一个新的基于身份的无线传感器网络密钥协商方案

郭江鸿[1] 李兴华[2] 武坚强[1]
(广东嘉应学院计算机系 梅州 514015)[1]
(西安电子科技大学网络与信息安全教育部重点实验室 西安 710071)[2]

摘 要 无线信道具有开放性,节点间建立配对密钥是无线传感器网络安全通信的基础。在大部分基于身份加密(Identity-Based Encryption,IBE)的传感器网络密钥协商方案中,使用双线对运算建立配对密钥,能耗高且耗时长。基于BNN-IBS身份签名提出了一个新的无线传感器网络密钥协商方案,节点通过Diffie-Hellman协议建立配对密钥,所需的密钥参数通过广播获得。与基于IBE的传感器网络密钥协商方案(IBE-based Key Agreement Scheme,IBEKAS)进行量化比较,结果表明本方案不仅提供了与IBEKAS同层次的安全性与可扩展性,且在能耗与时耗方面具有较明显的优势。

关键词 无线传感器网络,密钥协商,身份签名
中图法分类号 TP309 **文献标识码** A

New Identity-based Key Agreement Scheme for WSN

GUO Jiang-hong[1] LI Xing-hua[2] WU Jian-qiang[1]
(Department of Computer Science, Jiaying University, Meizhou 514015, China)[1]
(Key Laboratory of Computer Networks and Information Security of Ministry of Education, Xidian University, Xi'an 710071, China)[2]

Abstract For the openness of wireless channel, establishing pairwise key between sensor nodes is the basis of the secure communication in wireless sensor networks. In most of existing IBE-based key agreement schemes, the pairwise key was established using Tate pairing with high energy consuming and time consuming. In this paper, authors proposed a key agreement scheme based on BNN-IBS signature, sensors broadcast the parameters required for establishing pairwise key and compute the key using Diffie-Hellman key exchange technology. Compared with the IBE-based key agreement scheme, the proposed scheme has patent advantages in energy consuming and time consuming with the same security and scalability.

Keywords Wireless sensor network, Key agreement, Identity-based signature

1 引言

随着传感器技术的发展,无线传感器网络(Wireless Sensor Network,WSN)的应用范围日益广泛。WSN由大量资源有限的传感器节点组成,通过无线链路进行通信。由于无线链路的开放性,敌手可能发动多种攻击。建立节点间的配对密钥是实现传感器网络安全通信的基础。由于传感器节点本身存储能力、计算能力、通信带宽、节点能量等资源有限,使得许多成功的传统网络中的密钥协商方法(如RSA等)不能直接应用。如何有效地建立WSN配对密钥,一直是研究热点。

WSN密钥协商方案主要有两种:基于密钥预分配的密钥协商方案及基于公钥系统的密钥协商方案。

基于密钥预分配的方案建立配对密钥的开销较小,引起了广泛关注并出现了诸多研究成果。Eschenauer和Gligor[1]提出了概率密钥共享方式;Blundo[2]使用对称多项式对E-G方案进行了改进,在一定程度上提高了抗毁性;Chan[3]等对E-G方案进行改进并提出q-composite方案;Liu[4]等结合部署知识提出了基于地理信息的密钥分配方案,一定程度上提高了网络的密钥连通率;Younis[5]在层次式WSN里提出了基于位置信息的EBS动态密钥管理方案,一定程度上提高了抗串谋攻击的能力,但簇头节点受损对网络安全威胁大。

但密钥预分配方案也存在一些不足:1)抗毁性差。节点妥协攻击对网络安全影响较大,妥协节点数目超过阈值将威胁到整个网络的安全;2)网络扩展性受限;3)预分配的密钥存在冗余,节点预装的密钥或密钥材料中只有一部分可用于与邻居节点建立配对密钥。

由于ECC以160bit的密钥达到了RSA中1024bit密钥的安全性,因此基于ECC的公钥加密成为WSN密钥协商方案的研究热点。特别是基于身份加密(Identity-Based Encryption,IBE[6])的密钥协商方案,由于节点公钥由公开信息直接推导,无须进行公钥认证,因此有效地降低了计算复杂度和通信开销。如杨庚等[7]与程宏兵等[8]用IBE建立传感器

到稿日期:2010-04-04 返修日期:2010-07-06 本文受国家自然科学基金(60702059)资助。
郭江鸿(1975—),男,硕士,讲师,主要研究方向为无线移动安全等,E-mail:g_jh@jyu.edu.cn;李兴华(1977—),男,博士,副教授,主要研究方向为网络与信息安全等;武坚强(1975—),男,讲师,主要研究方向为信息安全与图像处理等。

网络密钥协商方案，对密钥参数、发起方 ID、目的节点 ID 进行身份加密，防止中间人攻击，节点间通过解密得到参数并使用 DH 技术建立配对密钥。

但传统的 IBE 基于双线对运算，计算开销较大且计算时间较长，不适合于资源有限的传感器。因此，如何在利用身份加密优势的基础上有效地降低建立配对密钥的时间与能耗是一个极有意义的研究问题。

本文提出了一种基于 BNN-IBS 身份签名[9]的传感器网络密钥协商方案。分析表明，本文方案继承了身份加密的优点，具有高的连通率、安全性与可扩展性；同时，在建立配对密钥所需的时间与能耗方面都优于基于 IBE 的密钥协商方案。

本文第 2 节简介 BNN-IBS 签名及其变形方案 vBNN-IBS[10]；第 3 节给出 BNN-IBS-KS 方案；第 4 节对 BNN-IBS-KS 方案进行分析，并通过量化分析将其与基于 IBE 的密钥协商方案进行比较。

2 预备知识

2.1 BNN-IBS 简介

Bellar 等于 2004 年提出了基于椭圆曲线的 IBS 方案(BNN-IBS)，并对该方案的安全性做出了证明[9]。在 BNN-IBS 中，签名的生成与验证主要是通过椭圆曲线上的点乘来完成。BNN-IBS 方案具体如下：

给定安全参数为 k；选择有限域 Fq 上的椭圆曲线 E/F_q，以 $E(F_q)$表示 E/F_q 上的点构成的群，$E(F_q)$阶为 n；$P\in E(F_q)$且 P 的阶为 p，p 为素数且 p^2 不整除 n；$\langle G\rangle$为由 P 生成的群。

· 系统参数设定：

1)选取 $E(F_q)$，P，p，选取 $x\in_R Z_p$，x 为系统私钥；计算 $Q=xP$，Q 为系统公钥；

2)选取两个加密哈希函数 $H_1:\{0,1\}\times G_1^*\rightarrow Z_p$，$H_2:\{0,1\}^*\rightarrow Z_p$；

3)公布系统参数$\langle E/F_q,P,p,Q,H_1,H_2\rangle$。

· 用户密钥生成：给定用户 ID 为 ID_u，$ID_u\in\{0,1\}^*$，则其私钥 SK_u 按以下步骤生成：

1) 选取 $r\in_R Z_p$，计算 $R=rP$；

2) 利用系统密钥 x 计算 $s=r+cx$，$c=H_1(ID_u||R)$；

用户 ID_u 的私钥 $SK_u=(R,s)$。

· 签名：用户 ID_u 对消息 m 的签名如下：

1)选取 $y\in_R Z_p$，计算 $Y=yP$；

2)计算 $z=y+hs$，其中 $h=H_2(ID_u,m,R,Y)$；

用户 ID_u 对消息 m 的签名为$\langle R,Y,z\rangle$。

· 签名验证：

给定用户 ID_u、系统参数、消息 m 及签名$\langle R,Y,z\rangle$，验证过程如下：

1) 计算 $h=H_2(ID_u,m,R,Y)$，$c=H_1(ID_u||R)$；

2) 检查 $zP=Y+h(R+cQ)$是否成立。

若 2)验证通过，则接收消息，否则丢弃。

2.2 vBNN-IBS 简介

为取得与 RSA1024 相同的安全性，BNN-IBS 中的参数 p，q 分别为 168bit 与 166bit，签名长度为 105B[9]。为减少签名长度，采用一个变形的 BNN-IBS 签名方案 vBNN-IBS。该方案与 BNN-IBS 具有相同的安全性及计算复杂度，但消息签名缩减为 83B[10]。其签名过程如下：

1)选取 $y\in_R Z_p$，计算 $Y=yP$；

2)计算 $z=y+hs$，其中 $h=H_2(ID_u,m,R,Y)$；

用户 ID_u 对消息 m 的签名为$\langle R,h,z\rangle$。

签名验证：给定用户 ID_u、系统参数、消息 m 及签名$\langle R,h,z\rangle$，验证如下：

1) 计算 $c=H_1(ID_u||R)$；

2) 检查 $h=H_2(ID_u,m,R,zP-h(R+cQ))$是否成立。

3 本文方案简介

本文方案使用 BNN-IBS 的变形方案 vBNN-IBS，对用于建立配对密钥的参数进行签名广播，邻居节点间进行签名验证以确定消息来源；邻居节点间从消息中提取参数，并使用 D-H(Diffie-Hellman)密钥交换技术建立配对密钥。vBNN-IBS 签名与 BNN-IBS 签名具有相同的安全性[10]，伪造合法签名的难度等同于求解椭圆曲线离散对数问题(ECDLP)。本文方案具体如下：

1) 密钥材料预分配：部署服务器，按照第 2.1 节所述，生成系统参数$\langle E/F_q,P,p,Q,H_1,H_2\rangle$，为每个节点分配 ID，并根据其 ID 生成相应的私钥$\langle R,s\rangle$，同时按以下方法为每个节点计算用于 DH 密钥交换的参数：取 $x<p$，计算 $y=g^x \bmod p$；p，g 为公开参数。服务器将上述密钥材料装入传感器节点。

2) 消息广播：部署后，对任一节点 A 按照 vBNN-IBS 的方法为其用于密钥交换的参数进行身份签名，并按照消息(I)的格式进行广播：

$$\langle ID_A,y_A,Sig\{ID_A,y_A\}\rangle \qquad (\mathrm{I})$$

式中，设$|y_A|=20\text{byte}$，$|ID_A|=2\text{byte}$。

3) 参数提取：设 B 为 A 的邻居节点，则 B 按照第 2.2 节中的验证步骤对消息进行签名验证，确定消息源的正确性，并提取消息中的密钥交换参数 y_A。

4) 配对密钥建立：A 与 B 分别如下计算配对密钥：

· A 计算：$K_{AB}=(y_B)^{x_A}=(g^{x_B})^{x_A}=(g)^{x_Bx_A}$；

· B 计算：$K_{BA}=(y_A)^{x_B}=(g^{x_A})^{x_B}=(g)^{x_Ax_B}$。

5) A，B 间通过建立的对称密钥进行消息的加解密。

4 本文方案性能分析

本节对本文方案进行性能分析，并与基于 IBE 的密钥协商方案进行开销对比(两种方案都基于身份加密，其连通率、可扩展性、抗毁性处于同一层次)。

4.1 连通率分析

由本文方案简介可知，邻居节点间通过验证带有签名的广播消息，确定消息源并提取消息中 D-H 协议中的密钥参数便可建立配对密钥，密钥连通率为 1，网络连通率也为 1。而各种随机密钥预分配方案由于密钥分配的随机性及节点部署的随机性而很难达到高的密钥连通率，如 E-G 方案中以 30% 的密钥连通率只达到了接近 1 的网络连通率。

4.2 可扩展性分析

新节点预装入身份签名的系统参数、D-H 协议的公开参数以及节点私钥，部署后可通过广播与邻居节点进行参数交互，以概率 1 与所有的邻居节点建立配对密钥，不会影响连通率，可扩展性好。而对于随机密钥预分配方案而言，新节点中

包含的密钥或密钥材料并不足以保证与所有的邻居节点建立配对密钥，大部分随机密钥预分配方案（如 Blundo[2] 的方案）的可扩展性一般。

4.3 安全性分析

在大部分随机密钥预分配方案中，妥协节点的数目直接影响到网络的安全性。妥协节点超过一定阈值时，整个网络的安全将受到威胁。如文献[6]中指出，在其方案下，当妥协节点数目超过 60%时，整个网络的安全性将得不到保障。

对于本文方案，不论妥协节点数目为多少，敌手都很难得到未妥协节点的秘密信息。这是因为公开信息是 BNN-IBS 及 D-H 协议的系统参数、通过 D-H 协议进行密钥协商所需要的参数以及节点 ID，敌手想通过公开信息获得未妥协节点私钥$\langle R,s\rangle$，其难度等同于解决 ECC 上的离散对数问题（EC-DLP）；而敌手想通过公开的密钥交换参数 y_A 得到节点的秘密参数 x_A，其难度等同于解决离散对数问题；同时，本文方案中通过身份签名有效地抵抗了中间人攻击。因此，妥协节点数目对本文方案的安全性不构成威胁，本文方案抗毁性好、安全性高。

4.4 开销分析

本节主要讨论本文方案的开销，并与文献[7]中基于 IBE 的传感器网络密钥协商方案（IBEKAS）做比较。后者使用 Boneh 等在 2001 年利用双线对提出的 IBE 方案[6]对密钥参数进行加解密，邻居间通过解密密文确定通信方身份，提取密钥参数并计算配对密钥。交互过程如图 1 所示。

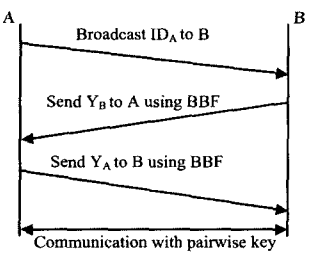

图 1 IBEAS 配对密钥建立过程

节点发送的消息格式为：

$$Id_B, ENC_{K_B}(Id_B, Id_A, y_B) \qquad (\text{Ⅱ})$$

式中，y_B 为的密钥参数，K_B 表示 B 的私钥。

同时，由于对 IBE 的相关研究已经很多，并取得了诸多成果，因此本文不再对 IBE 进行介绍，具体可参见文献[6]。方案的开销分析具体如下。

1）存储开销

两种方案中均要求节点预装系统参数、用于建立配对密钥的密钥参数及节点 ID。经过与邻居节点的通信及计算，均可以得到相应的配对密钥并存储。从这个方面来看，两种方案的存储开销处于同一层次。在随机密钥预分配方案中，由于密钥分配的随机性及节点部署的随机性，节点存储的部分密钥或密钥材料并不能用于同邻居节点建立配对密钥，密钥有冗余，对存储空间的利用不够理想。

2）通信开销

因为配对密钥根据密钥参数由节点计算生成，通信开销主要指节点间交换密钥参数所需的通信量。设两种方案采用消息封装格式为 32byte 载荷、9byte 包头及 8byte 前缀，在前缀中包含了源方、目的方、长度、包序号、CRC 及控制字节。IBEKAS 中的安全参数长度为 160bit（ECC-160），每个节点有 N 个邻居节点。

本文方案签名长度为 83byte，消息（I）的长度为 83+20+2=105byte，封装后的数据长度为：32 * 3+9+17 * 4=173byte。为了与邻居节点交换密钥参数，每个节点进行一次广播并接收 N 个邻居广播。

IBEKAS 密文长度为 60byte，消息（II）的长度为 60+2=62byte。封装后的消息长度为 32+30+17 * 2= 96byte。每个节点为获得一个邻居的密钥参数，需进行一次消息发送及一次消息接收；与 N 个邻居建立配对密钥，需发送 N 个消息并接收 N 个来自邻居的密文。

两种方案的通信量对比如表 1 所列。

表 1 通信量对比

方案	发送(byte)	接收(byte)
本文方案	173	173 * N
IBEKAS	96 * N	96 * N

MICA2 节点发送与接收一个字节的能耗分别为 59.2μJ，28.6μJ[11]，则两种方案的通信能耗如图 2 所示。

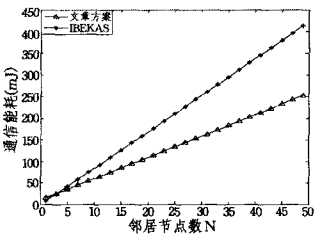

图 2 通信能耗

由图 2 可知，当邻居节点数为 40 时，为与所有邻居节点建立配对密钥，本文方案所需的通信能耗约为 208mJ；IBEKAS 能耗约为 337mJ，虽然其消息长度短，但使用加密方式确定通信方身份的方法会带来较多的通信次数，造成高的通信能耗。

3）计算开销

由于两种方案都是通过交换 D-H 密钥参数的方法建立配对密钥，因此主要的计算开销区别在于交换密钥参数需要的计算量。我们先对两种方案的计算复杂性进行分析（不考虑普通的加法与乘法），如表 2 所列。

表 2 计算复杂性分析

运算类型	文章方案		IBEKAS	
	签名	验证	加密	解密
双线对			1	1
哈希	1	2	2	1
点乘(ECC)	1	3	1	
点加(ECC)		2		
异或			1	1
指数			1	

为简化分析，我们以双线对运算及 ECC 上的点乘运算所消耗的能量衡量计算开销。根据 Gura 等的研究[11]，在 MICA2 传感器上（8bit，ATmega128L，8MHz，电压 3V，活动状态电流 8mAh）[12]，进行一次 ECC 点乘需 0.81s，能耗约为 0.81s * 3V * 8mAh=19.44mJ；根据 Bertoni 等的研究[13]，在 32bit，33MHz 的 ST22 智能卡处理器上，进行一次双线对运算约为 0.752s，则可估算在 MICA2 传感器上进行双线对运算的时间为 0.752 * 33/8=3.102s，能耗为 3.102s * 3V * 8mAh=74.45mJ。两种方案中节点与 N 个邻居节点交换密

钥参数所需要的计算时间及能耗如表 3 所列。

表 3　计算时间及能耗分析

方案	时间(s)	能耗(mJ)
本文方案	0.81 * (3N+1)	19.44 * (3N+1)
IBEKAS	(0.81+3.102 * 2) * N	(19.44+2 * 74.45) * N

不同邻居数目下两种方案的计算时间与计算能耗如图 3(a)、图 3(b)所示。

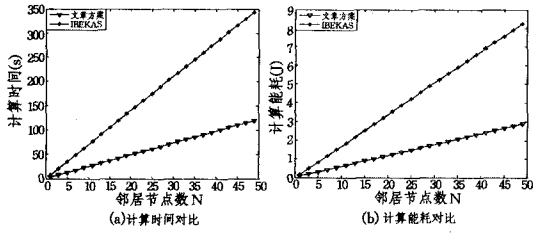

图 3　计算时间及计算能耗

由图 3 可看出，本文方案的计算时间与计算能耗较优，原因在于使用 ECC 上的点乘运算对消息进行签名与认证，$N=40$ 时，时间/能耗为 98s/2.35J；IBEKAS 基于双线对运算，$N=40$时，时间/能耗为 280s/6.734J，开销是本文方案的近 3 倍。

4) 综合能耗分析

通过对两种方案的通信开销及计算开销的分析，我们得到一个节点为与其 N 个邻居建立配对密钥，两种方案所需的综合能耗 E(设 E_T，E_C 分别为通信能耗与计算能耗)如下。

本文方案：$E=E_C+E_T=29.68+63.26*N$(mJ)

IBEKS：$E=E_C+E_T=176.77*N$(mJ)

两种方案的综合能耗对比如图 4 所示。

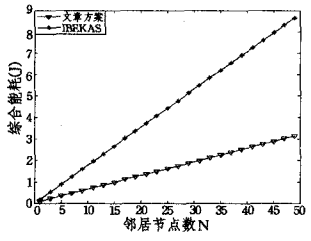

图 4　综合能耗分析

从图 4 可看出，本文方案的综合能耗较优，一个节点与 40 个节点建立配对密钥，所需的能耗约为 2.56J(D-H 协议通过指数运算计算配对密钥，相对于双线对运算及 ECC 上点乘运算而言，该能耗可以忽略)，平均建立一个配对密钥的开销约为 2.45s/64mJ；对于 IBEKAS 方案，则需要 7.07J，平均建立一个配对密钥的开销约为 7s/176.75mJ。

综上所述，本文方案具有基于身份加密的密钥协商方案的优点，如高的密钥连通率与网络连通率(=1)、抗毁性好、可扩展性好等；同时，相比基于 IBE 的传感器网络密钥协商方案，本文方案有效地减少了配对密钥的计算时间与能耗，邻居节点数为 40 时，建立配对密钥的平均开销(时间/能耗)为 IBEKAS 方案的 35%/36.21%，更适合于传感器网络。

结束语　基于 ECC 的身份加密系统的灵活性及安全性引起了广泛的关注，但如何减少基于身份加密的传感器密钥协商方案中建立配对密钥的能耗与时间，是一个有意思的研究问题。本文在 BNN-IBS 身份签名的基础上，提出了一个新的无线传感器网络密钥协商方案，通过带身份签名的广播在邻居节点间进行参数交换，节点通过 ECC 上的点乘进行签名验证并通过 D-H 密钥交换技术建立配对密钥。本文方案既保留了基于身份加密的传感器网络密钥协商方案的优点，又有效地解决了基于 IBE 的传感器网络密钥协商方案中双线对运算能耗较高且耗时较长的问题，比较适合当前的传感器网络。

参 考 文 献

[1] Eschenauer L, Gligor V. A key management scheme for distributed sensor networks[C]// Proc. of the 9th ACM Conf. on Computer and Communications Security. New York: ACM Press, 2002:41-47

[2] Blundo C, Santis A D, Herzberg A, et al. Perfectly secure key distribution for dynamic conferences[J]. Information and Computation, 1998, 146(1):1-23

[3] Chan H, Perrig A, Song D. Random key predistribution schemes for sensor networks[C]// Proc. of the 2003 IEEE Symp. on Security and Privacy. Washington: IEEE Computer Society, 2003: 197-213

[4] Liu D, Ning P. Location-based pairwise key establishments for static sensor networks[C]// Proc. of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks. New York: ACM Press, 2003:72-82

[5] Younis M, Ghumman K, Eltoweissy M. Location aware combinatorial key management scheme for clustered sensor networks [J]. IEEE Trans. on Parallel and Distribution System, 2006, 17 (8):865-882

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

[7] 杨庚，王江涛，程宏兵，等. 基于身份加密的无线传感器网络密钥分配方法[J]. 电子学报，2007，35(01)：180-184

[8] 程宏兵，费国臻. 基于身份的无线传感器网络密钥系统[J]. 计算机科学，2007，34(10)：116-119

[9] Bellare M, Namprempre C, Neven G. Security proofs for identity-based identification and signature schemes[C] // Proc. EUROCRYPT 2004. Springer-Verlag, 2004:268-286

[10] Cao X, Kou W, Dang L, et al. IMBAS: identity- based multi-user broadcast authentication in wireless sensor networks[J]. Computer Communications, 2008, 31:659-671

[11] Wander A, Gura N, Eberle H, et al. Energy analysis of public-key cryptography on small wireless devices[C]// Proc. PerCom' 05. IEEE, 2005:324-328

[12] MICA2 datasheet [EB/OL]. http://www.xbow.com/ Products/Product_pdf_files/ Wireless_pdf/MICA2_Datasheet.pdf/, 2006

[13] Bertoni G M, Chen L, Fragneto P, et al. Computing tate pairing on smartcards [EB/OL]. http://www.st.com/stonline products/families/smartcard/ches2005_v4.pdf/, 2005