第 37 卷 第 1 期
Vol.37 No.1

计 算 机 工 程
Computer Engineering

2011 年 1 月
January 2011

• 安全技术 •

文章编号：1000—3428(2011)01—0151—03 文献标识码：A 中图分类号：TP393.08

MIPv6 绑定更新机制及验证

韩明奎，潘 进，陈志广，李 波

(西安通信学院通信装备管理系，西安 710106)

摘 要： MIPv6 的绑定更新过程是其主要安全问题，IETF 草案对此给出一种新的基于 IKEv2/IPSec 协议的绑定更新机制，但是 IKEv2 协议存在不适合直接应用于移动环境的缺陷。为此，基于 Weil 对数字签名算法改进了 IKEv2 协议的缺陷，并在新协议的基础上改进了绑定更新过程。基于应用π演算验证了改进绑定更新机制的认证性。

关键词： 移动 IPv6；绑定更新；IKEv2 协议

Mobile IPv6 Binding Update Mechanism and Verification

HAN Ming-kui, PAN Jin, CHEN Zhi-guang, LI Bo

(Department of Communicating Equipment Management, Xi'an Communications Institute, Xi'an 710106, China)

【Abstract】 Mobile IPv6(MIPv6) binding update is primary security question, IETF draft proposes a new binding update mechanism based on IKEv2/IPSec protocol. However, IKEv2 protocol is unsuitable for MIPv6 directly because of flaws. This paper improves IKEv2 protocol based on Weil pairing's signature arithmetic, as well as the mechanism. The improved mechanism is verified in applied π calculus.

【Key words】 Mobile IPv6(MIPv6); binding update; IKEv2 protocol

DOI: 10.3969/j.issn.1000-3428.2011.01.052

1 概述

移动 IPv6 协议由移动节点 *MN*、对端节点 *CN* 和家乡代理 *HA* 3 个实体组成。当 *MN* 进入外地链路时，能够保持家乡地址 *HoA* 不变，并通过临时获得的转交地址 *CoA* 通信。*MN* 获得转交地址后，需要向 *HA*、*CN* 发送绑定更新消息通告 *CoA*，建立 *CoA* 和 *HoA* 的映射关系。绑定更新解决了移动 IPv4 中的“三角路由”问题，有利于降低网络负载、提高数据传输速率。但是绑定更新过程容易遭到攻击，是移动 IPv6 的主要安全问题。

2 研究现状及不足

目前，保护移动 IPv6 绑定更新的安全机制主要有返回路由可达过程、CGA 协议、CBU 协议等[1]。这些方法采用不同的技术体制保护了绑定更新过程，但未考虑难度较大的 *MN-CN* 通信安全。文献[2]在 IETF 草案中首次提出使用 IPSec 保护 *MN-CN* 绑定更新和业务通信。该草案基于 *MN* 的家乡地址建立 IPSec SA，通过 IKEv2 认证抵御中间人攻击、拒绝服务攻击，提高了移动 IPv6 的安全性。文献[3]在草案的基础上，基于 IKEv2/MOBIKE 实现了绑定更新与 IKEv2 协商过程的融合。但 2 种方案都存在不足，文献[2]解决了安全问题，然而未考虑绑定更新效率等；文献[3]解决了文献[2]的问题，但针对航空的特殊情况进行了较多扩展。本文在文献[2-3]的基础上，改进了 IKEv2 协议和绑定更新机制。

3 新的绑定更新机制

文献[2]提出的绑定更新机制令 *MN* 通过 *HA* 转发 IKEv2 协商消息，与 *CN* 建立基于 *HoA* 的 IKE SA 和共享密钥，然后使用 IPSec 保护 *MN-CN* 间的绑定更新消息信令。该方法是安全的，但 *HA* 转发 *MN-CN* 消息的过程增加了绑定更新时延和自身负担，容易造成 *HA* 的拒绝服务。

3.1 Weil 对的数字签名算法

基于身份认证的公钥密码体制最早由 Shamir A 提出，文献[4]提出的基于超椭圆曲线的 Weil 对技术是第 1 个公认有效的方案。该密码体制选用任意比特串生成公钥，实际使用中该比特串通常是用户的身份，因此，也称为基于身份的密码学。

设 G_1、G_2 分别是 q 阶的加法循环群和乘法循环群，其中，q 是大素数，且在 G_1、G_2 中离散对数问题都是难解的。$\hat{e}$ 是 $G_1 \times G_1 \to G_2$ 的双线性映射，满足双线性、非退化性和可计算性。

私钥生成中心(Private Key Generator, PKG)作为可信第三方，负责系统参数初始化、认证用户身份、生成和分发用户私钥等。基于 Weil 对的数字签名算法如下：

(1)建立系统参数

随机选择 $s \in Z_q^*$，计算 $P_{\text{pub}} = sP$，其中，$v = e(U + H_1(m,U)Q_{ID})$ 为 G_1 的生成元；定义 2 个 Hash 函数 $H_1 : \{0,1\}^* \to Z_q^*$ 和 $H_2 : \{0,1\}^* \to G_1$。其中，H_1 是将任意长度的输入映射到固定长度；H_2 是将用户身份信息映射成 G_1 中的一个元素。PKG 将 s 作为系统私钥保存，公开系统参数 $params = < G_1, G_2, \hat{e}, P, P_{\text{pub}}, H_1, H_2 >$。

(2)生成用户密钥

给定身份 $ID \in \{0,1\}^*$，可以计算公钥 $Q_{ID} = H_2(ID)$ 和私钥 $S_{ID}=sQ_{ID}$。

(3)签名

给定待签名的消息 m，取随机数 $r \in Z_q^*$，计算签名 $\delta = (U,V)$，其中，$U = rQ_{ID}$；$h = H_1(m,U)$；$V = (r+h)S_{ID}$。

基金项目： 国家“863”计划基金资助项目(2007AA01Z472)

作者简介： 韩明奎(1985－)，男，硕士研究生，主研方向：网络安全，形式化分析，移动 IPv6；潘 进，教授、博士生导师；陈志广、李 波，硕士研究生

收稿日期： 2010-04-22 **E-mail：** hmkwtt@126.com

(4)验证签名

计算 $Q_{ID}=H_2(ID)$， $u=e(V,P)$， $v=e(U+H_1(m,U)Q_{ID},P_{\text{pub}})$，如果 $u=v$，则通过认证，否则拒绝认证。

3.2 基于改进后 IKEv2 协议的绑定更新机制

在新的绑定更新机制中，*HA* 不再转发数据，只担任 PKG 角色。*MN* 对应于 IKEv2 协议[5]的发起方 *I*，其生成公钥的身份信息由转交地址和身份标识符组成 $ID_{MN}=CoA\,|\,ID_i$，则公钥 $Q_{ID\_MN}=H_2(ID_{MN})$，私钥 $S_{ID\_MN}=sQ_{ID\_MN}$；*CN* 对应于 IKEv2 协议的响应方 *R*，生成公钥的身份信息包括当前地址和身份标识符 $ID_{CN}=IP_{CN}\,|\,ID_i$，则公钥 $Q_{ID\_CN}=H_2(ID_{CN})$，私钥 $S_{ID\_CN}=sQ_{ID\_CN}$。

基于改进后 IKEv2 协议的绑定更新机制如图 1 所示，共有 8 条消息。

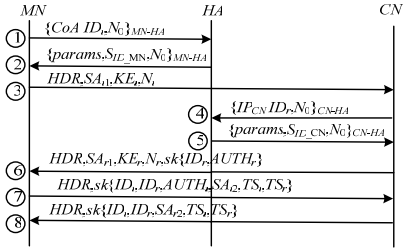

图 1 基于改进后 IKEv2 协议的绑定更新机制

其中，消息③、消息⑥~消息⑧是基于 Weil 对数字签名算法改进的 IKEv2 初始交互协议。

(1) $MN\rightarrow HA:\{CoA\,|\,ID_i,N_0\}_{MN\_HA}$

MN 在新的链路得到 *CoA* 后，向担负 PKG 任务的 *HA* 发送私钥生成请求消息。消息①、消息②中的 $\{\cdots\}_{MN\_HA}$ 和消息④、消息⑤中的 $\{\cdots\}_{CN\_HA}$ 表示内容通过安全的方式发送。

(2) $HA\rightarrow MN:\{params,S_{ID\_MN},N_0\}_{MN\_HA}$

HA 响应 *MN* 的请求，将生成的私钥和系统参数、随机值发送给 *MN*。

(3) $MN\rightarrow CN:HDR,SA_{i1},KE_i,N_i$

MN 向 *CN* 发送 *SA* 提议、Diffie-Hellman(D-H)交换值和随机值 N_i，提出绑定更新请求。消息源地址是 *CoA*，家乡地址选项是 *HoA*。

(4) $CN\rightarrow HA:\{IP_{CN}\,|\,ID_r,N_0\}_{CN\_HA}$

CN 收到消息后，从消息源地址、家乡地址选项提取 *CoA*、*HoA*，建立 IP 地址的缓存列表，同时向 *MN* 的家乡代理 *HA* 请求私钥和系统参数。

(5) $HA\rightarrow CN:\{params,S_{ID\_CN},N_0\}_{CN\_HA}$

HA 响应 *CN* 的请求，将生成的私钥和系统参数、随机值发送给 *MN*。

(6) $CN\rightarrow MN:HDR,SA_{r1},KE_r,N_r,sk\{ID_r,AUTH_r\}$

CN 选择 *SA* 提议并生成自己的 D-H 交换值 KE_r 和随机值 N_r，然后计算共享密钥、认证载荷和加密载荷。

认证载荷使用基于 Weil 对的签名算法生成，不再需要传递数字证书来验证身份，也就不需要部署 PKI。协议首先让响应方证明自己的身份，实现了对发起方身份的主动保护。

MN 根据收到的参数计算相关密钥，解密消息得到 *CN* 的身份载荷 ID_r；然后按照签名算法计算出 *CN* 的公钥 Q_{ID_CN} 对认证载荷进行验证。验证通过则生成消息(7)；否则，协商中止。

(7) $MN\rightarrow CN:HDR,sk\{ID_i,ID_r,AUTH_i,SA_{i2},TS_i,TS_r\}$

MN 计算并发送自己的认证载荷和 CHILD *SA*，发送的内容还包括双方的身份标识、认证载荷及流量选择符。

CN 对收到的认证载荷进行验证。若通过验证，则将 *CoA* 和 *HoA* 写入绑定缓存列表完成绑定更新；否则协商中止。

(8) $MN\rightarrow CN:HDR,sk\{ID_i,ID_r,SA_{r2},TS_i,TS_r\}$

CN 选择一个 CHILD *SA* 提议响应 *MN* 的认证消息，完成初始交互。完成初始交换后，*MN*-*CN* 建立了基于 *MN* 家乡地址和 *CN* 当前地址的 IPSec *SA*。

3.3 性能分析

SA 是 IPSec 的关键，它规定了相关的加密、认证等安全操作。基于 IKEv2 协议的绑定更新机制实现了对家乡地址、转交地址和身份的认证，同时协商出了共享密钥和基于 *HoA* 的 *SA*。*HoA* 的唯一性确保了 *SA* 在切换的情况下仍然有效，因此，可通过 IPSec 保护 *MN*-*CN* 绑定更新过程和业务通信。

本文的绑定更新机制在保留文献[2-3]主要做法的同时，改进了 IKEv2 协议和绑定更新流程。改进后的 IKEv2 协议不需要传递证书和部署 PKI，降低了系统开销；新的流程把绑定更新与 IKEv2 协商相结合，降低了认证内容的冗余性。

4 绑定更新机制的安全性分析

4.1 应用π演算与 ProVerif

应用π演算[6]是进程代数中的一种。它定义了完备的交互、并发理论框架，能够建模、描述并推导协议的安全属性。该演算适合分析并发、分布式协议，以其简洁高效的特点得到广泛应用。形式化建模绑定更新过程用到的函数主要包括：*fun S*/2（签名函数）；*reduce V*(*S*(*sk*(*k*),*v*),*pk*(*k*),*v*)=*true*(检验签名)；*fun E*/2(共享密钥加密)；*reduce D*(*k*,*E*(*k*,*v*))=*v*(共享密钥解密)；*fun H*/2(带密钥值的哈希函数)；*fun H1*/2(哈希函数 1)；*fun H*2/2(哈希函数 2)。

ProVerif 是一个验证应用π演算模型的自动化工具，可以降低分析过程的难度及手工推导失误，提高分析速度和准确性。Blanchet 等人于 2002 年提出了基于 Horn 逻辑的安全协议分析理论，并基于该理论开发出 ProVerif。本文在分析移动 IPv6 绑定更新机制安全性的过程中，首先形式化定义了协议的应用π演算模型和安全性质，然后采用 ProVerif 来完成验证，分析过程采用的是 ProVerif 最新版本 v 1.14p14。

4.2 绑定更新机制的应用π演算模型

应用π演算把协议的参与主体描述为进程，多个进程并发构成系统进程反映协议的运行情况。下面分别给出符合 ProVerif 输入格式的各个主体进程模型。

MN 的进程描述如下：

leMN=(newCoA; new N0;out(c1, (CoA, IDi, N0)); in(c1, (skMN, = N0)))|(in(init, (IDrp, sai1, sai2)); new di;let KEi=exp(g,di)in new Ni; out(c, cons1(N, sai1, KEi, Ni, IPha)); event MNinitB(IP); in(c, cons2 (=N, sar1, KEr, Nr, er, hr)); let K_{MN} in if H(Kar, (R, er))=hr then let(IDr, sa, IPcn)=D(Ker,er)in letIDr'=H(Kpr, IDr)in if V(sr, H1 (IPcn,IDr), (N, sar1, KEr, Nr, Ni, IDr'))=true then let IDi'=H(Kpi, IDi) in let si= S(skMN, (N, sai1, KEi, Ni, Nr, IDi'))in let ei=E(Kei, (IDi, IDr, sai2, si, CoA, TSi, TSr))in let hi=H(Kai, (tI, ei))in out(c, cons3(N, ei, hi)); event MNverifedCN(IPcn); in(c, cons4(N, er2, hr2)); if H(Kar, (R, er2))=hr2 then let(=IDi, =IDr, sar2, TSi, TSr)=D(Ker, er2)in out(connect, (IDr, sai2, sar2, Kv)); event MNfinishedB(CoA)

CN 的进程描述如下：

let CN=(new IPcn; new N1; out(c2, (IPcn, IDr, N1)); in(c2, (sk CN, = N1)))|(in(c, cons1(N, sai1, KEi, Ni, =IPha)); new dr; let KEr=exp(g, dr)in new Nr; let K_{CN} in let IDr'=H(Kpr, IDr)in let sr=S(skCN, (N, sar1, KEr, Nr, Ni, IDr'))in let er=E(Ker, (IDr, sr, IPcn))in let hr=H (Kar, (R, er))in out(c, cons2(N, sar1, KEr, Nr, er, hr)); in(c, cons3(=N, ei, hi)); if H(Kai, (I, ei))=hi then let(IDi, =IDr, sai2, si, CoA, TSi, TSr)=D(Kei, ei)in let IDi'= H(Kpi, IDi)in if V(si, H1(CoA, IDi), (N, sai1, KEi, Ni, Nr, IDi'))=true then new sar2; event CNverifedMN(CoA, HoA, IPha); out(accept, (IDi, sai2, sar2, Kv)); let er2=E(Ker, (IDi, IDr, sar2, TSi, TSr))in let hr2=H(Kar, (constR, er2))in out(c, cons4(N, er2, hr2)));

系统进程 process 由 *MN* 和 *CN* 进程并发组成，同时包括了 PKG 进程，PKG 进程负责生成用户名及公钥、私钥。

process

!new IDi; !new IDr; (new s; in(x, (x1, k, N)); let pk_i= H1(x1, x)in let pk(k)=pk_k in let sk_i=H2(s, pk_i) in let sk(k)=sk_i in out(x, (sk_i,N)))|!(new init;new connect; new accept; MN|CN)

其中，发起方的密钥值为：

$$K_{MN}=\prod_{u=Kai,Kei,Kpi,Kar,Ker,Kpr,Kv}\{K_u=H\{KE_r\hat{}d_i\}(N_i,N_r,u)\}$$

响应方的密钥值为：

$$K_{CN}=\prod_{u=Kai,Kei,Kpi,Kar,Ker,Kpr,Kv}\{K_u=H\{KE_i\hat{}d_r\}(N_i,N_r,u)\}$$

通道 *init*、*connect*、*accept* 代表协议与主机交互的隐藏信道，环境无法与这些信道进行交互。通道 *c*1、*c*2 分别用来建模 PKG 与 *MN*、*CN* 传递信息的私有、安全信道。

4.3 安全性分析

绑定更新保护机制用于认证相关内容，确保所绑定转交地址的合法性，因此协议必须满足认证性。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。协议认证性的分析通过 ProVerif 对模型进行以下查询(query)来完成：

query ev: MNfinishedB(XCoA)==>(ev:CNverifedMN(XCoA, XHoA, XIPha)==>ev:MNverifedCN(XIPcn)&ev:MNinitB(XIP))

该查询可以用对应性断言解释：绑定更新完成之前，必然有 *MN* 通过了 *CN* 认证；而 *MN* 通过认证之前，*CN* 必定通过了 *MN* 的认证，并且 *MN* 发起了绑定更新请求。输出结果为 *true* 表示协议满足认证性。

5 结束语

移动 IPv6 的主要安全问题是绑定更新的认证，文献[2]提出了一种基于 IPSec 的绑定更新新机制。该机制存在 2 个问题：基于的 IKEv2 协议存在不足，绑定过程效率低且存在安全隐患。本文首先基于身份认证的数字签名算法改进了 IKEv2 协议，然后基于新的 IKEv2 协议优化了绑定更新过程，改进后的协议更加适合移动通信环境。最后形式化分析了新的绑定更新机制的认证性，结果表明该绑定更新机制满足认证性。

参考文献

[1] 侯雅毅, 钱焕延, 王晓喃. MIPv6 中基于身份的安全路由优化[J]. 计算机工程, 2009, 35(9): 127-129.

[2] Dupony F, Combes J M. Using IPSec Between Mobile and Correspondent IPv6 Nodes[EB/OL]. (2009-08-10). http://www.draft-ietf-mip6-cn-ipsec-08.txt.

[3] Bauer C, Ayaz S, Ebalard A. Solution Space for Aeronautical NEMO RO[EB/OL]. (2009-10-20). http://www.draft-bauer-mext-aero-solspace-00.txt.

[4] Boneh D, Franklin M. Identity Based Encryption from the Weil Pairings[C]//Proc. of Crypto'01. Berlin, Germany: [s. n.], 2001.

[5] Kaufman C. Internet Key Exchange(IKEv2) Protocol[S]. RFC 4306, 2005.

[6] Abadi M, Fournet C. Mobile Values, New Names and Secure Communication[C]//Proc. of the 28th ACM Symposium on Principles of Programming Languages. London, UK: [s. n.], 2001.

编辑 索书志

(上接第 150 页)

图 5、图 6 给出了 3 种方案组密钥更新过程的时延情况。其中，LKH 方案的时延最大，TGK 方案最小，而且随着被删除节点数的不断增加，TGK 方案的时延增加幅度是 3 种方案中最小的。

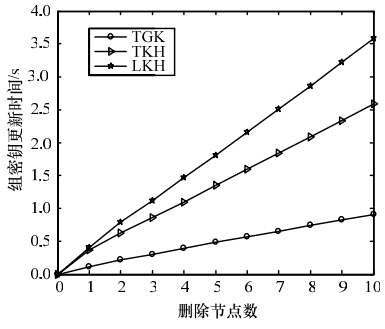

图 5 删除节点数与组密钥更新时延关系(*N*=512)

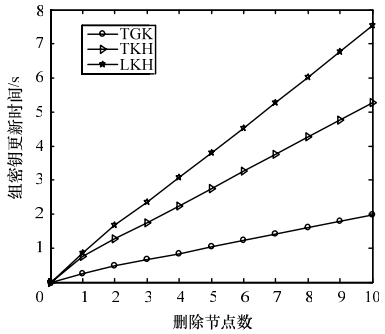

图 6 删除节点数与组密钥更新时延关系(*N*=1 024)

4 结束语

本文针对异构无线传感器网络的特点，提出一种基于拓扑信息的组密钥管理方案。该方案利用节点拓扑信息构建密钥管理树，在密钥管理树的生成与更新过程中对其进行结构优化，从而减少组密钥更新的能量消耗与更新时延。仿真实验表明在相同网络规模和删除节点的情况下，该方案具有较低的能量消耗和较小的更新时延，适合应用于异构无线传感器网络中。

参考文献

[1] 苏 忠, 林 闯. 无线传感器网络密钥管理的方案和协议[J]. 软件学报, 2007, 18(5): 1218-1231.

[2] Chandha A, Liu Yonghe, Das S K. Group Key Distribution via Local Collaboration in Wireless Sensor Networks[C]//Proc. of the 2nd Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks. [S. l.]: IEEE Press, 2006: 46-54.

[3] 李 辉. 基于密钥树的批量密钥更新方法[J]. 计算机工程, 2009, 35(23): 133-135.

[4] Jiang Yixin, Lin Chuang, Shi Minghui, et al. Self-healing Group Key Distribution with Time Limited Node Revocation for Wireless Sensor Networks[J]. Ad Hoc Networks, 2007, 5(1): 14-23.

[5] Wong C, Gouda M, Lam S. Secure Group Communications Using Key Graphs[J]. IEEE/ACM Transactions on Networking, 2000, 8(1): 16-30.

[6] Son Ju-Hyung, Lee Jun-Sik, Seo Seung-Woo. Topological Key Hierarchy for Energy-efficient Group Key Management in Wireless Sensor Networks[J]. Wireless Personal Communications, 2010, 52(2): 359-382.

编辑 顾逸斐