无线 Mesh 网络轻量级容侵 CA 方案

郭 萍[1,2] 傅德胜[1] 朱节中[3] 袁程胜[1]
(南京信息工程大学计算机与软件学院 南京 210044)[1] (南京理工大学计算机科学与工程学院 南京 210094)[2]
(南京信息工程大学滨江学院 南京 210044)[3]

摘 要 为解决公钥体制过于复杂而难以在资源受限的无线环境中布署的问题,结合轻量级 CA(Certification Authority)概念、(t,n)门限机制和椭圆曲线离散对数公钥体制,构建一个适用于无线 Mesh 网络的轻量型容侵 LT-CA(Lite Tolerant CA)方案。分析表明,LT-CA 简化了传统基于证书 CA 公钥产生、验证及管理的复杂性,具有公钥产生轻量化、公钥验证轻量化、无需证书管理的特点;在没有显著增加系统复杂性的情况下,采用门限机制使 LT-CA 私钥具有容侵能力,可抵御无线环境下易于实施的多种攻击。

关键词 无线 Mesh 网络,椭圆曲线密码,门限机制,轻量级 CA
中图法分类号 TP309 **文献标识码** A

Scheme of Lite and Tolerant Certification Authority for Wireless Mesh Network

GUO Ping[1,2] FU De-sheng[1] ZHU Jie-zhong[3] YUAN Cheng-sheng[1]
(College of Computer and Software, Nanjing University of Information Science and Technology, Nanjing 210044, China)[1]
(College of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing 210094, China)[2]
(Binjiang College, Nanjing University of Information Science and Technology, Nanjing 210044, China)[3]

Abstract In order to solve the problems of complex public key cryptography which is difficult to implement in a resource-constrained wireless environments, a lite and tolerant CA(LT-CA) infrastructure was proposed which combines threshold mechanism with the idea of lite-CA(Certification authority) and ellipse curve cryptograph(ECC) public key mechanism. Comparing LT-CA with traditional Certification-based CA system, analysis shows LT-CA reduces the complications of producing and verifying public keys by generating public/private keys more flexibly and conveniently and it has the added benefit that it is certificateless. Moreover, LT-CA's private key possesses the ability of intrusion tolerance without obviously increasing the cost of system computing and payloads, and LT-CA can effectively defend against attacks that are known to occur in wireless environments.

Keywords Wireless mesh network, Ellipse curve cryptograph, Threshold mechanism, Lite-CA

1 引言

无线 Mesh 网络(Wireless Mesh Network, WMN)正成为无线网络研究的一个热点。WMN 是移动 Ad hoc 网络的一种特殊形态,是一种新型的宽带无线网络结构,是无线局域网(Wireless LAN)和 Ad hoc 网络的融合,并兼具二者优势。WMN 技术可应用于军事通信网、无线城域网、无线传感器网络、无线局域网等网络的"最后一公里",目前安全性是制约 WMN 广泛应用的最大障碍。身份认证是安全通信的基础,是系统安全的第一道防线,认证技术对开放的无线网络尤为重要。近年来公钥认证技术在 WMN 中的应用得到广泛研究[1-3],文献[1]构建一个安全的 WMN 漫游用户认证协议;文献[2]设计一个 WMN 中多方匿名认证协议;文献[3]提出一个解决密钥托管问题的基于身份 WMN 认证协议。这些认证方案都是基于单一认证服务器的,可能会遭遇两种不同的认证失效。第一种是误操作或错误配置导致认证服务器不可用;第二种是认证服务器遭受攻击,尤其是 DoS(Denial of Services)攻击,这对 WMN 是致命的,可引起整个网络的瘫痪或大量涉密信息的泄露。通常单一认证服务器是整个系统的失效点,在有线网络中,保存系统密钥的单一认证服务器受到层层保护,攻击者很难在有限时间内攻陷。无线环境的开放性及资源受限难以采用有线网络中常用的安全措施,因此利用单一服务器保存密钥是极不安全的。

1979 年,Shamir[4] 和 Blakley[5] 独立提出密钥分散管理概念,实现这一思想的机制称为(t,n)门限方案。随着无线设备容量、计算能力的不断增强,原来认为由于资源限制而不适用于无线环境的门限方案得到广泛研究[6-8]。文献[6]提出一个 WMN 分布式的信任机制,只有超过门限值的认证服务器合

到稿日期:2013-03-04 返修日期:2013-06-11 本文受国家科技部创新基金项目(10C26216205256),中国气象局项目([2013]069)资助。
郭 萍(1973-),女,博士,讲师,CCF 会员,主要研究方向为多跳无线网络安全、无线网络认证体系结构、认证协议及密钥管理;傅德胜(1951-),男,教授,博士生导师,CCF 会员,主要研究方向为信息安全、网络安全;朱节中(1975-),男,硕士,副教授,主要研究方向为信息安全、网络安全;袁程胜(1989-),男,主要研究方向为无线网络安全、密码学。

作才能颁发证书；文献[7]提出一种基于(t,n)门限机制WMN认证方案，其允许节点动态变化重组得到认证服务器私钥；文献[8]提出一种有效的抵御口令猜测攻击的门限口令认证方案。以上的认证方案虽然都采用了(t,n)门限方案，使得CA(Certificate Authority)具有一定的容侵性，但这些方案都是基于传统公钥证书的CA机制，这种CA体系任务繁重，承担对证书的管理、维护、撤销、更新等，在资源相对丰富的有线网络中也易成为系统瓶颈，再加上门限方案计算复杂，各认证服务器间需更多协同工作，无疑会进一步增加系统负载及复杂性，这使得在诸如Ad hoc、无线传感器网络等无线环境中，利用门限机制来共享密钥很难取得理想效果。WMN不同于一般的无线网络，它是有部分基础设施支持的无线网络，计算资源、存储能力及电源供应通常比其它无线网络丰富，这为在WMN中部署门限机制奠定了很好的物质基础。但是，还需要对传统基于公钥证书的CA系统加以改造才能应用到WMN中。

本研究工作将门限密码思想与基于轻量级CA公钥体制相结合，以椭圆曲线离散对数(Ellips Curve Cryptography，ECC)为主要加密算法，构建一种轻量级容侵CA架构(Lite Tolerant CA，本文简写为LT-CA)。该方案使CA具有容侵性，增强系统的可信性及顽健性；同时简化传统CA的功能及实现，避免传统基于证书CA公钥体制下繁杂的证书管理。

本文第2节介绍轻量级CA公钥密码系统的一般模型及Shamir秘密共享思想；第3节提出适用于WMN的轻量级容侵CA(LT-CA)方案；第4节对所提方案的性能及安全性进行分析；最后总结全文。

2 理论背景

2.1 轻量级CA(Lite CA)密码系统的一般模型

文献[9,10]系统阐述了轻量级CA密码系统的主要思想，与传统有线网络CA系统类似，产生一对公/私钥，所不同的是，前者将公钥通过CA签发的证书与用户身份绑定在一起，而轻量级CA系统中，公/私钥均由用户产生，公钥被分为两部分：一部分与传统CA系统的公钥一样是由密码算法决定的与私钥相对应的单向变换(本文称为主公钥)，另一部分是LCA对主公钥与用户身份的签名而生成的(本文称为辅公钥)。这样做的目的，一是取代了传统CA系统中的证书，达到轻量化的目的；二是将用户的公钥与其身份绑定，以辅公钥形式提供给其它用户以快速验证主公钥的合法性及权威性。这解决了基于身份公钥体制中易遭受替换公钥攻击[3]的问题：身份即公钥，因此无需证书，由于没有证书，公钥与其持有者的身份间缺乏权威绑定而易遭受恶意第三方替换公钥攻击。

轻量级CA(LCA)密码系统[11]是一个五元组$\Pi=(G_i, E_P, S_P, Sign, Verf)$，定义如下：

1. 产生用户主公钥及私钥算法G_i。G_i由用户执行，输入系统安全参数集K，输出用户的主公钥/私钥对$(PK_U^{\{Master\}}, SK_U)$，其中$PK_U^{\{Master\}}$为用户主公钥。

2. LCA产生用户辅公钥算法E_P。E_P由LCA执行，输入系统安全参数集K、LCA私钥SK_{LCA}(已由LCA上一级CA初始化时产生)及用户主公钥$PK_U^{\{Master\}}$、身份ID_U，输出用户的辅公钥$PK_U^{\{Slavery\}}$。

3. 产生用户全部公钥算法S_P。S_P由用户执行，输入系统安全参数集K、SK_{LCA}、$PK_U^{\{Master\}}$、$PK_U^{\{Slavery\}}$、ID_U，输出用户最终公钥对$(PK_U^{\{Master\}}, PK_U^{\{Slavery\}})$当且仅当$(PK_U^{\{Master\}}, ID_U)$经LCA合法签名。

4. 签名算法$Sign$。$Sign$是一个由任何相对消息进行签名的系统成员执行的签名算法，输入消息$m\in M$、系统安全参数集K、签名者私钥SK，得到输出$s\in S(s=Sign_{SK}(m))$。

5. 验证算法$Verf$。$Verf$是一个由验证者执行的验证算法，输入签名消息对(M,s)、系统安全参数集K、签名者公钥PK，由验证者执行并输出true或false。

2.2 Shamir秘密共享及主动秘密共享

文献[4]第一次提出秘密共享的概念，即(t,n)门限机制。密钥x(通常是系统的主密钥，如CA的签名私钥)可以被n个认证服务器$\{S_1, S_2, \cdots, S_n\}$所共享，其中任意大于或等于$t$个服务器可合作恢复密钥，而任意$t-1$或更少的服务器不能伪造出密钥。$x$按照如下方式分片：

1. 随机选择大素数$p(>x)$，及在Z_P上的$t-1$次多项式$f(\cdot)$，满足$f(0)=x$；

2. 将值$x_i=f(i)$秘密发送给服务器$S_i(i=1,2,\cdots,n)$。

当任意t个服务器合作时，密钥x可以根据拉格朗日插值定理有效求出。令$\phi\subset\{1,2,\cdots,n\}$且$|\phi|=t$，那么给定$(i, x_i)(i\in\phi)$，可以求出：$f(z)=\sum_{i\in\phi}(x_i\prod_{j\in\phi,j\neq i}\frac{z-j}{i-j})=\sum_{i\in\phi}x_iL_i^z$，其中$L_i^z=\prod_{j\in\phi,j\neq i}\frac{z-j}{i-j}$是拉格朗日系数，因此$x=f(0)=\sum_{i\in\phi}(x_iL_i^0)$。在秘密共享的基础上，周期性地刷新$n$个认证服务器的子密钥，并使得刷新后的各子密钥与旧子密钥不同，但并不改变原始密钥x即主动秘密共享，会进一步提高(t,n)门限机制的安全性。

3 适用于无线Mesh网络的轻量型容侵CA(LT-CA)方案

根据上述模型，构造一种更适用于无线Mesh网络(WMN)的LT-CA方案，其应满足如下一些要求：

1. 用户或Mesh节点的公/私钥全部由自己产生(用户专指WMN的本地用户，不含异地访问用户(这部分用户访问WMN需要与家乡网络合作进行认证，篇幅所限，本文不涉及)；本文Mesh节点主要指负责认证的无线路由器)。

2. 为解决用户公钥与其身份绑定问题，仍需传统意义上的CA，这里引入文献[11]将其轻量化的思想，最大限度地减少传统CA所承担的工作，减少与WMN的交互，轻量级CA符合这样的要求。

3. LT-CA的私钥仍然是整个系统最为重要的信息。为了避免整个系统的单点失效，有效抗击DoS攻击，引入(t,n)门限机制，将LT-CA私钥由n个认证服务器分享，只有当其中任意t个认证服务器共同合作，才能恢复出LT-CA私钥。利用门限方案，可以有效地提高系统可用性，即使有少数认证服务器被攻陷或离线，剩余的认证服务器($>=t$)仍然可提供服务。同时，门限存储也极大提高了密钥的安全性。

4. 选择一种高效且运算尽量少的加密算法，本方案采用离散对数椭圆曲线加密算法(ECC)。

3.1 无线Mesh网络(WMN)中LT-CA角色描述

1. CA(有线网络CA)：有线网络CA帮助LT-CA进行初

始化，设置系统安全参数，初始化结束后，有线网络 CA 以离线方式存在，在系统参数不变的情况下，无需再与 WMN 进行交互。

2. LT-CA(轻量型容侵 CA)：本方案中的 LT-CA 由一组认证服务器$\{MAS_1, MAS_2, \cdots, MAS_n\}(n\geqslant 2)$组成($MASs$ 是 WMN 中负责认证的 Mesh 路由器)，在轻量型 CA 基础上进一步采用(t,n)门限机制，LT-CA 私钥由 n 个服务器共享。负责 WMN 中本地用户 *MeshUsers*(MUs)初始化，将 MUs 产生的主公钥与其 ID 信息由 LT-CA 绑定签名产生用户辅公钥，同时对访问 WMN 的异地用户进行身份认证。

3. WMN 本地用户 *MeshUsers*(MUs)：由其自己产生主公钥及私钥，并假设已在有线网络 CA 处注册，是允许进入 WMN 的合法用户，但是由 WMN 的 LT-CA 为其主公钥及身份进行签名产生辅公钥，这相当于 LT-CA 对 MU“颁发证书”，初始化结束后，获得自己全部的公/私钥对$\{(PK_{MU}^{(Master)}, PK_{MU}^{(Slavery)}), SK_{MU}\}$。可以合法访问 WMN，获取相关数据；与其它合法用户或服务器进行通信。

由上所述，LT-CA 结构如图 1 所示。

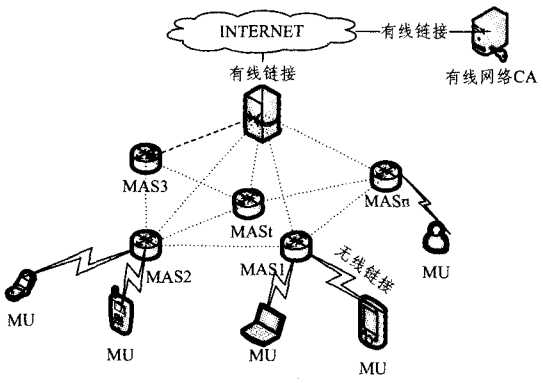

图 1　无线 Mesh 网络 LT-CA 结构

3.2　LT-CA 公/私钥生成

初使化在有线网络 CA 的帮助下完成如下步骤：

1. 参数准备。获得椭圆曲线系统参数 $T=\{p,F_q,a,b,G,n,h(\cdot)\}$，更多椭圆曲线密码系统细节详见文献[12]。选取安全椭圆曲线 $E(F_q)$，其中 F_q 是一有限域(p 是大素数)，基点 $G\in E(F_q)$，n 为素数且 $order(G)=n$，$a,b\in E(F_q)$，$h(\cdot)$是单向哈希函数：$h:\{0,1\}^*\rightarrow\{0,1\}^n$。

2. 有线网络 CA 随机选取 F_q 上一个 $t-1$ 次多项式 $f(x)$，且 $f(0)=d$(d 为 LT-CA 私钥)。

3. 计算 $Q=dG$，如果 Q 是无穷远点或 G 转第 2 步，否则 Q 是 LT-CA 公钥。

4. 选取互异元素 $x_1,x_2,\cdots,x_n\in F_q$，计算 $d_i=f(x_i)\pmod q$，$Q_i=d_i\times G(i=1,2,\cdots,n)\in E_p(a,b)$，公开 $Q_i(i=1,2,\cdots,n)$。

5. $d_i(i=1,2,\cdots,n)$为子私钥，$Q_i(i=1,2,\cdots,n)$为与 d_i 相对应的子公钥。由 Shamir 门限方案，已知$(x_i,d_i)(i=1,2,\cdots,n)$中任意 t 个可重构私钥 d。假设现已知$(x_i,d_i)(i=1,2,\cdots,t)$，由 Lagrange 插值公式易通过计算 $d=f(0)=\sum_{i=1}^{t} d_i\prod_{j=1,j\neq i}^{t}\frac{x_j}{x_j-x_i}\pmod q$恢复私钥 d。

6. 有线网络 CA 通过安全信道秘密地将 $d_i(i=1,2,\cdots,n)$传送给认证服务器组 $MASG=\{MAS_1,MAS_2,\cdots,MAS_n\}(n\geqslant t)$，每个服务器验证 $Q_i=d_i\times G(i=1,2,\cdots,n)$是否成立，若成立则接受 $d_i(i=1,2,\cdots,n)$作为自己的子私钥，否则不接受。各认证服务器获得一对子公/私钥$(Q_i,d_i)(i=1,2,\cdots,n)$，公开 $Q_i(i=1,2,\cdots,n)$，保密 $d_i(i=1,2,\cdots,n)$。

通过以上 6 步，LT-CA 的私钥被分配到 n 个认证服务器上，各认证服务器获得一对子公/私钥$(Q_i,d_i)(i=1,2,\cdots,n)$，有线网络 CA 销毁 d 及 d_i，以离线方式存在。

3.3　WMN 本地用户(MU)公/私钥生成

3.3.1　MU 主公钥及私钥生成

MU 执行 G_i 算法，输入系统参数 $T=\{p,F_q,a,b,G,n,h(\cdot)\}$，输出 MU 主公钥/私钥对$(PK_{MU}^{(Master)}, SK_{MU})$，其中 $SK_{MU}\in F_q$，$PK_{MU}^{(Master)}=SK_{MU}G$。

3.3.2　MU 辅公钥的生成

LT-CA 执行 *Sign* 算法，辅公钥即是 LT-CA 对用户 MU 主公钥签名的过程：

1. LT-CA 的认证服务器 $MAS_r(r\geqslant t)$执行 *Sign* 算法。

2. MU 随机产生一整数 $k_i(1\leqslant k_i\leqslant n-1)$，计算并广播 $R_i=k_iG$。

3. MU 向 MAS_r 发送签名请求$\langle Request, ID_{MU}, M, k_i, R_i\rangle$，其中 $M=(ID_{MU}\,|\,PK_{MU}^{(Master)})$为签名消息，为确保所有子签名能够在同一周期内返回，MU 启动本机定时器进入计时等待状态。

签名服务器组 MAS_r 响应过程：$MAS_r(r\geqslant t)$接收到 MU 的请求后，首先对 MU 身份进行认证(篇幅所限，认证过程另著文述之)，执行如下步骤：

1. 计算 $r=R_{ix}\pmod n$(R_{ix}是点 R_i 的 X 轴坐标值)；$s_i=d_ir+k_ih(M)\pmod n$。

2. MAS_r 向 MU 发送响应消息$\langle Response,r,s_i\rangle$。

MU 端签名重构：在签名时间定界内，MU 收到 t 个$\langle Response,r,s_i\rangle(i=1,2,\cdots,t)$响应消息后，计算 $s=\sum_{i=1}^{t}s_i$，然后输出 $PK_{MU}^{(Slavery)}=(r,s)$作为 MU 的辅公钥。

3.3.3　MU 对辅公钥验证

MU 执行验证算法 $Verf$：

1. 输入椭圆曲线系统参数 $T=\{p,F_q,a,b,G,n,h(\cdot)\}$、MU 的主公钥 $PK_{MU}^{(Master)}=SK_{MU}G=Q'$和辅公钥 $PK_{MU}^{(Slavery)}=(r,s)$。

2. MU 检查 r 是曲线上的有效点，并且 $1<s,r<n-1$。

3. MU 计算 $e=h(M)$，$w=e^{-1}$和 $V=swG-rwQ'$。

4. $v_x=V_X\bmod n(V_X$ 是点 V 的 X 轴坐标值)，若 $v_x=r$，则验证成功，$PK_{MU}^{(Slavery)}=(r,s)$为 $M=(ID_U\,|\,PK_{MU}^{(Master)})$的签名，MU 接受$(r,s)$作为其辅公钥。

3.3.4　MU 获取全部密钥阶段

1. E_P 是由 LT-CA 执行的算法，输入系统安全参数集 $T=\{p,F_q,a,b,G,n,h(\cdot)\}$、$PK_{MU}^{(Master)}$、$ID_{MU}$，输出用户辅公钥 $PK_{MU}^{(Slavery)}$，其中 $PK_{MU}^{(Slavery)}=(r,s)$，$s=\sum_{i=1}^{t}s_i=\sum_{i=1}^{t}(d_ir+k_ih(ID_{MU}\,|\,PK_{MU}^{(Master)}))$，即 LT-CA 中至少 t 个认证服务器用自己的子密钥对 MU 身份及其主公钥签名，MU 收集 t 个子签名重构后生成其辅公钥。

2. S_P 是由 MU 执行的算法，输入系统安全参数集 $T=\{p,F_q,a,b,G,n,h(\cdot)\}$，$PK_{LTCA}$，$(ID_{MU}, PK_{MU}^{(Master)})$，$PK_{MU}^{(Slavery)}$，输出 MU 最终公钥$(PK_{MU}^{(Master)}, PK_{MU}^{(Slavery)})$当且仅当$(PK_{MU}^{(Master)}, ID_{MU})$经 LT-CA 合法签名。

3. MU 发布自己的公钥参数$(ID_{MU}, PK_{MU}^{(Master)},$

$PK_{MU}^{(Slavery)}$），同时保密其私钥 SK_{MU}。

4 LT-CA 方案分析

4.1 LT-CA 结构特点

1. 权威中心 LT-CA 的轻量化

传统基于证书公钥系统的运行过程中，对 CA 的安全性要求极高，整个系统安全是建立在假设 CA 是完全可信的前提下。但本方案中，由一组认证服务器构成的 LT-CA 无需完全可信，它为 WMN 本地用户的身份及主公钥签名生成辅公钥。MU 的私钥/主公钥由其自己产生，一来减轻 LT-CA 的负担，二来使得 WMN 对用户密钥管理是分布式的，避免了 LT-CA 成为整个系统的瓶颈。辅公钥一方面用于证明 MU 是经 LT-CA 认证的合法用户；另一方面用于需要相互通信的 MU 之间的身份验证；同时也避免了恶意第三方由于没有证书而对主公钥实施的替换攻击。辅公钥不参与通信中的加/解密工作。所以本方案中的 LT-CA 不仅功能上轻量化，安全可信方面也达到轻量化。

2. LT-CA 的容侵能力

LT-CA 私钥 $SK_{LTCA}=d$ 是整个系统最重要的秘密信息。因此本文采用 (t,n) 门限机制将其分片后存储到 n 个认证服务器上，只有其中的 t 个或多于 t 个服务器合作才能恢复出私钥 d，换言之，即使 $t-1$ 服务器遭受攻击瘫痪或泄露其子密钥，系统还是安全的，这有效地提高了 LT-CA 私钥的安全性，对抗击 DoS 攻击赢得宝贵时间，达到一定的入侵容忍目的。t 和 n 取值的改变可以满足更高的安全需求，LT-CA 还可以对各服务器的子密钥进行周期性刷新，且刷新后各服务器的新子密钥与之前的旧子密钥不同，但所有服务器仍共享私钥 d，这意味着攻击者必须在同一周期内攻陷服务器的个数达到门限值 t 才有可能获得私钥 d，否则每个周期中都不能获得 LT-CA 私钥，这使得 LT-CA 系统具有前向安全性。

3. 与其它容侵公钥系统结构的比较

本文方案构建在轻量级 CA 系统之上，与其它容侵公钥系统相比，本方案(LT-CA)的特点如表 1 所列。

表 1 LT-CA 与其它公钥系统的比较

比较项	基于证书容侵 CA 系统[13]	基于身份容侵系统[14]	轻量级容侵 CA 系统
生成私钥方	CA	PGC	用户
生成公钥方	CA	用户身份	用户和 LT-CA
公/私钥管理方式	集中式	私钥集中式，公钥分布式	分布式
公钥与用户身份一致性证明	传统证书	无证书，用户身份即公钥	LT-CA 对用户身份及主公钥签名生成辅公钥
是否需要证书	是	否	否
密钥更新方式	CA	PGC 及用户	用户及 LT-CA
发现恶意用户敏感度	敏感，定期发布 CRL 列表	较敏感	较敏感，辅公钥类似于证书
第三方可信性	高(CA)	高(PGC)	中(LT-CA)
第三方是否系统瓶颈	是(CA)	是(PGC)	不完全是(LT-CA)
系统可扩展性	优	一般	良
系统容侵性	相当	相当	相当
主要缺陷	过于复杂，不适用于无线网络	私钥被 PGC 强制托管	初始化过程仍需要比 LT-CA 更可信的高一级 CA 帮助

从表 1 可见，LT-CA 既克服了传统 CA 公钥系统繁杂的证书管理，又避免了基于身份公钥系统中用户私钥被私钥生成中心(Private Key Generation Center，PGC)强制托管的问题。更为重要的是，与传统 CA 相比，LT-CA 不持有用户的公/私钥，由 LT-CA 签名用户身份及主公钥而生成的辅公钥只起验证用户身份的作用，并不参与任何加/解密工作。因此 LT-CA 是一个无需完全可信的第三方实体，适用于资源受限，难以部署复杂安全措施的无线环境。

4.2 LT-CA 认证复杂性分析

本文中 LT-CA 利用椭圆曲线离散对数公钥体制构建整个方案，因此，方案中涉及的主要运算是椭圆曲线上倍点运算。而原有的无证书 CA 系统多建立在基于身份密码学基础上，不可避免地要使用双线性对计算。相比较而言，椭圆曲线上对运算所耗费的时间远大于椭圆曲线上的倍点运算[15]。本文中的算法主要需要进行点乘运算 TG_{pmul}、乘法运算 TG_{mul}、加法运算 TG_{add}、单向散列运算 T_H 和数模运算 T_M 等；n 是认证服务器个数，t 是门限值。用户端和认证服务器组在各个阶段的计算量详见表 2。

表 2 计算复杂性

	初使化阶段	签名阶段	验证阶段
用户端计算量	$2TG_{pmul}$	tTG_{add}	$2TG_{pmul}+2TG_{mul}+TG_{add}+T_H$
认证服务器组计算量	$nTG_{pmul}+ntTG_{mul}$	$2tTG_{mul}+tTG_{add}+T_H+tT_M$	
交换信息次数	0	2	0

用户初使化阶段仅指主公钥和私钥的产生，经过签名阶段和验证阶段才能产生辅公钥。通过表 2 可以看出，本方案算法基本采用的是运算速度较快的点乘运算、乘法运算、加法运算、散列运算和数模运算，没有比较耗时的双线性对运算和指数运算。

4.3 LT-CA 与单 CA 认证系统性能比较

1. LT-CA 与轻量级单 CA 认证方案的比较

按照以上设计，本文实现了一个(3,5)原型系统(C++语言编程，认证服务器配置为 Intel DuoCore 1.99GHz CPU，2GB RAM)，为便于比较，用同样的轻量级思想实现单 CA 认证方案。图 2 是本方案与单 CA 认证方案均采用 ECC 算法的签名效率对比(注：轻量级 CA 中签名过程即是辅公钥生成过程)。

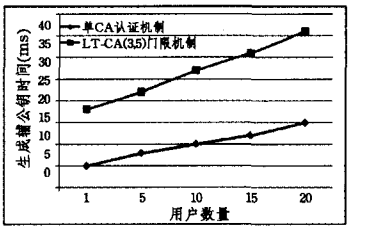

图 2 签名效率对比

由图 2 可见，LT-CA 门限机制签名代价高于单 CA 认证方案，用户数量为 20 时，单 CA 认证方案约需 18ms 为 20 个用户生成辅公钥，而本方案约需 48ms，但是本方案具有一定的入侵容忍特性，安全性远高于单 CA 认证方案，时间代价的增长在可接受范围内。

2. LT-CA 与基于身份(ID-RSA)单 CA 认证方案的比较

为了进一步说明本方案 LT-CA 提供服务的时间性能，与文献[16]基于身份的 RSA 算法构建的单 CA 认证方案进行对比，采用仿真环境 SWANS(Scalable Wireless Ad hoc Net-

work)[17]模拟两方案为不同规模节点签名生成辅公钥/证书的时间代价，仿真环境参数如表3所列。

表3 仿真参数

参数	参数值
MAC协议	MAC-802.11
路由协议	GPSR(Greedy Perimeter Stateless Routing)
频率	2.4GHz
带宽	11Mb/s
计算机	Intel DuoDorel.99GHz CPU
RAM	2GB
RSA	1024bits
双线性对参数	参见文献[18]
ECC	160bits
节点规模	[10,100]

ID-RSA方案是基于身份的以RSA算法构建的单CA认证系统，本文LT-CA方案采用(3,5)门限机制及ECC算法构建，仿真结果如图3所示。

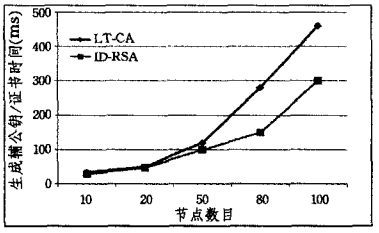

图3 LT-CA(生成辅公钥)与ID-RSA(生成证书)用时对比

由图3可见，本文所构建的LT-CA在(3,5)门限机制情况下与文献[16]构建的ID-RSA单CA认证系统为节点提供服务(LT-CA生成辅公钥过程，ID-RSA生成证书过程)的时间在节点数目小于50时相当，即使数目达到100，LT-CA比ID-RSA多耗时约150ms，但本方案具有容侵能力，而ID-RSA是单CA认证方案，时间代价的增长在可接受范围内。

3. 存储量比较

初始化完成后，LT-CA中的认证服务器需存储公钥，签名私钥份额，Mesh用户需存储自己的私钥、主公钥、辅公钥(由LT-CA生成)。为便于分析，本方案与单认证服务器方案均采用椭圆曲线公钥密码算法(ECC-160bits，下文b代表比特，B代表字节)，用户ID号为16b，公/私钥为160b，辅公钥为480b[19]。随着用户数量的增多，本方案实现的(3,5)门限机制存储量与单CA认证机制存储量的比较结果见表4。

表4 存储量对比

比较项	本方案-(3,5)门限机制	单CA认证机制
私钥/私钥的份额	160b	160b
公钥	160b	160b
辅公钥	480b	480b
初始化结束后认证系统的存储量	至少500B	至少100B
初始化结束后一个用户/节点的存储量	约200B	约120B
申请用户/节点平均数目为10时认证系统的总存储量	约2500B	约1300B

由表4可见，初始化结束后，单CA认证服务器存储量至少为100B(私钥160b+公钥160b+辅公钥480b)，本方案(3,5)门限机制LT-CA系统存储量约为500B(100B×5)；单CA认证服务器一个用户/节点的存储量约为120B(私钥160b+公钥160b+辅公钥480b+CA公钥160b)，本方案LT-CA一个用户的存储量约为200B(私钥160b+公钥160b+辅公钥480b+CA服务器组公钥(160b×5))；申请用户/节点平均数目为10时单CA认证系统的总存储量约为1300B(100B+120B×10)，而本方案LT-CA系统的总存储量约为2500B(500B+200B×10)。由分析可见，本文构造的LT-CA认证方案存储量与单CA认证系统的存储量接近，却使系统主密钥具有容侵特性，极大地提高了安全性。

4.4 LT-CA安全性分析

1. 密码学基础的安全性：本方案所采用的密码算法的安全性是椭圆曲线离散对数难解性问题及(t,n)门限机制的安全性无条件保障。

2. DoS攻击：LT-CA各认证服务器分别对持有的子密钥进行周期性刷新，并使新的子密钥仍然共享同一个私钥d。这意味着恶意攻击者必须在同一周期内攻陷并获取的子密钥个数达到门限值t，否则无法获取LT-CA的私钥d。即使攻击者已攻陷$t-1$个认证服务器并获取$t-1$个子密钥，刷新后，旧的子密钥对攻击者获取新的子密钥没有任何帮助。因此n,t的取值及合适的刷新周期，三者相互制衡，极大提高了LT-CA对抗DoS攻击的有效性。

3. 伪装攻击：攻击者如果想伪装成合法用户登陆WMN，必须拥有LT-CA颁发的辅公钥，即使假造一个$PK_{attacker}^{(Slavery)}$，声称自己是合法用户，访问WMN网络，也因为其$PK_{attacker}^{(Slavery)}$没有经过LT-CA签名，用LT-CA的公钥解密$PK_{attacker}^{(Slavery)}$，无法得到$(ID_{attacker}|PK_{attacker}^{(Master)})$，因此很容易判定攻击者不是经LT-CA认证的合法用户。由于辅公钥的使用类似于传统CA系统中的证书，在不知道LT-CA私钥情况下，攻击者不能伪造虚假身份，因此类似中间人攻击很容易被识别。

4. 替换攻击：在基于身份的公钥机制或无证书公钥机制中，公钥与公钥持有者身份间的绑定无从证明，在交互双方通过公钥进行会话密钥的协商过程中，极易被未授权第三方发起中间人攻击，进而替换合法用户的公钥，或冒充成合法用户窃取机密信息。在本方案中，辅公钥是LT-CA的私钥对合法用户身份及其主公钥签名，相当于轻量型的证书。攻击者想替换合法用户的主公钥，首先要获得LT-CA对其身份及主公钥的签名，这在它进入WMN的认证阶段就已严格控制，在WMN用户的交互过程中攻击者想发起替换攻击是不可行的。

结束语 无线网络的开放性，使得密钥安全更为重要。设计一个CA系统，使其既有传统CA系统分发密钥认证的安全可信，又能避免证书管理的繁杂；考虑到WMN具有一定基础设施的支持，计算资源相对丰富，采用分布式CA使系统具有一定的容侵性，进一步提高WMN网络CA系统的安全性，是本文致力解决的问题。本文所提LT-CA方案与前人研究工作不同之处在于：1)结合(t,n)门限机制，构建具有一定容侵能力的分布式CA认证系统，克服前人工作多是构建单CA系统，造成CA是整个系统单失效点的缺陷；2)引入轻量级CA概念，设计一种更适用于资源受限无线环境、避免证书管理的轻量级CA结构，解决了前人工作中以传统CA为基础，导致证书管理是无线网络中不可逾越的瓶颈问题。分析表明：LT-CA结构简化了传统基于证书CA公钥机制产生及验证的复杂性，具有产生公钥轻量化、公钥验证轻量化、无

(下转第232页)

应用[J]. 中文信息学报,2009(5):125
[4] 刘振鹿,王大玲,冯时,等. 一种基于 LDA 的潜在语义区划分及 Web 文档聚类算法[J]. 中文信息学报,2011,25(1):60-67
[5] 曹娟,张勇东. 一种基于密度的自适应最优 LDA 模型选择方法[J]. 计算机学报,2008,31(10):1780-1788
[6] 李文波,孙乐,黄瑞红,等. 基于 Labeled-LDA 模型的文本分类新算法[J]. 计算机学报,2008,31(4):620-627
[7] 石晶,范猛,李万龙. 基于 LDA 模型的主题分析[J]. 自动化报,2009,36:1586-1593
[8] Wei Xing, Croft W B. LDA-Based Document Models for Ad-hoc Retrieval[C]// SIGIR'06. Seattle, WA, USA, August 2006
[9] Friedman N, Geiger D, Goldszmidt M. Bayesian Network Classifiers[J]. Machine Learning, 1997, 2:131
[10] 姚全珠,宋志理,彭程. 基于 LDA 模型的文本分类研究 [J]. 计算机工程与应用,2011,13:29-38
[11] 徐戈,黄厚峰. 自然语言处理中主题模型的发展[J]. 计算机学报,2011,34(8):1423-1437
[12] 张明慧,王红玲,周国栋. 基于 LDA 主题特征的自动文摘方法[J]. 计算机应用与软件,2011,10:215
[13] Doucet A, Godsill S, Andrieu C. On sequential Monte Carlo sampling methods for Bayesian filtering[J]. Statistics and Computing, 2000, 3:197
[14] 马海云. 基于 Gibbs 抽样的测试用例生成技术研究[J]. 自动化与仪器仪表,2011,2:89-118
[15] Duda R O, Hart P E, Stork D G. Pattern Classification(2ed)[M]. 李宏东,姚天翔,等译. 机械工业出版社,2003:508
[16] Lin J. Divergence measures based on Shannon entropy[J]. IEEE Transactions on Information Theory, 1991, 37(14):145
[17] 王燕. 一种改进的 k-means 聚类算法[J]. 计算机应用与软件,2004,10(3):122
[18] 周昭涛. 文本聚类分析效果评价及文本表示研究[D]. 北京:中国科学院研究生院,2005

(上接第 204 页)

需证书管理;同时 LT-CA 私钥采用(t,n)门限机制由 n 个认证服务器共享,各服务器对持有的子密钥进行周期性刷新,使更新后的各子密钥仍然共享同一个秘密,系统的入侵容忍性极大提高,可抵御无线环境下易于实施的多种攻击;原型实现及仿真实验表明,门限机制并没有明显增加系统的计算量及负载,时间代价在可接受范围内,系统安全性显著增强,适用于资源受限的 WMN 网络。

参 考 文 献

[1] Qi Ji, Zhao Yi, Wang Xing-ming, et al. Security authentication and an undeniable billing protocol for WMNs[C]// Sterritt R. Proceedings of International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery. Huang Shan, China: IEEE Publisher, 2010:266-269
[2] Durahim A O, Savas E. A2-MAKE: An efficient anonymous and accountable mutual authentication and key agreement protocol for WMNs[J]. Ad Hoc Networks, 2011, 9(5):1202-1220
[3] Boudguiga A, Lauren URENT M. Key-escrow resistant ID-based authentication scheme for IEEE 802.11s Mesh Networks [C]// Kingston D. Proceedings of IEEE Wireless Communications and Networking Conference (WCNC). Quintana Roo, Mexico: IEEE Publisher, 2011:784-789
[4] Shamir A. How to share a secret [J]. Communications of the ACM, 1979, 22(11):612-613
[5] Blakley G R. Safeguarding cryptographic keys[C]// Smith M. Proceedings of the National Computer Conference. New York, USA: IEEE Publisher, 1979:313-317
[6] Kim J, Bahk S. Design of certification authority using secret redistribution and multicast routing in wireless mesh networks [J]. Computer Networks, 2009, 53(1):98-109
[7] Yang Kan, Jia Xiao-hua, Zhang Bo, et al. Threshold key redistribution for dynamic change of authentication group in Wireless Mesh Networks[C]// LIANG J. Proceedings of IEEE Global Telecommunications. Miami, USA: IEEE Publisher, 2010:1156-1151
[8] Chai Zhen-chuan, Cao Zhen-fu, Lu Rong-xing. Threshold password authentication against guessing attacks in Ad hoc networks[J]. Ad-hoc Networks, 2007, 5(7):1046-1054
[9] Dong Xiao-lei, Wang Li-cheng, Cao Zhen-fu. New public key cryptosystems with lite certification authority[EB/OL]. http://ePrint.iacr.org/2006/154, 2013-3-16
[10] 潘耘,王励成,曹珍富,等. 基于轻量级 CA 的无线传感器网络密钥分配方案[J]. 通信学报,2009,30(3):130-134
[11] Dong Xiao-lei, Wei Li-fei, Zhu Hao-jin, et al. EP^{2}DF: an efficient privacy-preserving date-forwarding scheme for service-oriented vehicular Ad Hoc networks[J]. IEEE Transactions on Vehicular Technology, 2011, 60(2):580-591
[12] Nenal K. Elliptic curve cryptosystems[J]. Mathematics of Computation, 1987, 48(13):203-209
[13] Roman R, Alcaraz C. Applicability of public key infrastructures in Wireless Sensor Networks[C]// LOPEZ J. Proceedings of European PKI Workshop: Theory and Practice. Palma de Mallorca, Spain: Springer LNSC4582, 2007:313-320
[14] He B, Agrawal D P. An identity-based authentication and key establishment scheme for multi-operator maintained Wireless Mesh Networks[C]// Nayak A, Stojmenovic I. Proceedings of Mobile Ad Hoc and Sersor Systems. San Francisco, USA: IEEE Publisher, 2010:71-78
[15] Lin Xiao-dong, Lu Rong-xing, Ho Pin-han, et al. TUA: a novel compromise-resilient authentication architecture for Wireless Mesh Networks[J]. IEEE Transactions on Wireless Communications, 2008, 7(4):1389-1399
[16] Eissa T, Razak S A, Ngadi M D. Towards providing a new light-weight authentication and encryption scheme for MANET[J]. Wireless Network, 2011(17):833-842
[17] Barr R. Swans-scalable wireless Ad hoc network simulator user's guide[EB/OL]. http://www.isi.edu/nsnam/ns, 2013-03-21
[18] Barreto P S L M, Kim H Y, Lynn B, et al. Efficient algorithms for pairing-based cryptosystems[C]// Yung M. Proceedings of the 22nd annual international cryptology conference on advances in cryptology. Santa Barbara, USA: Springer, 2002:354-368
[19] Gura N, Patel A, Wander A, et al. Comparing elliptic curve cryptography and RSA on 8bit CPUs[C]// Joye M, Quisquater J J. Proceedings of Workshop on Cryptographic Hardware and Embedded Systems. Boston, USA: Springer, 2004:119-132