基于身份加密的无线传感器网络密钥分配方法

杨 庚[1,2],王江涛[2],程宏兵[2],容淳铭[3]
(1. 南京邮电大学数理学院,江苏南京 210003;2. 南京邮电大学计算机学院,江苏南京 210003;
3. Department of Electrical and Computer Engineering, University of Stavanger, N-4036, Norway)

摘 要: 由于无线传感器网络在电源、计算能力和内存容量等方面的局限性,传统的网络密钥分配和管理方法已不适用. 本文从基于身份密钥体系出发,提出了一种适用于无线传感器网络的密钥预分配方法. 首先简要介绍了身份密钥体系,特别是 Boneh-Franklin 算法,然后基于身份密钥系统和 Diffie-Hellman 算法,给出我们的密钥分配方法,并从方法的复杂性、安全性、健壮性和内存需求等方面,与随机算法等进行了分析比较,结果表明我们的算法在这些方面有一定的优势. 最后我们讨论了可进一步研究的内容.

关键词: 基于身份标识密钥系统; 网络安全; Diffie-Hellman 算法; 无线传感器网络
中图分类号: TP393 **文献标识码**: A **文章编号**: 0372-2112 (2007) 01-0180-05

A Key Establish Scheme for WSN Based on IBE and Diffie-Hellman Algorithms

YANG Geng[1,2], WANG Jiang-tao[2], CHENG Hong-bing[2], RONG Chun-ming[3]
(1. *College of Mathematics & Physics, Nanjing University of Posts & Telecommunications, Nanjing, Jiangsu* 210003, *China*;
2. *College of Computer, Nanjing University of Posts & Telecommunications, Nanjing, Jiangsu* 210003, *China*;
3. *Department of Electrical and Computer Engineering, University of Stavanger, N*-4036, *Norway*)

Abstract: It is an important challenge to find out a suitable key establishment scheme for wireless sensor networks due to limitations of power, computation capability and storage resources. Many schemes based on random predistrubution technique and public key cryptography are investigated. Recently, a practical identity-based encryption technique is proposed. This paper presents an identity-based key establishment scheme for key predistribution and exchange in wireless sensor networks. It reviews first the identity-based encryption, particularly, the Boneh-Franklin algorithms. It describes a novel key establishment scheme based on the basic Boneh-Franklin and Diffie-Hellman algorithms. It discusses the efficiency and security of our scheme by comparing with random key assignment technique and symmetric key technique.

Key words: identity-based cryptography; network security; Diffie-Hellman key exchange; wireless sensor network

1 引言

近几年来无线传感器网络(Wireless Sensor Network, WSN)研究引起了人们的极大关注. 它可以应用在众多的工程领域,如军事、环境和安全监视、设备跟踪等等. 无线传感器网络通常由大量的可自控的节点组成. 每个节点由电池作为能源,并集成了数字信号处理器和射频电路. 与传统的无线计算机网络相比,传感器网络有其自身的特点. 这就是依靠电池能源、计算能力较弱、存储量小等. 由于这些局限性使传感器网络的研究面临与传统网络众多不同的挑战,如密钥管理、认证、路由、抗干扰、抗 DoS 攻击等. 而安全始终是人们关注的问题,特别是对一些重要场合的应用,安全性就显得尤为重要. 为了建立一个安全可靠的传感器网络,就必须有安全的算法和协议来完成网络密钥的设置管理和数据加密,传统的方法已不适应传感器网络,因为在传感器网络中没有认证中心,通信双方是对等的,而且计算与存储能力较弱. 为此,人们在密钥的分配和管理方面进行了广泛的研究[1~5],特别是在传感器网络的广播算法和密钥分配方面进行了探索,到目前为止,结果并不令人满意.

首先在密钥分配方面,我们知道,由于节点在传感器网络的位置往往是随机的,这就为节点间通信密钥的分配带来了巨大的挑战. 在网络生成阶段,所有的节点必须获取相邻节点的信息及网络拓扑结构. 一个简单的密钥分配方法就是让所有的节点事先都存储一个相同的对称密钥,通信双方都用这个密钥进行通信. 但这种方法缺点是一旦一个节点被攻破,全网就被攻破,通信就不安全. 尽管我们可以采用硬件手段存储这个密钥,增强其安全性,但研究结果表明成本和电源消耗太大,而且安全性也不一定得到保证[6]. 一个相应的改进方法是

收稿日期:2005-12-14;修回日期:2006-06-20
基金项目:江苏省自然科学基金重点预研项目(No. BK2004218);江苏省"青蓝工程"基金(No. KZ0040704006);南京邮电大学"攀登计划"基金(No. 05KJD520144);江苏省"六大人才高峰"基金(No. 06-E-044)

在网络拓扑形成后,通信双方立刻用存储的密钥交换新的密钥,从而形成各自不相同的对称密钥,并消除开始的公共密钥,这个方法的最大缺点是无法加入或移动节点,即网络的拓扑是不能变化的.因此这两种方都不具有实用化.

与上面方法对应的另一个极端是在每个节点都存储 $N-1$ 个密钥(N 是网络的节点数).这样能够保证一个节点与另一个节点的通信密钥不一样,增强了网络的健壮性(Resilience).但由于传感器节点的存储能力有限,且节点数往往较大,所以,这种方法同样也不实用.

近来 Eschenauer 和 Cligor 提出了一种基于概率的密钥分配方法[7].在此基础上 Pietro 等给出了一种随机密钥预分配方法[8].其思路概括为从一个选定的密钥空间中随机取出一密钥子空间,对每个传感器,再从这子空间中随机取出一组密钥,并存入传感器节点.在网络拓扑结构形成后,每个节点与它相邻的节点通信,找出它们共有的密钥,并作为以后通信加密的密钥.这种方法的缺点是不能完全保证每对通信双方都能找出共有的密钥,只能在某概率 p 的条件下可找到共有的密钥.基于这种方法,文献[9]进行了改进,提出了 q-composite 方法,它使得通信双方能够共有 q 个密钥,从而增强了网络的健壮性.研究结果表明改变 q 的值可以使网络被破坏的可能性限定在一定范围之内.

上面讨论的方法中都是针对对称密钥的分配问题.与非对称密钥相比,对称密钥的最大优点是计算量小.但是其明显的缺点是必须有一个密钥预分配过程,即事先将对称密钥存储在节点中,对增加和替换节点就显得不够灵活.人们一直在试图寻求非对称密钥系统在无线传感器网络中的应用[10,11].

基于身份标识的加密算法(Identity-Based Encryption,IBE)由 Shamir 于 1984 年首先提出[12].这种加密算法的基本思想是公钥可以是任何唯一的字符串,如 e-mail 地址、身份证或其他标识,它的优点是公钥是可识别的,不需要通常 PKI 系统的证书发放,同是可以以椭圆曲线形式实现该算法.尽管在 Shamir 之后人们提出了多种实现技术,但直到 2001 年 Boneh 和 Franklin[13]的论文才给出了一个可实际应用的实现方法,随后,人们根据不同的应用方向,提出了一些基于身份标识的加密算法[14,15].

由于身份标识加密算法是椭圆曲线类型的算法,前面的讨论启发我们去探讨其在无线传感器网络中的应用.因此,本论文的目的就是针对无线传感器网络,研究基于身份标识加密算法的密钥预分配方法.论文将首先简要介绍 IBE 算法的思想,然后提出一种进行密钥预分配的方法,同时从内存需求、算法复杂性和安全等方面分析了方法的性能,最后讨论了可进一步研究的工作.

2　IBE 算法

IBE 算法的主要特征是加密用的公钥不是从公钥证书中获取,而是直接使用标识用户身份的字符串.目前可实用的 IBE 方案由 Boneh 等在 2001 年提出,下面简要叙述文献[13]中的 IBE 方案.记负责生成并传送用户私钥的可信第三方记为 PKG(Private Key Generator).

A. 安全假设

IBE 加密方案的安全性建立在 CDH(Computational Diffie-Hellman)困难问题的一个变形之上,称之为 BDH(Bilinear-Diffie-Hellman)问题.IBE 的核心是使用了超奇异椭圆曲线上的一个双线性映射(Weil pairing).我们记 Zq 为素数阶 q 的加法群,$Zq=\{0,\cdots,q-1\}$,Z^+ 为正整数.

(1) 设 p 是一个大的素数,$p\equiv 2 \bmod 3$,并且存在大素数 q 使得 $p=6q-1$;

(2) $E/GF(p)$ 是在 $GF(p)$ 上构造的椭圆曲线:$y^2=x^3+1$,P 是该曲线上阶为 q 的一个点,由 P 生成的循环群记为 G;

(3) BDH 问题:对随机 $a,b,c\in Z_p^*$,已知 (P,aP,bP,cP) 来计算 $\hat{e}(P,P)^{abc}\in GF(p^2)$.其中 $\hat{e}:G\times G\to GF(p^2)$ 是一具有下列性质的映射:

①双线性性:如果对所有的 $x,y\in G$,$a,b\in Z$,都有 $\hat{e}(x^a,y^b)=\hat{e}(x,y)^{ab}$,则映射 $\hat{e}$ 称为一个双线性映射.

②非退化性:存在 $P,Q\in G$,使得 $\hat{e}(P,Q)\neq 1$.

③可计算性:有一个多项式时间算法来计算 $\hat{e}(P,Q)$.

B. Boneh-Franklin 算法

基本的 Boneh-Franklin IBE 算法主要由四个函数组成:Setup,Extract,Encrypt 和 Decrypt 分别完成系统参数建立、密钥提取、加密和解密的功能.

算法 1:基本 Boneh-Franklin(BBF)算法

(1) Setup:

Step1:PKG 选择 k 比特长的素数 p,找一条满足 WDH 安全假设的超奇异椭圆曲线 $E/GF(p)$,生成 $E/GF(p)$ 上的 q 阶子群 G 和 G 的生成元 P,以及双线性映射 $\hat{e}:G\times G\to GF(p^2)^*$.

Setp2:PKG 随机取 $s\in Z_q^*$,计算 $P_{pub}=sP$.

Step3:选择散列函数 $H_1:\{0,1\}^*\to E/GF(p)$,$H_2:GF(p^2)\to\{0,1\}^n$.明文空间为 $M=\{0,1\}^n$,密文空间为 $C=E/GF(p)\times\{0,1\}^n$,输出的系统公共参数为 $\pi=\{q,p,\hat{e},n,P,P_{pub},H_1,H_2\}$,$s\in Z_q^*$ 为主密钥(Master key).

(2) Extract:对给定的字符串 $Id\in\{0,1\}^*$,生成密钥.

Step4:计算 $Q_{Id}=H_1(Id)\in E/GF(p)$.

Step5:取密钥为 $KId=(Q_{Id})^s$.

(3) Encrypt:对原文 $m\in M$ 和公钥 Id,加密步骤如下.

Step6:计算 $Q_{Id}=H_1(Id)\in E/GF(p)$.

Step7:随机取 $r\in Z_q^*$,加密的密文为:

$$c=\langle rP,m\oplus H_2(g_{Id}^r)\rangle$$

其中 $g_{Id}=\hat{e}(Q_{Id},P_{pub})\in GF(p^2)$.

(4) Decrypt:设 $c=\langle U,V\rangle$ 为密文,解密步骤为:

Step8:应用密钥 $K_{Id}(E/GF(p))$,计算原文

$$m=V\oplus H_2(\hat{e}(K_{Id},U))$$

IBE 加密算法的安全性建立在 Diffie-Hellman 问题复杂性基础上.研究结果表明 BBF 算法是单向身份加密算法(one-way identity-based encryption scheme,ID-OWE),详细的结论参见文献[14].

3 一种新的密钥预分配方法

基于 Boneh-Franklin 算法,本节我们给出一种可应用于无线传感器网络的对称密钥预分配方法. 方法的基本思想是应用 IBE 算法进行公共参数的交换,应用 Diffie-Hellman 算法计算对称密钥,再应用该对称密钥进行正常的数据通信. 为了便于算法的描述,我们先给出方法的一般形式,然后在定义其具体的计算方法.

A. 方法的一般形式

算法的一般形式包含了 7 个阶段,分别完成相应的功能. 具体定义如下.

算法 2:方法的一般形式

(*a*) 初始化过程:计算所有 IBE 算法中的参数和 Diffie-Hellman 密钥交换算法中的参数,并存入每个节点.

(*b*) 广播过程:将传感器节点标识 *Id* 广播给相邻的节点.

(*c*) 公共参数计算过程:所有节点计算 Diffie-Hellman 密钥交换算法中的参数.

(*d*) 公共参数交换过程:应用 Boneh-Franklin 算法在两个节点中交换参数.

(*e*) 密钥计算过程:根据交换的参数,应用 Diffie-Hellman 算法计算对称密钥.

(*f*) 加密解密过程:应用该对称密钥和对称加密算法(如 DES)进行数据的加密和解密.

本方法的最大优点是用非对称系统进行参数交换,用对称系统进行通信的数据加密,充分利用了两者的优点. 同时不存储多余的密钥,对内存需求小. 采用 IBE 算法交换参数,简单安全,不需要认证过程. 详细的分析将在后面讨论.

B. 方法的详细描述

在详细分析之前,我们先讨论一下无线传感器网络节点的初始化过程. 在无线传感器中,由于没有类似于服务器的主节点等特殊性,必须在节点拓扑生成之前做一个初始化过程,其目的是将有关信息分配到节点,并存储到节点中. 这个过程可以由两种方式完成. 一是在构造传感器网络时,利用一个类似基站的节点向所有节点广播参数,包括应用于 IBE 的公共参数 π 等,一旦参数被广播节点后,基站就消失,节点依靠自身的计算能力生成网络拓扑及密钥对;另一个是在节点系统生成阶段,将有关的参数存入节点,就象网卡的 MAC 地址一样,而不是在现场广播,可以利用一个管理系统,对节点进行初始化. 对基于 IBE 的密钥管理方法后者更具有优越性. 我们可以以传感器网络的使用范围进行节点的管理,如某部队、某消防队等. 他们的节点管理系统完成对节点的初始化,然后供现场使用. 主密钥 s 只存在管理系统中,使密钥系统更为安全. 若需增加新节点,就用管理系统对其进行初始化,这样能很好地解决新增节点和替换节点的问题.

下面我们给出对应于算法 2 的详细描述,即算法 3.

算法 3:方法的详细描述

(1) 初始化过程:

(*a*) 运行 BBF 算法中的 Setup 函数,得到所有 IBE 算法中的参数 π 和主密钥 s.

(*b*) 运行 BBF 算法中的 Extract 函数,得到与节点 *Id* 相对应的密钥.

(*c*) 应用上面讨论的两种方法将参数 π,以及密钥分配到相应的节点,完成节点的初始化过程.

(2) 广播过程:

我们有两种选择:

(*a*) 一节点 *A* 向相邻节点显式广播自己的身份标识 Id_A,所有相邻节点获取节点 *A* 的标识 Id_A.

(*b*) 节点 *A* 应用算法 1 的 BBF 方法加密 Id_A,算法中的标识为一特殊的广播地址标识,就像 TCP/IP 协议中的广播地址一样,所有的相邻节点解密后得到节点 *A* 的标识 Id_A,当然,对应于广播地址的加密和解密密钥必须在初始化过程中存入节点内存.

(3) 公共参数计算过程:

对每个相邻节点(记为 *B*),做:

(*a*) *A* 计算参数 Y_A 如下:

选取 $X_A < q$.

计算参数 $Y_A = \eta^{X_A} \bmod q$.

(*b*) *B* 计算参数 Y_B 如下:

选取 $X_B < q$.

计算参数 $Y_B = \eta^{X_B} \bmod q$.

(4) 公共参数交换过程:

对每个相邻节点(记为 *B*),做:

(*a*) *B* 节点应用 Encrypt 函数对数据 Y_B, Id_B 和 Id_A 进行加密,并发送给 *A*.

(*b*) *A* 节点应用 Decrypt 函数进行数据解密,获取 Y_B 和 Id_B.

(*c*) 相应地,*A* 节点应用 Encrypt 函数对数据 Y_A, Id_B 和 Id_A 进行加密,并发送给 *B*.

(*d*) *B* 节点应用 Decrypt 函数进行数据解密,获取 Y_A.

(5) 密钥计算过程:

(*a*) *A* 计算并保存密钥 $K = (Y_B)^{X_A} \bmod q$,

(*b*) *B* 计算并保存密钥 $K = (Y_A)^{X_B} \bmod q$.

(6) 加密解密过程:

通信双方应用对称密钥 K 进行加密解密,如应用 DES 算法. 算法的交互过程如图 1 所示.

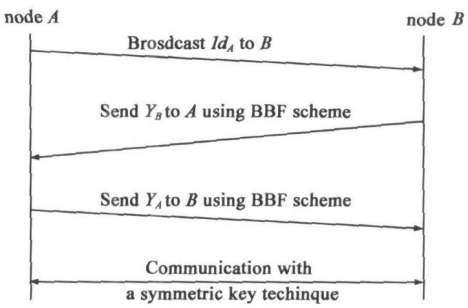

图 1 密钥预分配方法序图

4 方法性能分析

本节将通过与其他密钥预分配和加密算法的比较,分析

我们提出的方法的效益和安全性,主要讨论方法的内存需求、复杂性和安全性.

A. 效益分析

(1) 内存开销

我们知道,对无线传感器网络中的节点,理想的内存需求是仅仅存储与相邻节点的密钥. 在我们的方法中,每个节点需要保存的信息有在 IBE 算法用到的参数 π,以及与相邻节点的密钥,与理想的内存开销相比,仅仅多了公共参数,与所有的存储密钥内存开销相比,这一部分是相对小的,因此,在内存开销方面,我们的方法达到了一定的层次.

(2) 复杂性

在我们的方法中,使用 IBE 算法进行对称密钥的交换,尽管这是一个非对称的密钥系统,但只在网络拓扑形成时的密钥分配与建立过程中执行一次,除非有新的节点加入或节点进行了移动. 一旦一个节点与它相邻节点的密钥建立起来后,后面的通信数据加密都是采用对称密钥系统. 同时必须注意到研究结果表明椭圆曲线类型的算法在复杂性和安全性方面有一定的优势[16,17],密钥长度分别为 160-bit 和 224-bit 的椭圆曲线算法,与 RAS-1024 和 RSA-2048 的安全性相当. 因此,椭圆曲线类型的算法比通常的非对称密钥系统的计算成本要低.

事实上,算法主要需要进行两个散列函数的计算、一个 XOR 运算、一个双线性映射等(见表 1).

表 1　计算复杂性

	基本 Boneh-Franklin 算法	
	加密过程	解密过程
e 运算	1	1
哈希运算	2	1
XOR 运算	1	1
乘法运算	1	0
指数运算	1	0

(3) 与随机密钥预分配方法的比较

随机密钥预分配方法包含两个部分:密钥预分配过程和密钥发现过程. 密钥预分配过程将从一个选定的密钥空间中随机取出一密钥子空间,每个传感器存储一组从这子空间中随机取出的密钥. 研究结果表明每对相邻节点共享密钥数是密钥子空间维数和节点密钥数的函数. 对维数 1000 的密钥子空间,每个节点存储 50 个密钥,则存在共享密钥的概率是 0.9[5]. 密钥发现过程中,哈希函数运算、XOR 运算和节点间的通信都是必须的,而通信对能量的消耗是较大的. 同时,当新增加节点时随机密钥预分配方法必须重新执行密钥发现过程. 因此,与我们的方法相比,算法的复杂性处于同一层次,但我们的方法在新增节点处理上要优于随机密钥预分配方法.

B. 安全性分析

(1) 健壮性

在我们的算法中,生成的每对对称密钥都不相同,只有进行通信的双方拥有这对密钥. 在建立密钥的过程中采用 Diffie-Hellman 算法计算对称密钥,因此,即使交换的公共参数被攻击者获取,他也无法计算出密钥. 由于每对节点的密钥不同,当一个节点被破获后,牵涉不到其他节点的安全,更影响不到全网的安全. 这样保证了网络的强健壮性.

而在随机算法中[8,9],网络的健壮性被描述为一个概率问题,如在 *q*-composite 随机预分配算法中,在节点被破获后,其他节点不被破获的概率是 $(1-m/S)^x$,其中 x 是被破获的节点数、m 是节点中存储的密钥总数、S 是密钥子空间的维数. 这就需要 S 充分大,m 尽量小,但 S 较大、或 m 较小都有可能导致相邻节点找不到共有的密钥,使它们之间的正常通信无法进行,这样的结果是非常严重的. 所以,人们一直希望具有更好的随机算法出现,但到目前为止,文[8,9]的结果目前是最好的.

另一方面,随机算法中所有节点的密钥都是从一个密钥子空间中选取的,尽管是随机选取,但不可避免会造成多对节点的密钥相同,特别是一般的无线传感器网络的节点树都比较大,密钥的重复可能性就更大,这就给网络的安全带来隐患. 在因此,在健壮性和安全性方面我们的方法比目前的随机算法更具有优越性.

(2) 参数交换协议安全

我们应用 IBE 算法进行参数的交换,这样做的优点之一是可以用节点的标识作为公钥,因此,不需要身份认证. 同时,利用 IBE 算法可以将加密和认证结合在一起,使算法更为有效和安全[16,18]. 再则,密钥的计算是通过 Diffie-Hellman 算法获得,而不是一直使用 IBE 算法,使后面的通信可以采用对称密钥算法实现,显示了我们方法的独到之处.

5　结论

无线传感器网络的研究和应用已引起了人们的高度重视,在军事和民用方面有着广泛的应用,相关的产品已经问世,我们开发的产品已应用于某监狱系统的监控. 在初期的体系结构相对完成后,就象当初 Internet 网络的发展过程一样,安全问题就显得越来越重要. 由于无线传感器网络与固定网络和一般的无线网络不同,有其自身的特征,这就为进行密钥的分配和管理提出了新的挑战.

对称密钥系统与非对称密钥系统相比,在计算复杂性方面有优势,但在密钥的管理和安全性方面有不足之处,非对称密钥系统一直被认为不适合无线传感器网络系统,但基于椭圆曲线的算法在计算复杂性方面已经有所改善,特别是 2001 年实用化的基于身份密钥系统的提出,为非对称密钥系统在无线传感器网络中的应用提供了可能. 本文正是将非对称与对称密钥系统有效地结合起来,进行密钥的分配与管理. 分析表明,与目前的随机类型算法相比,在内存需求、健壮性和安全性方面都有改进,已有的研究结果和我们的分析表明,在计算复杂性方面也是可接受的.

因此,作为下一步的工作,我们将应用无线传感器网络测试平台 TinyOS 和 TingPK[19],对我们提出的算法进行更深入的算法复杂性研究,从理论和应用角度,得到更详细的结果. 另一方面,寻求更有效适合于无线传感器网络的广播和组播算法也是一个很有意义的研究课题.

参考文献:

[1] Akyildiz I F, et al. Wireless sensor networks: a survey [J]. Computer Networks, 2002, 38(4): 393 - 422.

[2] Perrig A, et al. TESLA: multicast source authentication transform [EB/OL]. IRTF draft, ftp://ftp.rfc-editor.org/in-notes/rfc4082.txt, 2000-07-20.

[3] Perrig A, et al. SPINS: security protocols for sensor networks [J]. Wireless Networks, 2002, 8(7): 521 - 534.

[4] Liu D, Ning P, Li R. Establishing pairwise keys in distributed sensor networks [J]. ACM Transactions on Information and System Security, 2005, 8(1): 41 - 77.

[5] Du W, et al. A pairwise key predistribution scheme for wireless sensor networks [J]. ACM Transactions on Information and System Security, 2005, 8(2): 228 - 258.

[6] Anderson R, Kuhn M. Tamper resistance-a cautionary note [A]. Proceedings of the 2nd Usenix Workshop on Electronic Commerce [C]. Washington DC, USA: ACM Press, 1996. 1 - 11.

[7] Eschenauer L, Gligor V D. A key-management scheme for distributed sensor networks [A]. Proceedings of the 9th ACM Conference on Computer and Communications Security [C]. Washington DC, USA: ACM Press, 2002. 41 - 47.

[8] Pietro R D, Mancini L V, Andmei A. Random key assignment for secure wireless sensor networks [A]. ACM Workshop on Security in Ad Hoc and Sensor Networks (SASN '03) [C]. Washington DC, USA: ACM Press, 2003. 62 - 71.

[9] Chan H, et al. Random key predistribution schemes for sensor networks [A]. IEEE symposium on Research in Security and Privacy [C]. New York: IEEE publishing, 2003. 197 - 213.

[10] Gura N, et al. Elliptic curve cryptography and RSA on 8-bit CPUs [A]. Proceedings of the Workshop on Cryptography Hardware and Embedded Systems (CHES 2004) [C]. Berlin: Springer-Verlag, 2004. 11 - 13.

[11] Liu D, Ning P. Multi-level μTESLA: broadcast authentication for distributed sensor networks [J]. ACM Transactions in Embedded Computing Systems (TECS), 2004, 3(4): 800 - 836.

[12] Shamir A. Identity-based cryptography and signature schemes [A]. Advances in Cryptology, CRYPTO '84, Lecture Notes in Computer Science [C]. Berlin: Springer-Verlag, 1985, 196: 47 - 53.

[13] Boneh D, Franklin M. Identity-based encryption from the Weil pairing [A]. Advances in Cryptology, CRYPTO 2001, Lecture Notes in Computer Science [C]. Berlin: Springer-Verlag, 2001. 2139. 213 - 229.

[14] Boyen X. Multipurpose identity-based signcryption, a swiss army knife for identity-based cryptography [A]. Lecture Notes in Computer Science [C]. Berlin: Springer-Verlag, 2003. 2729. 383 - 399.

[15] Chen L, Kudla C. Identity-based authenticated key agreement protocols from pairings [EB/OL]. Cryptology ePrint Archive, http://eprint.iacr.org/2002/184, 2002-11-28.

[16] Wander A S, et al. Energy analysis of public-key cryptography for wireless sensor networks [A]. Proceedings of the 3rd Int'l Conf on Pervasive Computing and Communications [C]. New York: IEEE Publishing, 2005. 324 - 328.

[17] Lauter K. The advantages of elliptic curve cryptography for wireless security [J]. IEEE Wireless Communications, 2004, 11(1): 62 - 67.

[18] Lynn B. Authenticated identity-based encryption [EB/OL]. Cryptology ePrint Archive, http://eprint.iacr.org/2002/072, 2002-06-04.

[19] Watro R, et al. TinyPK: Securing sensor networks with public key technology [A]. Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks SASN '04 [C]. New York: ACM Press, 2004. 59 - 64.

作者简介:

杨 庚 1961 年生于江苏建湖, 1994 年加拿大 Laval 大学博士毕业, 1994 至 1996 在加拿大 Montreal 大学计算技术及其应用中心进行博士后工作, 先后在加拿大 ORTECH、Motorola 等公司任软件工程师和数据库专家, IEEE CE 和中国计算机学会会员. 现为南京邮电大学计算机学院教授、博士生导师. 目前研究方向为计算机通信与网络、网络安全、分布与并行计算等. E-mail: yangg@njupt.edu.cn

容淳铭 1969 年生于广州, 1993、1995 年和 1998 年在挪威 Bergen 大学获计算机科学学士、硕士和博士. 现为挪威 Stavanger 大学计算机与工程学院教授, 国际 International Journal of Mobile Communications (IJMC) 杂志编委, IEEE CE 和 ACM 会员. 目前的研究方向为计算机安全、密码学、电子商务、移动计算等.

王江涛 男, 1978 年生于安徽马鞍山, 南京邮电大学计算机学院博士研究生, 研究方向为信息安全, 计算机网络与通信.

程宏兵 男, 1979 年生于江西九江, 南京邮电大学计算机学院博士研究生, 研究方向为信息安全, 计算机网络与通信.