

无线 Ad hoc 网络中基于身份的密钥管理方案

徐 倩¹, 张福泰¹, 刘志高^{1, 2}

(1 南京师范大学 数学与计算机学院, 江苏 南京 210097; 2 安徽工业大学 职业技术学院, 安徽 马鞍山 243001)

[摘要] 基于身份的密码体制 (ID-based cryptography) 是 SHAMIR 在 1984 年提出的, 使用该体制进行加密、签名和认证可以有效地减小系统中用户的存储代价和运算量. 将其应用到无线 Ad hoc 网络中, 提出了一个基于身份的密钥管理方案. 它采用基于身份的密码体制、秘密分享技术来实现私钥的分布式生成, 并且利用盲短签名机制有效地实现了私钥的安全分发. 该新方案可满足无线 Ad hoc 网络中密钥的安全需求, 同时能节省网络资源、提高网络性能.

[关键词] 无线 Ad hoc 网络, 密钥管理, 基于身份的密码体制, 秘密分享, 安全传输

[中图分类号] TP393 **[文献标识码]** A **[文章编号]** 1672-1292(2006)03-0056-06

The ID-based Key Management Scheme in Wireless Ad hoc Networks

XU Qian¹, ZHANG Futai¹, LIU Zhigao^{1, 2}

(1 School of Mathematics and Computer Science, Nanjing Normal University, Nanjing 210097, China)

2 College of Vocational Technology, Anhui University of Technology, Maan Shan 243001, China)

Abstract ID-based cryptography was introduced by Shamir in 1984. With this scheme for encryption, signature and authentication can effectively reduce the cost of storage and computational in systems. In this paper, we propose a new key management scheme for wireless ad hoc networks based on it. The recently developed techniques of ID-based cryptography and secret sharing are deployed to realize the distributed generation of the nodes' private keys. It also makes use of the blind short signature to ensure the secure distribution of the private key shares of nodes in public channel. Our scheme can satisfy all the security demands of key in wireless ad hoc networks. It can also save the resource of the network so that the network performance is greatly improved.

Key words wireless Ad hoc networks, key management, ID-based cryptography, secret sharing, secure transmission

0 引言

无线 Ad hoc 网络是由一组带有无线收发器的移动终端相互协作形成的一种新型网络, 它独立于固定的基础设施, 采用分布式管理技术, 能够快速配置、自组织工作. 由于其具有动态的网络拓扑结构、有限的资源、多跳的通信等固有特点, 将会受到更多的安全威胁. 所以在无线 Ad hoc 网络中, 必须利用密码学的理论与技术来有效地防范潜在的攻击. 而密码理论与技术在实际使用中的安全性, 主要依赖于密钥管理的安全性. 根据 Ad hoc 网络的特点, 一般要求节点密钥能动态生成且不依赖任何固定的第三方, 并确保密钥在传输中的安全, 同时具有较小的计算量、存储量和通信量.

基于身份的密码体制, 是 SHAMIR 在 1984 年提出的^[1]. 使用基于身份的密码体制, 不需要保存每个用户的公钥证书, 也无需利用一个公共文件存储所有用户的公钥, 所以能有效地减少传统公钥体制下用于证书管理的存储和计算开销.

利用基于身份的密码体制来实现无线 Ad hoc 网络中的密钥管理, 是提高网络性能的一种有效手段.

收稿日期: 2005-02-10

基金项目: 江苏省自然科学基金资助项目 (BK2006217) 和教育部计算机网络与信息安全重点实验室 (西安电子科技大学) 开放课题 (211070B456).

作者简介: 徐 倩 (1980-), 女, 硕士研究生, 主要从事密码学、网络安全等方面的学习和研究. E-mail: xuqian1@njjn.edu.cn

通讯联系人: 张福泰 (1965-), 博士, 教授, 主要从事信息安全及电子商务方面的教学与研究. E-mail: zhangfuta@njjn.edu.cn

目前在这一方面的研究成果还不多. 2003 年, KHALILI 和 KATZ 在文献 [2] 中首先提出了一个用于无线 Ad hoc 网络的基于身份的密钥管理方案. 该方案的基本思想是由一组选定的节点共同承担私钥产生中心 (KGC) 的职责, 它们根据 (t, n) 门限方案获得系统主密钥的一个份额, 联合为节点产生私钥. 此方案的最大缺点是承担 KGC 职责的节点固定, 它们不能随意离开网络. 由于其身份的特殊性可能成为网络的瓶颈, 甚至主密钥的泄漏. 最近 DENG 等人又提出一种新的基于身份的密钥管理方案^[3], 希望实现以完全分布式的方式建立用户私钥. 但其中产生新节点 u_p 主密钥份额的方法是错误的. 他们的方法是: 邻节点 u_i 利用自己的份额 s_i 计算出新节点的系统私钥子份额 $s_{s_i, i}$, 即 $s_{s_i, i} = s_i l_i(p)$ ($l_i(p)$ 是 Lagrange 系数), 再将计算出的 $s_{s_i, i}$ 发送给请求者 u_p . 这样做, 本质上 $u_{p, i}$ 已将自己的 s_i 泄漏给了 u_p . 如果 u_p 是攻击者, 那么在获得 t 个子份额后, 就可恢复出主密钥, 显然该方法不可行. 且现有基于身份的方案都要求节点间必须存在秘密信道用以传输私钥份额, 否则攻击者就能轻易获取节点所有的私钥份额, 再利用其解密实际通信中的消息或假冒签名. 但无线 Ad hoc 网络的特点使得事先建立安全信道相对比较困难.

鉴于现有方案都存在不足, 还不能完全满足无线 Ad hoc 网络的要求, 我们提出了一个基于身份的密钥管理方案. 它充分利用基于身份密码体制的优点, 同时采用基于可验证秘密分享的分布式密钥生成技术^[4-5]和盲短签名^[6]技术来实现私钥的生成、传输和管理, 不仅可较好的满足节点私钥的分布式生成以及在公开信道上的安全传输等安全需求, 而且有效地节省了网络的存储和计算代价.

1 预备知识

1.1 基于身份的密码体制 (ID-based cryptography)

在基于身份的密码体制中, 用户的公钥可以由任何人根据其唯一的身份计算出来, 而私钥则是由可信中心统一生成. 可见, 这种密码体制的优点在于: 公钥的获取需要很少的计算量以及通讯量; 不使用证书可以减少用户很多的存储量; 而且公钥的撤销也很容易实现. 可通过在公钥中增加终止期限或时间戳来完成. 所以, 在资源有限的无线 Ad hoc 网络中使用这种密码体制是具有一定优势的.

目前, 利用双线性映射, 已构造出许多安全高效的基于身份的加密方案^[7]和签名方案^[8-9].

定义 1 基于身份的加密方案 IBE 由 4 个算法 (IB-Gen, IB-Ext, IB-Enc, IB-Dec) 组成:

- IB-Gen 可信中心的系统参数和主密钥生成算法. 输入安全参数 k , 返回系统参数 $params$ 和 KGC 主密钥 $\langle IBPK, IBSK \rangle$.
- IB-Ext 用户私钥的生成算法. 输入主密钥、用户身份 ID (任意字符串), 返回对应于该身份的用户私钥 S_D .
- IB-Enc 基于身份的加密算法. 输入用户身份 ID 和需加密的消息 m , 返回该消息的密文.
- IB-Dec 基于身份的解密算法. 输入消息的密文以及用户私钥, 获得对应的消息 m .

定义 2 基于身份的签名方案 IBS 由 4 个算法 (IB-Gen, IB-Ext, IB-Sign, IB-Verify) 组成:

- IB-Gen 可信中心的系统参数和主密钥生成算法. 输入安全参数 k , 返回系统参数 $params$ 和 KGC 主密钥 $\langle IBPK, IBSK \rangle$.
- IB-Ext 用户私钥的生成算法. 输入主密钥、用户身份 ID (任意字符串), 返回对应于该身份的用户私钥 S_D .
- IB-Sign 基于身份的签名算法. 输入主密钥、需签名的消息 m 和签名者的私钥, 返回对该消息的签名 σ .
- IB-Verify 基于身份的验证算法. 输入消息 m 、相应的签名 σ 及用户身份 ID, 输出 $b \in \{0, 1\}$. 如果为 1 表示该签名有效可以接收, 否则拒绝.

1.2 门限秘密分享 (Threshold Secret Sharing)

秘密分享的概念由 SHAMIR 等人在 1979 年提出^[10]. 它是指将秘密 s 分割成若干个份额在一组参与者 $P = \{P_1, P_2, \dots, P_n\}$ 中进行分配, 使得每一个参与者都得到关于该秘密的一个份额. 而只有 P 的一些特定子集才能有效地恢复出 s . P 的其它子集将不能恢复 s , 甚至得不到关于秘密 s 的任何有用信息. 在秘密分享系统中最常见的是门限体制. 已提出的门限体制有多种, 其中 SHAMIR 的 Lagrange 内插多项式体制、BLAKLEY 的矢量体制、ASMUTH 的同余类体制及 KARNIN 的矩阵法体制是主要代表, 并已得到广泛的应

用. 我们主要采用 SHAM R 的方案.

SHAM R (t, n) 门限方案的基本参数为: n 为分享者 (参与者) 的数目; t 为门限值; p 为大素数, 且 $p > n \geq t$. 同时要求 p 大于秘密可能的最大取值. 秘密空间与份额空间相同, 均为有限域 $GF(p)$. x_1, x_2, \dots, x_n 为 $GF(p)$ 中 n 个互不相同的元素. 以上这些参数都是公开的.

SHAM R (t, n) 门限秘密分享方案由以下两个算法组成:

- S. Share 份额的分配算法: 分发者 D 首先随机选取 $GF(p)$ 上的一个 $t-1$ 次多项式 $h(x) = a_0 + a_1x + a_2x^2 + \dots + a_{t-1}x^{t-1}$, 使得 $a_0 = h(0) = s$ 为要在 n 个分享者中分享的秘密. D 对 $h(x)$ 保密. 然后 D 计算 $s_j = h(x_j) \bmod p, j = 1, 2, \dots, n$. s_j 就是 D 要发送给第 j 个分享者 P_j 的秘密份额.
- S. recover 恢复算法: 由任何 t 个点 $(x_{j_1}, s_{j_1}), (x_{j_2}, s_{j_2}), \dots, (x_{j_t}, s_{j_t})$ 根据 Lagrange 多项式插值法恢复出 $h(x)$, 并可计算出秘密 $s = h(0)$.

(t, n) 门限方案需假定分发者和分享者都是诚实的, 这在实际中是不现实的. 因此, 实际应用中, 往往要采用能抵抗分发者和分享者欺骗的可验证秘密分享方案^[5, 11]. 本文生成 KGC 主密钥时将用基于可验证秘密分享的分布式密钥生成技术^[4], 无需假定分发者和分享者为诚实的. 由网络中所有初始节点联合来产生 KGC 的主密钥, 而任意单个节点无法恢复出主密钥.

1.3 盲短签名 (blind short signature)

短签名^[12] 是 BONEH 等人提出的, 对于相同的安全参数, 其签名长度仅为 DSA 签名的一半, 但却可以提供相似的安全级别. 它能有效的减少签名在传输中的通讯代价, 这一点对在带宽有限的无线 Ad hoc 网络中实现安全传输是很有利的. 2003 年 BOLDYREVA 给出一种简单且高效的盲签名方案^[13]. 结合它们的优点, 文献 [7] 提出了盲短签名, 并用之于密钥在公开信道的安全传输. 本文将其应用到无线 Ad hoc 网络中, 实现了在公开信道中以分布式方式安全传输节点私钥.

设 $E(F_q)$ 为一个椭圆曲线, $P \in E(F_q)$ 是椭圆曲线的基点, 阶为素数 p 且 $p \neq q, p \nmid q-1$. G 是生成元为 P 的 Abe 加法群, $H: \{0, 1\}^* \rightarrow G$ 为单向 Hash 函数, 签名者的公钥记为 P_{sgn} , 则公开参数为 $\text{params} = \{G, p, P, H, P_{\text{sgn}}\}$. 文献 [7] 中的盲短签名方案包括下列 3 个算法:

- BS. Gen 签名密钥生成算法. 输入系统参数 params , 随机选择 $s \in Z_p^*$, 计算 $P_{\text{sgn}} = sP$, 返回 $(pk = (G, p, P, H, P_{\text{sgn}}), sk = s)$.
- S. Sign 盲短签名算法. 输入 params , 私钥 sk 及消息 $m \in G$, 输出 (m, σ) . 签名过程如下:
 - (1) 请求签名的用户随机选择 $r \in Z_p^*$, 计算 $\eta = H(m) \in G$, 将 η 发送给签名者;
 - (2) 签名者计算 $\rho = s \cdot \eta$, 将其发送给请求者;
 - (3) 请求签名的用户计算 $\sigma = r^{-1} \cdot \rho$, 恢复出对消息 m 的签名.
- S. Vrfy 盲短签名验证算法. 输入签名公钥 pk 及 (m, σ) , 检验 $e(P, \sigma) \stackrel{?}{=} e(P_{\text{sgn}}, H(m))$, 等式成立时输出逻辑值 1 以表示签名有效, 否则输出逻辑值 0 表示签名无效.

2 基于身份的安全密钥管理方案

本方案将工作在无线 Ad hoc 网络的初始化阶段 (Network Initialization) 和运行阶段 (Running System). 初始化阶段, 网络中所有节点联合产生基于身份体制下 KGC 的主密钥, 并使所有节点共同分担 KGC 的职责. 再通过本文提出的私钥传输方案分布式建立每个节点的私钥. 网络运行阶段, 允许节点动态加入. 新节点请求加入网络时, 由至少 t 个邻节点联合为其产生私钥. 采用和初始阶段相同的方法生成私钥后, 再从它任意 t 个邻节点处安全地获取自己的主密钥份额. 由此, 实现系统的完全分布式.

假设无线 Ad hoc 网络的初始化阶段有 n 个移动节点. 用于为节点生成私钥的系统主密钥记为 $\langle s, P_{\text{pub}} \rangle$. 其中: s 是系统私钥, 将在主密钥产生服务中以分布式方式生成, 并以 (t, n) 门限方案被所有节点分享, $P_{\text{pub}} = sP$ 是系统公钥. 节点通过向其邻节点请求私钥产生服务来建立自己的私钥.

下面详细介绍新方案的 3 个基本操作: 系统主密钥的产生、节点私钥的生成、新节点系统主密钥份额的产生.

2.1 系统主密钥的产生

采用文献 [14] 中的分布式密钥生成方案来产生系统主密钥是一个好的选择. 但为叙述简捷、节省篇

幅, 我们在这里用文献 [4] 中基于 Feldman 可验证秘密分享的分布式密钥生成方案. 过程如下:

- (1) 协商系统参数 params 由网络中所有初始节点共同协商一个安全参数集合 (包括门限值 $t \in \{G, p, q, P, H\}$ 等), 任何不愿接受这个安全参数集合的节点都可以拒绝加入该网络.
- (2) 每个节点 u_i 随机选择一个秘密 $x_i \in Z_q^*$, 并作为分发者将 x_i 在所有 n 个节点中分享. u_i 随机选取 F_p 上的一个 $t-1$ 次多项式 $f_i(z) = x_i + a_1z + \dots + a_{t-1}z^{t-1}$; 然后广播 $X_{ik} = a_{ik}P, k = 1, 2, \dots, t-1$ 及 $X_{i0} = x_iP$; 再计算给所有节点的关于 x_i 的子份额 $s_{ij} = f_i(j), j = 1, 2, \dots, n$, 并将其安全的发给节点 u_j .
- (3) 在成功接收到 $n-1$ 个子份额后, u_j 将先验证所接收到来自其它节点的子份额 s_{ij} . 即对所有 $i = 1, 2, \dots, n$ 验证 $s_{ij}P = \sum_{k=0}^{t-1} j^k X_{ik}$. 如果索引号为 i 时上式不成立, 那么 u_j 广播一个对 u_i 的抱怨. 当对 u_i 的抱怨多于 t 个, 就认为此节点是恶意的, 将撤销它的身份标识, 并把其所选的秘密值和它给各参与者的份额都记为默认值 0. 同时把各相应的公开信息记为无穷远点. 当对 u_i 的抱怨不超过 t 个时, 作为对每个抱怨的回应, u_i 广播相应的有效份额. 如其广播的某个份额仍无效, 则所有节点也将 u_i 所选的秘密值记为 0 相应的公开值记为无穷远点.

(4) u_j 计算对 $f(z) = f_1(z) + f_2(z) + \dots + f_n(z)$ 系数的承诺 $X_j = X_{1j} + X_{2j} + \dots + X_{nj}, j = 0, 1, \dots, t-1$.

(5) u_j 根据公式 $s_j = \sum_{i=1}^n s_{ij} = \sum_{i=1}^n f_i(j)$ 计算出它的系统私钥份额, 相应的公钥份额为 $T_j = s_jP = \sum_{k=0}^{t-1} j^k X_{jk}$, 所有参与者可从公开信息中计算出.

经过上述 5 步就以分布式方式安全地建立了系统主密钥 $\langle s, P_{\text{pub}} \rangle$, 其中: $s = \sum_{i=1}^n x_i \bmod q$ 作为共享秘密被保密, $P_{\text{pub}} = \sum_{i=1}^n X_{i0} = sP$ 作为系统的公开参数. 各参与者可计算对一个秘密的多项式 $f(z) = a_0 + a_1z + \dots + a_{t-1}z^{t-1}$ 的承诺: $X_i = \sum_{j=1}^n X_{ji}, i = 0, 1, \dots, t-1$. 此多项式满足 $s_i = f(i), a_0 = s$. 参与生成系统主密钥的每个节点 u_i 各自拥有关于 s 的一个份额 s_i . 利用基本门限方案的恢复算法, 任意 t 个节点联合由 $f(z) = \sum_{i=1}^t s_i l_i(z)$ ($l_i(z) = \prod_{j=1, j \neq i}^t \frac{z-j}{i-j}$ 是 Lagrange 系数) 可恢复出系统私钥.

2.2 节点私钥的产生

本方案采用基于身份的密码体制, 所以节点公钥由其身份直接计算, 即 $Q_{\text{id}} = H(\text{id})$. 而节点私钥由它任意 t 个邻节点联合产生. 假设节点 u_{id} 需要得到自己的私钥, 它首先广播请求, 并公布其身份 id . 接收到请求的任意 t 个邻节点将联合为 u_{id} 生成私钥. 同时利用文献 [6] 中的盲短签名技术实现了私钥份额在公开信道中的安全传输.

假设用户 A 是请求私钥产生的网络节点或是申请加入网络的新节点, u_i 是 A 的某个邻节点. 网络的系统参数为 $\text{params} = \{G, p, q, P, H, P_{\text{pub}}\}$, A 的有效身份为 ID_A , 公钥为 $Q_A = H(\text{ID}_A)$. T_i 是 u_i 的系统公钥份额. 则根据图 1 中的私钥传输方案, 用户 A 可从其邻节点处以交互方式安全地获取自己的私钥份额 ($\text{IBSK}_{\text{ID}_A}^{(i)}$). 成功接收至少 t 个有效的份额后, 根据基本门限方案就可恢复出对应于身份

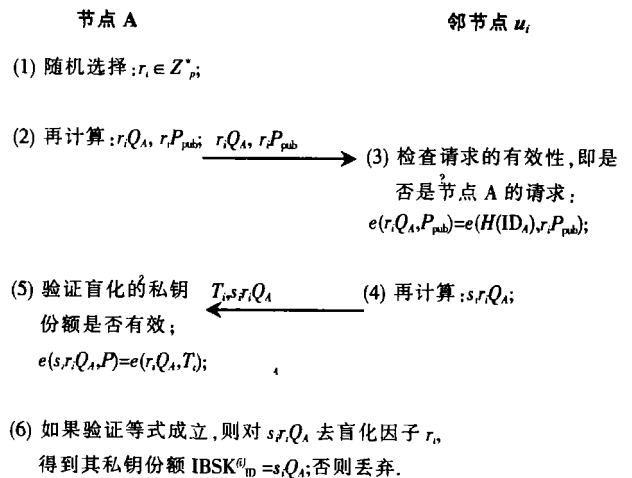


图 1 私钥的安全传输方案

D_A 的私钥 $IBSK_{D_A} = \sum_{i=1}^t l_i(z) IBSK_{D_A}^{(i)}$, $l_i(z)$ 是 Lagrange 系数.

2.3 新节点系统主密钥份额的产生

网络运行时, 节点可动态加入. 它首先发送请求建立个人私钥. 然后, 再向邻节点请求获得自己的主密钥份额, 从而在以后的网络生存时间内也能作为提供私钥产生服务的节点.

假设新节点为 u_p (其索引号为 p), 在建立好个人私钥后, 它广播请求以得到主密钥份额. 若邻节点中存在至少 t 个主密钥份额的拥有者 $\{u_{p_1}, u_{p_2}, \dots, u_{p_t}\}$, 则由它们来为新节点分配份额. 具体方法如下 (其中, T_{p_i}, X_i 分别为 u_{p_i} 的系统公钥份额和对多项式系数的承诺, 作为公开信息):

- (1) u_{p_1} 随机选择 $r \in Z_p^*$, 计算 $c_1 = r + s_1 l_1(p)$, 广播 $d_1 = rP$, 同时发送 c_1 给 u_{p_2} ;
- (2) for($i = 2$ to t ; $i++$)
 - u_{p_i} 验证 $c_{i-1}P = d_1 + l_1(p)T_{p_1} + l_2(p)T_{p_2} + \dots + l_{i-1}(p)T_{p_{i-1}}$;
 - 若成立, 计算 $c_i = c_{i-1} + s_i l_i(p)$;
 - 发送 c_i 给 $u_{p_{i+1}}$;
- (3) u_{p_t} 验证 $c_{t-1}P = d_1 + l_1(p)T_{p_1} + l_2(p)T_{p_2} + \dots + l_{t-1}(p)T_{p_{t-1}}$, 若成立, 则计算 $c_t = c_{t-1} + s_t l_t(p)$, 再发送 c_t 给 u_p , 广播 $c_t P$;
- (4) u_{p_1} 验证 $c_t P = d_1 + l_1(p)T_{p_1} + l_2(p)T_{p_2} + \dots + l_t(p)T_{p_t}$, 若成立, 则把秘密 r 发送给 u_p ;
- (5) 最后, u_p 计算出自己的系统私钥份额 $s_p = c_t - r$, 相应的公钥份额为 $s_p P = \sum_{k=0}^{t-1} P^k X_k$.

可以证明新节点以此算法获得的系统主密钥份额是正确的. 在主密钥的产生过程中, 节点的系统私钥份额 $s_j = \sum_{i=1}^n s_{ji} = \sum_{i=1}^n f_i(j)$. 同理, 新节点 u_p 应具有的系统私钥份额为:

$$s'_p = \sum_{i=1}^n f_i(p) = \sum_{i=1}^n \left[\sum_{j=1}^t f_i(j) \cdot l_j(p) \right] = \sum_{j=1}^t \left[\sum_{i=1}^n f_i(j) \right] \cdot l_j(p) = \sum_{j=1}^t s_j \cdot l_j(p).$$

可见 s'_p 和通过上述算法获得的 s_p 一致. 所以, 由该算法生成的系统主密钥份额有效. 该算法较好的解决了文献 [3] 中方案的安全缺陷, 可保证在生成新节点主密钥份额的过程中邻节点的 s_i 不泄漏给请求者.

3 安全性分析

新方案在产生系统主密钥时, 采用了基于 Feldman 可验证秘密分享技术的分布式密钥生成方案. 由于 Feldman-VSS 本身具有以下的安全特征: 利用公开信息 $X_0 = x_i P$, 不能得到需分享秘密 x_i 的任何信息, 这是基于求解离散对数的困难性. 且该方案不但可以有效的防止不诚实节点的干扰, 而且所建立的系统私钥具有很好的分布特征.

在建立节点私钥时, 采用基于盲短签名的私钥传输方案, 能实现在传输私钥份额时不再需要节点间事先存在任何安全关联, 并提供对将要建立私钥的认证. 所采用的盲短签名方案的安全性已经在文献 [6] 中得到了证明. 盲短签名实现了对私钥份额的一次性加密, 而所用的一次性加密密钥仅由合法的接受方所拥有. 在请求私钥份额时, 响应节点对请求节点的身份进行认证, 确认其身份合法后才把与之对应的部分私钥份额发送给它, 这一点实现了密钥的认证性.

新节点主密钥份额的产生算法, 不仅能实现新节点主密钥份额的分布式生成, 而且使用随机数 r 加密子份额的方法保证了 u_{p_i} 的秘密份额 s_i 不被泄漏. 该算法中在点对点传输时可方便的利用节点的公/私钥来建立安全信道以保证消息的机密性. 且此算法通过加入验证功能, 有效防止了在传输过程中对消息的各种攻击.

由此可见, 此方案可满足密钥的各种安全需求, 其良好的分布式产生特点也充分体现出了无线 Ad hoc 网络的动态性要求.

4 结束语

本文提出了一个用于无线 Ad hoc 网络的基于身份的密钥管理方案, 包括主密钥生成、节点私钥生成、

新节点主密钥份额生成 3 个操作. 和现有无线 Ad hoc 网络中的密钥管理方案相比, 它能提供更高的安全性, 同时保证相对较好的运行效率. 利用基于身份的密码体制可减少系统中的存储开销、通信量以及用户的计算代价; 采用可验证秘密分享技术有效地防范了节点的不诚实行为; 同时利用盲短签名实现了私钥份额在公开信道的安全传输; 为新节点分配系统主密钥份额的算法能使所有网络节点共同分享主密钥承担 KGC 的职责. 与目前已有的其他方案相比, 新方案能更好的适应无线 Ad hoc 网络动态变化、缺乏可信中心、网络资源紧张等特点, 为节点间的安全通信奠定了牢固的基础.

[参考文献] (References)

- [1] SHAMIR A. Identity-based cryptosystems and signature schemes[C] // Proc of Cryptology-Crypto 84 CA: Springer-Verlag 1984: 47- 53.
- [2] KHALILIA, KATZ J. Toward secure key distribution in truly Ad-Hoc networks[C] // Proc of The Symposium on Applications and the Internet Workshops Berlin: Springer-Verlag 2003: 342- 346.
- [3] DENG H, MUKHERJEE A, AGRAWAL D P. Threshold and identity-based key management and authentication for wireless Ad-Hoc networks[C] // Proc of IEEE International Conferences on Information Technology (ITCC04). 2004: 107- 110.
- [4] PEDERSEN T. A threshold cryptosystem without a trusted party[J]. Computer Science Berlin: Springer-Verlag 1991: 547 (10): 522- 526.
- [5] FELDMAN P. A practical scheme for non-interactive verifiable secret sharing[C] // Proc of 28th IEEE Symposium on Foundations of Computer Science Berlin: Springer-Verlag 1987: 427- 437.
- [6] SUIT A, SHERMAN SM, LUCAS CK, et al. Secure and anonymous identity-based key Issuing without secure channel[EB/OL]. <http://eprint.iacr.org> November 2004 (20- 11- 2004) [30- 11- 2004].
- [7] BONEH D, FRANKLIN M. Identity-based encryption from the weil pairing[C] // Proc of Crypto 2001 CA: Springer-Verlag 2001: 213- 229.
- [8] HESS F. Exponent group signature schemes and efficient identity based signature schemes based on pairing [EB/OL]. <http://eprint.iacr.org> 2002 (4- 1- 2002) [22- 1- 2002].
- [9] PATERSON K. ID-based signatures from pairing on elliptic curves[EB/OL]. <http://eprint.iacr.org> 2002.
- [10] SHAMIR A. How to share a secret[J]. ACM Communications 1979 22(11): 612- 613.
- [11] PEDERSEN T. Non-interactive and information-theoretic secure verifiable secret sharing[C] // Proc of CRYPTO' 91. Berlin: Springer-Verlag 1991: 129- 139.
- [12] BONEH D, LYNN B, SHACHAM H. Short signatures from the weil pairing[C] // Proc of Cryptology-A siacrypt 2001. Berlin: Springer-Verlag 2001: 514- 532.
- [13] BOLDYREVA A. Efficient threshold signature, multisignature, and blind signature schemes based on the gap diffie-hellman group signature scheme[C] // Public Key cryptography Berlin: Springer-Verlag 2003: 278- 282.
- [14] GENNARO R, JARECKI S, KRAWCZYK H. Secure distributed key generation for discrete-log based cryptosystems[C] // EUROCRYPT' 99 Berlin: Springer-Verlag 1999: 295- 310.

[责任编辑: 刘 健]