把数据上传到岩溶地质所网站上, 实现实时远程监控的功能.

参考文献

1 张颖,李俊甫,杨臻.基于 SimpliciTI 协议的无线自组织网络系统设计.自动化仪表,2012.

2 SimpliciTI Sample Modular RF Network Specification. 2007-2011.

3 SimpliciTI Application Programming Interface Version 1.2. 2009.

4 王军强.基于 SimpliciTI 的无线传感器网络关键技术研究[学位论文].重庆:重庆大学,2009.

5 万时光,马小铁,李凯.星型无线传感器网络的应用研究.通信技术,2009.

6 宋继勐.无线小型自组织网络协议分析与实现[学位论文].北京:北京交通大学,2009.

7 季国鹏.基于 SimpliciTI 协议的无线网络温度采集系统的设计与实现[学位论文].合肥:安徽大学,2012.

8 STM32F103x8,STM32F103xB 数据手册.2009

9 ADF7021_N,2008

10 杨立林.SimpliciTI 网络协议的无线数据采集系统设计.单片机与嵌入式系统应用,2010.

11 朱葑葑.CSMA/CA 协议在传感器网络中的应用与改进[学位论文].成都:电子科技大学,2007.

12 王果. M2M 通信随机接入算法研究[学位论文].北京:清华大学,2011.

13 方飞,毛玉明.时隙 ALOHA 稳定性控制算法研究.计算机应用研究,2013.

(上接第 178 页)

对 LMA 和 MAG 这两个实体提出了更高的计算能力. 如何更加合理的在安全和性能方面做出平衡, 还需要进一步的深入研究.

参考文献

1 Johnson D, Perkins C, Arkko J. IETF RFC3775. Mobility Support in IPv6. June 2004.

2 Gundavelli S, Leung K, Devarapalli V, et al. IETF RFC 5213. Proxy Mobile IPv6. 2008.

3 周华春,张宏科,秦雅娟.一种代理移动 IPv6 认证协议.电子学报,2008,(10):1873−1880.

4 游红.移动 IPv6 中绑定更新认证协议设计及分析[学位论文].重庆:重庆大学,2006.

5 Yi MK, Choi JW, Yang YK. A comparative analysis on the signaling load of proxy mobile IPv6 and hierarchical mobile IPv6. ISWPC 2009. New Jersey: IEEE Press, 2009.1−5.

6 张一芳,张奇支.基于快速切换的代理移动 IPv6 路由优化方案.计算机应用,2012,32(2):335−339.

7 胡建中.移动 IPv6 中绑定更新注册的研究[学位论文].南京:南京理工大学,2008.

8 张仕斌,万武南,张金全.应用密码学.西安:西安电子科技大学出版社,2009.

9 曹昉,杜学绘,钱雁斌.基于 CGA 技术的移动 IPv6 绑定更新安全机制.计算机工程,2008,34(6):167−169.