文章编号:1000-582X(2012)04-117-06

无双线性对的基于无证书的移动 IP 注册协议

张曼君[1,2],裴昌幸[1],党岚君[1]
(1.西安电子科技大学 综合业务网国家重点实验室,陕西 西安 710071;
2.西安邮电学院 通信工程系,陕西 西安 710121)

摘 要:目前大多数基于无证书的移动 IP 注册协议需要复杂的双线性对运算,这使得移动 IP 的注册过程开销较大,效率较低,不利于实时通信。基于无对运算的无证书签名方案,提出了高效安全的移动 IP 注册协议。由于在注册的过程中省去了复杂的对运算,所以减少了注册时间,提高了注册效率。此外,该协议通过在注册过程中用移动用户的临时身份代替真实身份实现了用户匿名性;通过使用临时随机数 Nonce 可以抵抗重放攻击。安全性分析的结果表明所提出的协议是高效的、安全的。此外,与同类协议进行的安全和性能比较结果证明在能提供同样高的安全性能级别的协议中,该协议所设计的 IP 注册过程的时延是最短的。

关键词:移动 IP;注册;无证书;双线性对;安全
中图分类号:TN 918.1 **文献标志码**:A

Mobile IP registration protocol in certificateless public key infrastructure without pairing

ZHANG Man-jun[1,2], *PEI Chang-xing*[1], *DANG Lan-jun*[1]
(1. The State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an 710071, Shaanxi, P. R. China; 2. Department of Communication Engineering, Xi'an University of Posts & Telecommunications, Xi'an 710121, Shaanxi, P. R. China)

Abstract: An efficient and secure mobile IP registration protocol is proposed, which is based on certificateless public key signature scheme without pairing to minimize the registration time. Vser anonymity is achieved via the temporary identity (TID) transmitted by the mobile user, instead of the true identity. Additional replay protection is included by introducing Nonce in the registration message to prevent a possible replay attack. Security analyses demonstrate that the new scheme is both secure and efficient. Numerical experimental results and security performance analyses show that the new scheme outperforms the existing ones regarding the registration time and computational load while improving security.

Key words: mobile IP; registration; certificateless; pairing; security

移动 IP 是移动通信的互联网标准,旨在支持移动用户从家乡网络向外地网络移动时数据的无缝传输。通过将无线技术与 IP 技术相融合,移动 IP 对于未来全 IP 移动通信系统中不同网络之间的全球

收稿日期:2011-09-12
基金项目:国家自然科学基金资助项目(60572147)
作者简介:张曼君(1980-),女,西安电子科技大学博士,主要从事无线通信及网络安全方向的研究,(Tel)13379037116;(E-mail)zhangmanjun@xupt.edu.cn。

移动提出了简单可行的解决方案。

在移动IP中每一个移动节点 MN 都由家乡网络中的家乡代理HA和家乡地址所确定。当移动节点离开家乡网络漫游到外地网络时，根据他所在的当前位置获得一个转交地址COA，同时他在家乡代理处注册这一转交地址。如果有数据包发往移动用户的家乡地址，家乡代理将其送往移动用户所在的外地网络的代理 FA，最终将该数据包送至移动用户的转交地址。

当移动用户漫游到外地网络时，他与其他用户之间的通信需要远程转交，而这一过程很容易受到敌手的攻击，所以注册对于通信安全的保障是非常重要的。最早的移动IP注册协议采用由RFC2002[1]提出的方案，即依赖手动分发对称密钥来完成移动实体之间的相互认证，这种方法注册时延短，但是不便于密钥管理，而且对于具有大量移动用户的环境，网路扩展性不好。为了解决这一问题，研究人员提出了基于传统的公钥证书加密的方案[2-4]。这种方法网络扩展性很好，但是移动用户端的资源有限，对于证书的操作需要很大的开销，这样会影响协议的性能，使得注册时延变长。为了克服这个缺点，文献[5-7]提出了把对称密码体制和基于证书的密码体制相结合，只在家乡代理和移动代理之间尽可能少地使用基于证书的公钥体制来改善移动IP的注册性能。为了进一步改善注册性能，减少证书的计算开销，文献[8-12]用基于身份的公钥密码体制引入移动IP注册，避免了证书带来的繁琐的管理问题。但是基于身份密码体制存在密钥的托管问题，所以对于移动IP注册引来了潜在的安全威胁。近年来人们提出了基于无证书的签名方案，它既没有证书管理的问题也不存在密钥托管的问题。将这种签名方案用于移动IP的注册，可以使注册过程得到更好的安全保障和更短的注册时延，克服了基于传统的公钥证书的算法和基于身份的算法中的无法避免的缺陷。其中Dang提出的无证书的移动IP注册方案[13]在现有的方案中具有很高的安全级别，同时经过证明又比同类安全级别的方案有更高的注册效率。但是在现有的基于无证书的注册方案中都需要用到耗时的双线性对运算，为了进一步减小运算量，缩短注册时延，提高注册效率，使方案更适合于实时通信，基于文献[14]中的无对运算的无证书签名算法提出了一个更加高效的移动IP注册协议，在现有的基于无证书的移动IP注册协议中本协议是第一个不涉及对运算的，因此所提出的协议是同类协议当中注册时延最短的，并且与Dang的协议一样具有很高的安全级别。

1 预备知识

1.1 信任模型

RFC2002[1]提出了移动IP注册的信任模型，其中家乡代理 HA 和外地代理 FA 为移动节点 MN 提供移动IP业务。家乡代理是移动节点可信的服务提供者，他们之间建立长期的安全关联。当移动节点漫游到外地网络时，外地网络中的某个外地代理将为移动节点提供服务，移动节点将得到一个转交地址，他在家乡代理处登记该转交地址，这样当他离开家乡网络时通信也不会中断。

1.2 无双线性对的无公钥证书签名方案

这一概念由J. Beak[13]首先提出。方案由7个算法组成：系统初始化(Set up)、部分私钥提取(Partial-Key-Extract)、秘密值生成(Set-Secret-Value)、私钥生成(Set-Private-Key)、公钥生成(Set-Public-Key))、签名(Signature)和验证(Verification)。

Set up：密钥生成中心KGC运行这一算法，产生系统参数params和主密钥 x。

KGC挑选2个素数 p 和 q 满足 $q \mid p-1$，选择随机数和一个的生成元 g，计算 $y=g^x$。定义2个哈希函数 H1：$\{0,1\}^* Z_p^* \rightarrow Z_q^*$，H2：$\{0,1\}^* \times \{0,1\}^* \times Z_p^* \rightarrow Z_q^*$。公布系统参数 params $=(p,q,g,y,$ H1, H2)。系统的主密钥为 x。

Partial-Key-Extract：KGC运行这一算法，输入params、主密钥 x 以及用户的身份 ID，输出 P_{ID}，D_{ID} 分别作为部分公钥和部分私钥。KGC随机选择，计算 $P=g^s$ 和 $t=s+xH_1(ID,P)$，得到 $(P_{ID}, D_{ID})=(P,t)$。

Set-Secret-Value：用户随机选择作为秘密值 $S_{ID}=r$。

Set-Private-Key：用户生成私钥 $SK_{ID}=(S_{ID}, D_{ID})=(r,t)$。

Set-Public-Key：用户根据 $P_{ID}=P$ 和 $S_{ID}=r$，计算 $F=g^r$，生成公钥 $PK_{ID}=(P,F)$。

Signature：用户输入明文消息 m，身份 ID，私钥 $SK_{ID}=(r,t)$，计算签名 $\sigma=tH_2(m,ID,P)+r$

Verify：输入系统参数params，签名者的身份，签名者的公钥 PK_{ID} 以及相对应的明文签名对 (m,σ)，计算 $h_1=H_1(ID,P)$，$h_2=H_2(m,ID,P)$，检查 $g^{\sigma}=F(Py^{h_1})^{h_2}$ 是否成立，如果等式成立，证明签名是正确的，否则拒绝此签名。

在此协议中Setup和Partial-Key-Extract运算是由KGC进行的，部分密钥是通过一个安全的信道由PGC交给用户的，而Set-Secret-value，Set-

Private-Key，Set-Public-Key 是由用户完成的，这样可以避免基于身份的方案中的密钥托管问题。

2　无对运算的基于无证书公钥的移动 IP 注册协议

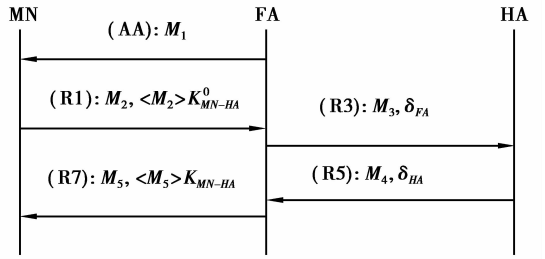
2.1　协议描述

1）MN 在家乡网络的登记

当一个移动节点 MN 加入到一个移动 IP 系统中时，HA 首先要证实 MN 的身份 ID_{MN}，如果身份是真实的，HA 选择一个与 MN 共享的初始密钥 K^0_{MN-HA}，产生一个初始随机数 N^0_{HA}，并且为 MN 计算临时身份标识符 TID$=H(ID_{MN}\|N^0_{HA})$用于下一次注册请求。这里，用来产生 TID 的哈希函数 H：$\{0,1\}^*\rightarrow\{0,1\}^*$。随后，$HA$ 通过安全信道把数据$(H(ID_{MN}\|N^0_{HA}),K^0_{MN-HA},N^0_{HA})$发送给 MN，同时在数据库中为 MN 保存初始记录$(ID_{MN},H(ID_{MN}\|N^0_{HA}),K^0_{MN-HA},N^0_{HA})$。$MN$ 也保存此记录。

2）MN 在外地网络向家乡代理进行的注册

当 MN 离开家乡网络时，需要通过外地代理向家乡代理进行注册，将新的转交地址和家乡地址进行绑定，从而保证漫游时通信不会中断。图 1 是所提出的新的移动 IP 注册协议的流程。



$M_1=$Advertisement，FA_{id}，MN_{CoA}，N_{FA}

$M_2=$ Request，Key-Request，FA_{id}，HA_{id}，MN_{CoA}，N^0_{HA}，N_{MN}，N_{FA}，$H(ID_{MN}\|N^0_{HA})$

$M_3=M_2$，$<M_2>K^0_{MN-HA}$，FA_{id}，F，$P_{FA}\delta_{FA}=Sig(S_{FA},M_3)$

$M_4=M_5$，$<M_5>K^0_{MN-HA}$，N_{FA}，$\{K_{MN-FA}\}K_{FA-HA}$，H，$P_{HA}\delta_{HA}=Sig(S_{HA},M_4)$

$M_5=$Reply，Result，Key-Reply，MN_{HM}，HA_{id}，N'_{HA}，N_{MN}

图 1　移动 IP 注册协议

a）代理广播（Agent Advertisement）：

（AA）$FA\rightarrow MN$：Advertisement，FA_{id}，MN_{CoA}，N_{FA}，

FA 向 MN 发送代理广播的标识符 Advertisement，FA 的身份标识 FA_{id}，MN 在外地网络的转交地址 MN_{CoA} 以及 FA 产生的随机数 N_{FA}

b）注册（Registration）：

（R1）$MN\rightarrow FA$：M_2，$<M_2>K^0_{MN-HA}$

这里 $M_2=$Request，Key-Request，FA_{id}，HA_{id}，MN_{CoA}，N^0_{HA}，N_{MN}，N_{FA}，$H(ID_{MN}\|N_{HA})$

其中 Request 表示注册请求的比特值，Key-Request 表示会话密钥请求的比特值，N_{MN} 是 MN 产生的临时随机数 MN 收到代理广播之后，如果发现自己的网络接入点发生变化，就构造一条注册请求消息，然后把它发送给 FA。这条注册请求消息包括定长部分（Request，Key-Request，HA_{id}，MN_{CoA}，N^0_{HA}，N_{MN}），非认证扩展部分（N_{FA}，FA_{id}，$H(ID_{MN}\|N^0_{HA})$），以及用 HA 与 MN 共享的初始密钥 K^0_{MN-HA} 计算 $<M_2>K^0_{MN-HA}$ 作为 M_2 的消息认证码 MAC，将其作为移动－家乡认证扩展部分。

（R2）FA 收到 MN 发送的注册请求消息后首先检查 M_2 中的 N_{FA} 与自己刚广播的 N_{FA} 是否相同。如果相同，根据介绍的签名方案，FA 随机选择 $r_{FA}\in Z^*_q$，计算 $F=g^{r_{FA}}$，用私钥 $SK_{FA}=(r_{FA},t_{FA})$ 对 $(M_3=M_2,<M_2>K^0_{MN-HA},FA_{id},F,P_{FA})$ 签名 $\delta_{FA}=\mathrm{Sig}(SK_{FA},M_3)=t_{FA}H_2(M_3,ID_{FA},P_{FA})+r_{FA}$，其中 FA 的公钥 $PK_{FA}=(F,P_{FA})$；如果不相同，FA 忽略这个注册请求消息，并返回 1 个带有否认码的注册回复消息给 MN。

（R3）$FA\rightarrow HA$：M_3，δ_{FA}。

FA 把 $(FA_{id},F\ P_{FA})$ 作为非认证扩展，把 δ_{FA} 作为外地－家乡认证扩展，附加在注册请求消息 M_2，$<M_2>K^0_{MN-HA}$ 的后面，并把这个新的注册消息发送给 HA。

（R4）当 HA 收到由 FA 转发过来的注册请求消息时，首先检查 M_3 中的 FA_{id} 与 M_2 中的 FA_{id} 是否相同。如果相同，根据介绍的签名方案中的 Verify，HA 计算 $h_1=H_1(ID_{FA},P_{FA})h_2=H_2(M_3,ID_{FA},P_{FA})$，通过验证 $g^{\delta_{FA}}=F(P_{FA}y^{h_1})^{h_2}$ 是否成立来完成他对 FA 的认证。HA 根据收到消息中的临时身份标识符 TID$=H(ID_{MN}\|N^0_{HA})$在他的动态参数数据库中搜索属于 MN 的记录，并且用该记录去检查收到消息的有效性；如果收到的消息 R3 中的 N^0_{HA} 是有效的，再用记录中的 MN 与 HA 之间的共享密钥 K^0_{MN-HA} 去验证 $<M_2>K^0_{MN-HA}$。如果验证时计算出的消息认证码 $<M_2>K^0_{MN-HA}$ 与接收到的相同，则 HA 认证 MN 成功。如果 HA 对 FA 和 MN 的认证都通过，则 HA 接受 MN 的注册请求。随后，HA 随机选择 $r_{HA}\in Z^*_q$，并计算 $H=g^{r_{HA}}$ 和 HA 与 FA 之间的会话密钥 $K_{FA-HA}=r_{HA}F$，动态分配家乡地址给 MN，并且绑定家乡地址和接收到的转交地址。接着，HA 更新注册参数如下：

a）随机产生一个新的 HA 的 nonce，N'_{HA}，然后计算 MN 下一次注册请求时需要的临时身份标识

符 $TID'=H(ID_{MN}\|N'_{HA})$。

b)计算 MN 与 HA 之间新的共享密钥 K'_{MN-HA} 和 MN 与 FA 之间的共享密钥 K_{MN-FA}。[14-15]

$K'_{MN-HA}=\mathrm{HMAC-SHA-1}(K^0_{MN-HA},N'_{HA}\|N_{MN}\|HA_{id})$ $K_{MN-FA}=\mathrm{HMAC-SHA-1}(K^0_{MN-HA},N^0_{HA}\|N_{MN}\|FA_{id})$。

c)HA 更新保存关于 MN 的新记录$(ID_{MN},H(ID_{MN}\|N'_{HA}),K'_{MN-HA},N'_{HA})$,用于 MN 的下一次注册。

(R5)$HA\rightarrow FA:M_4,\delta_{HA}$。

$M_4=M_5,<M_5>K^0_{MN-HA},N_{FA},\{K_{MN-FA}\}K_{FA-HA},H,P_{HA}$ $M_5=$Reply,Result,Key-Reply,$MN_{HM},HA_{id},N'_{HA},N_{MN}$ 其中 Reply 表示注册回复的比特值,Result 表示注册请求结果的数值,Key-Reply 表示会话密钥回复的比特值。MN_{HM} 表示移动节点 MN 的家乡地址。HA_{id} 表示家乡代理的身份标识。随后,HA 计算回复消息的定长部分 M_5 在密钥 K^0_{MN-HA} 下的 MAC 值$<M_5>K^0_{MN-HA}$,并且根据介绍的的无证书签名方案用他的私钥 $SK_{HA}=(r_{HA},t_{HA})$ 对消息 M_4 进行签名 $\delta_{HA}=\mathrm{Sig}(SK_{HA},M_4)=t_{HA}H_2(M_4,ID_{HA},P_{HA})+r_{HA}$ 并在随后丢弃 r_{HA}。HA 把$<M_5>K^0_{MN-HA}$作为移动一家乡认证扩展、$(N_{FA},\{K_{MN-FA}\}K_{FA-HA},H,P_{HA})$作为非认证扩展,$\delta_{HA}$ 作为外地一家乡认证扩展依次附加在回复消息的定长部分 M_5 的后面,然后发送给 FA。

(R6)一旦收到来自 HA 的回复,FA 检查回复消息中的 N_{FA} 是否与其刚广播的 N_{FA} 相同。如果相同,FA 计算他与 HA 之间的会话密钥 $K_{FA-HA}=r_{FA}H$,并丢弃 r_{FA}。随后 FA 验证 HA 的签名 δ_{HA}:计算 $h_1=H_1(ID_{HA},P_{HA})$,$h_2=H_2(M_4,ID_{HA},P_{HA})$。通过验证 $g^{\delta_{HA}}=H(P_{HA}y^{h_1})^{h_2}$ 是否成立来完成对 HA 的认证。接着用 K_{FA-HA} 解密$\{K_{MN-FA}\}K_{FA-HA}$得到 K_{MN-FA} 作为外地代理与移动节点之间的会话密钥。

(R7):$FA\rightarrow MN:M_5,<M_5>K^0_{MN-HA}$。

最后 FA 把 M_5 和$<M_5>K^0_{MN-HA}$转发给 MN。

(R8) MN 收到消息 R7 后,首先验证 N_{MN} 的有效性。如果收到的 N_{MN} 是有效的,MN 用在 R1 中使用过的密钥 K^0_{MN-HA} 去验证$<M_5>K^0_{MN-HA}$来完成对 HA 的认证。

然后计算

$K'_{MN-HA}=\mathrm{HMAC-SHA-1}(K^0_{MN-HA},N'_{HA}\|N_{MN}\|HA_{id})$,

$K_{MN-FA}=\mathrm{HMAC-SHA-1}(K^0_{MN-HA},N^0_{HA}\|N_{MN}\|FA_{id})$,并计算新的临时身份标识符 $TID'=H(ID_{MN}\|N'_{HA})$。

最后更新动态参数存储器里的参数$(ID_{MN},H(ID_{MN}\|N'_{HA}),K'_{MN-HA},N'_{HA})$用作下一次注册请求消息的构造。

3)移动节点 MN 与通信节点 CN 之间通过隧道技术进行的通信,当 CN 向 MN 发送数据时,HA 截获该数据包,并通过隧道封装数据包发送到 MN 的转交地址。在隧道的出口,FA 解封该数据包,并把它转发给 MN。

2.2 安全性分析

2.2.1 移动 IP 中 3 个移动实体之间的相互认证

提出的这个协议里面,MN 与 HA 之间的相互认证是通过在 R4 和 R8 分别验证$<M_2>K^0_{MN-HA}$和$<M_5>K^0_{MN-HA}$来实现的。采用前述的无证书签名方案,FA 与 HA 之间通过在 R4 和 R6 分别验证 δ_{FA} 和 δ_{HA} 来完成相互认证。MN 与 FA 之间相互认证是间接的方式通过对 HA 的认证来完成的。

2.2.2 完整性保护

如果一个攻击者改变了 FA 和 HA 之间的注册消息,那么 HA(或者 FA)对于在 R4 和 R6 接收到的外地一家乡认证扩展域里的 δ_{FA}(或者 δ_{HA})用算法 Verify 进行验证,就可以知道消息是否被修改过。MN 和 HA 之间的注册消息的完整性可以通过计算消息认证码$<M_2>K_{MN-HA}$和$<M_5>K_{MN-HA}$来确保。

2.2.3 重放保护

协议通过生成临时随机数 nonce 抵抗重放攻击。如果一个攻击者重放一个以前被 HA 成功接收过的注册请求消息,由于这个请求消息里面旧的 N_{HA} 不等于 HA 目前保存的 nonce,所以 HA 将会拒绝这个注册请求消息。同理,MN 也通过 N_{MN} 为注册回复消息提供重放保护。如果攻击者试图从以前成功运行的注册过程中选择按次序重放一个有效的注册请求消息和之对应的回复消息给 FA,由于我们的协议在注册消息中使用了 FA 的临时随机数 N_{FA},那么 FA 通过查看将会发现这 2 个注册消息中的 N_{FA} 不同于 FA 在最近一次代理广播中发送的 nonce,所以攻击者不能欺骗 FA。因此,包含 N_{FA}、N_{MN} 和 N_{HA} 的注册消息能够抵制所有的重放攻击。

2.2.4 一次注册后密钥的安全分发

长时间使用相同的密钥是安全方案的 1 个潜在的弱点。因此,HA 分别产生动态的密钥 K'_{MN-HA} 和 K_{MN-FA};同样地,这 2 个密钥是在 MN 端本地产生,而不是由 HA 通过链路传送给 MN,这意味着更高级别的安全。HA 用密钥 K_{FA-HA} 加密 K_{MN-FA} 后把密文传送给 FA,FA 解密得到密钥 K_{MN-FA}。在该协议中,FA 与 HA 之间的动态密钥 K_{FA-HA} 产生如下 $K_{FA-HA}=r_{FA}H=r_{FA}r_{HA}P=r_{HA}r_{FA}P=r_{HA}F$。

2.2.5 保密性

协议中,密钥 $K_{MN\text{-}FA}$ 和 $K_{FA\text{-}HA}$ 分别可以保证

MN-FA 和 FA-HA 之间的通信数据的安全。为了防止攻击者窃听，密钥 $K_{MN\text{-}FA}$ 是 HA 用密钥 $K_{FA\text{-}HA}$ 加密后传送给 FA 的。

2.2.6　用户匿名性

协议在构造注册消息时用一个不断变化的临时身份标识符代替用户的真实身份来提供用户的匿名性。这个临时身份标识符 TID 是通过对用户的真实身份 ID_{MN} 和 HA 的临时随机数 N_{HA} 进行哈希运算得到的，即 $\mathrm{TID}=H(ID_{MN}\|N_{HA})$，由于每次注册过程中 HA 的 nonce 都是变化的（$N_{HA}\neq N'_{HA}$），所以攻击者不能确认用户的真实身份或者跟踪用户的移动轨迹和当前位置。

2.3　安全及性能比较

2.3.1　安全性比较

首先将协议与已有方案进行安全属性比较。对比参照方案包括移动 IP 标准 RFC3344 建议的基本移动 IP 注册方案[1]、基于 CA-PKI 的方案[4]，以及 Yang 的协议[7]。对比结果见表 1，表中“＋”表示协议满足该属性，“－”表示不满足该属性。

由表 1 的结果可见，协议提供了比其它 3 个现有协议更高的安全级别。

表 1　安全性能比较

类型	实体间的双向认证	重放保护	数据保密	用户匿名性
基本协议	－	－	－	－
基于 CA－PKI	＋	－	＋	－
Yang	－	＋	＋	－
所提出的协议	＋	＋	＋	＋

2.3.2　性能比较

在性能对比中，选择基于 CA-PKI 的方案[4]，Yang 的方案[7]，Dang 的方案[12-13] 以及所提出的方案进行对比，原因是 4 个方案具有近似的安全强度和稳定性。

系统参数的取值直接参考以前的文献[15-16]。在 FA 和 HA 端选取 Pentium Ⅳ 2.1 GHz 处理器，运行 Windows XP SP 1.386；在 MN 端采用 206 MHz Strong ARM 处理器，运行 windows CE pocket PC 2002 操作系统。FA 和 HA 端的密码操作的运算时间是根据文献[17-18]估计的；MN 端密码操作的运算时间是从文献[19]获得的。系统参数和各个操作的运算时间与文献[13]一致。在此基础上，使用文献[12-20]中的估算方法来计算各个被比较协议的注册时延 $\mathrm{Registration\ time}=\mathrm{RREQ}_{MN-FA}+\mathrm{RREQ}_{FA-HA}+\mathrm{RREP}_{HA-FA}+\mathrm{RREP}_{FA-MN}$，下面从计算时延和信令开销 2 个部分对 4 个协议进行性能对比。

根据 Dang[13] 的计算结果，基于 Yang 的方案[7] 的时延为 36.663 ms，Dang 的时延为 21.840 ms，新提出的协议在移动用户与外地代理之间的 RREQ $MN-FA$ 和 RREP FA-MN 与 Dang 的协议相同，而外地代理和家乡代理之间的 RREQFA-HA 和 RREPHA-FA 与 Dang 的协议相比省去了费时的对运算，对其时延的估算结果约为 15.12 ms。由于基于 CA-PKI 的协议[4] 在 MN、FA 和 HA 端都有计算代价高的基于证书的公钥密码运算，所以它的注册时延一定较长，在此不做估算比较。图 2显示了 3 个协议的注册时延的比较结果。

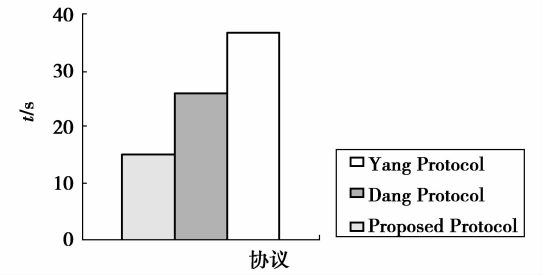


图 2　3 个协议注册时延的比较结果

由上述比较结果可见，相比于已有协议，提出的协议可以提供更完善的安全保护。同时，与 Dang 的协议相比，新协议的注册时延大约减少了 30%，与 Yang 的协议相比大约减少了 58%，获得上述改进的原因是

1）新协议采用无双线性对的基于无证书的公钥体制实现家乡代理和外地代理之间的认证。

2）移动节点和家乡代理之间的会话密钥由移动节点自己产生，节省了传输的时间以及加密解密的时间。

注册消息的大小则参考了 RFC2002 中规定的消息格式来计算。在新的协议中 MN 与 FA 之间链路上传输的消息略小于 Dang 的协议，而 FA 与 HA 之间的消息大小与 Dang 的协议相同。根据 Dang 的协议的估算结果，相比于 Yang 的协议，Dang 的协议传输的消息要小的多。具体结果可以参考 Dang 的协议，在此不作具体描述。

3　结　语

提出了 1 个不需要对运算的基于无证书的安全高效的移动 IP 注册协议。协议具有以下特点：

1）由于使用无对运算的无公钥证书的签名算法，从而减少了方案的运算量，降低了协议运行以及安全方面的开销；

2)协议通过使用消息认证码实现了 *MN*、*HA* 以及 *FA* 之间的两两互认证;会话密钥的本地生成使得协议具有高级别的安全保密性;在通信中用移动节点的临时身份代替真实身份从而实现了匿名性以及位置的隐私性。

3)通过在 *MN*、*HA* 及 *FA* 之间使用临时随机数 Nonce 从而可以抵抗任何可能的重放攻击。

如何将协议应用于 WLAN、CDMA 以及 3G 等各种不同的无线网络中是下一步的工作。

参考文献:

[1] PERKINS C. IETF RFC 2002 IP Mobility Support[S]. New York: IBM Network Working Group, 1996.

[2] ZAO J, KENT S, GAHM J, et al. A public-key based secure mobile IP[J]. Wireless Networks, 1999, 5: 373-390.

[3] YOO J P, KIM K, CHOO H, et al. Secure and scalable mobile IP registration scheme using PKI[C]// Proceedings of the International Conference on Computational Science and Its Applications, May 18-21, 2003, Montreal, Canada. Heidelberg: Springer-Verlag, 2003: 220-229.

[4] JACOBS S. Mobile IP public key based authentication [EB/OL]. (2008-03) http://www3.ietf.org/proceedings/9mar/slides/mobileip-key-99mar.pdf.

[5] YANG C C, HWANG M S, LI J W, et al. A solution to mobile IP registration for AAA[J]. Lecture Notes in Computer Science, 2003, 2524:329-337.

[6] MUFTI M, KHANUM A. Design and implementation of a secure mobile IP protocol[C]// Proceedings of the International Conference on Networking and Communication, June 11-13, 2004. Lahore, Pakistan: IEEE, 2004: 53-57.

[7] YANG C Y, SHUI C Y. A secure mobile IP registration protocol [J]. International Journal of Network Security, 2005, 1(1): 38-45.

[8] CAO X F, KOU W D, DANG L J, et al. Efficient mobile IP registration from pairings[C]// Proceedings of the IET International Conference on Wireless Mobile and Multimedia Networks, Nov. 6-9, 2006. Hangzhou, China: IEEE, 2006:143-147.

[9] CAO X, KOU W, LI H. Secure mobile IP registration scheme with AAA from parings to reduce registration delay[C]// Proceedings of the International Conference on Computer Intelligence and Security, Nov. 3-6, 2006. Guangzhou, China: IEEE, 2006: 1037-1042.

[10] CAO X F, KOU W D, LI H P, et al. An efficient anonymous registration scheme for Mobile IPv4[J]. Lecture Notes in Computer Science, 2007, 4456: 758-766.

[11] LEE B G, CHOI D H, KIM H G, et al. Mobile IP and WLAN with AAA authentication protocol using identity-based cryptography[C]// Proceedings of the 10th International Conference on Telecommunications, Feb. 23-March 1, 2003. Tahiti, Papeete: IEEE, 2003, 1: 597-603.

[12] JEONG K C, CHOO H, HA S Y. ID-based secure session key exchange scheme to reduce registration delay with AAA in mobile IP networks[J]. Lecture Notes in Computer Science, 2005, 3525: 487-506.

[13] DANG L, KOU W, DANG N, et al. Mobile IP registration in certificateless public key infrastructure [J]. IET Information Security, 2007, 1(4): 167-173.

[14] 王会歌,王彩芬,李泳斌,等. 没有 pairing 的无证书公钥签名方案[J]. 计算机应用, 2008, 28(6): 1395-1397.
WANG HUI-GE, WANG CAI-FEN, LI YONG-BIN, et al. Certificateless public key signature scheme without pairing[J]. Journal of Computer Applications, 2008, 28(6): 1395-1397.

[15] HESS A, SHAFER G. Performance evaluation of AAA mobile IP authentication [C/OL]// The 2nd Polish-German Teletraffic Symposium (PGTS'02), Gdansk, Poland, September, 2002: impact on https://www-tkn.ee.tu-berlin.de/publications/papers/pgts2002.pdf

[16] MCNAIR J, AKYILDIZ I F, BENDER M D. An inter-system handoff technique for the IMT-2000 system[C]// Proceedings of the Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies, March 26-30, 2000. Tel Aviv, Israel: IEEE, 2000, 1: 208-216.

[17] DAI W. Speed comparison of popular crypto algorithms: crypto++ 5.2.1 benchmarks [DB/OL]. (2004-07). http://www.weidai.com/index.html.

[18] BARRETO P S L M, KIM H Y, LYNN B, et al. Efficient algorithms for pairing-based cryptosystems[C]// Proceedings of the 22nd Annual International Cryptology Conference, August 18-22, 2002, Santa Barbara, California, USA. London: Springer-Verlag, 2002: 354-368.

[19] ARGYROUDIS P G, VERMA R, TEWARI H, et al. Performance analysis of cryptographic protocols on handheld devices[C]// Proceedings of the 3rd IEEE International Symposium on Network Computing and Applications, Aug. 30-Sep. 1, 2004, Cambridge, MA, USA. Washington: IEEE Computer Society, 2004: 169-174.

[20] JEON H, CHOO H, OH J H. Identification key based AAA mechanism in mobile IP networks[J]. Lecture Notes in Computer Science, 2004, 3043: 765-775.

(编辑 侯 湘)