带认证的 ZigBee 密钥分配方案

郁 滨 杨同豪*
(信息工程大学电子技术学院 郑州 450004)

摘 要：针对 ZigBee 节点组网时缺乏身份认证，密钥分配安全性不足的问题，该文提出一种基于身份的无双线性对运算的 ZigBee 节点身份认证及密钥分配方案。该方案继承了基于身份的认证方案的优点，在实现身份认证的同时完成了 ZigBee 密钥分配过程，具有较高的安全性和可扩展性。实验结果表明，该文方案具有存储开销小、能耗低等优势。

关键词：身份认证；密钥分配；ZigBee；基于身份
中图分类：TP309.1 **文献标识码**： A **文章编号**：1009-5896(2012)09-2277-05
DOI: 10.3724/SP.J.1146.2012.00104

A Key Distribution Scheme with Authentication for ZigBee

Yu Bin Yang Tong-hao
(*Institute of Electronic Technology*, *Information Engineering University*, *Zhengzhou* 450004, *China*)

Abstract: ZigBee nodes are deficient in identity authentication and key distribution security. For purpose of solving those issues, an identity-based ZigBee identity authentication and key distribution scheme without weil pairing is proposed. This scheme bears the strongpoint of identity-based authentication scheme. The completion of ZigBee key distribution can be simultaneous with identity authentication implementation with high security and extensibility. Experiments show that the proposed scheme has the advantage of limited storage cost, low energy consumption etc..

Key words: Identity authentication; Key distribution; ZigBee; Identity-based

1 引言

ZigBee 规范中采取的安全措施[1,2]能够满足一般网络通信的安全需求，但 ZigBee 网络在节点身份认证和密钥分配等方面仍存在诸多安全缺陷。首先，ZigBee 协议规定的加密模式采用的是单一的对称密钥加密算法[2]，其无法提供安全的身份认证服务。其次，对于 ZigBee 网络中的密钥分配，规范中采用的是基本的预共享密钥分配模型，即每对节点之间都预共享一个主密钥；而在没有共享主密钥的前提下，网络采用的是非安全即明文传输密钥命令[2]。此类密钥分配方案虽执行简单，但具有安全性不高、扩展性差、网络免疫力低等缺点[3]。

文献[4]提出了改进的基于信任中心的认证方案，此方案能够解决移动节点的认证问题，但同时加重了 ZigBee 网络中协调器的计算负担。文献[3]详细分析了 ZigBee 协议中每层所采用的安全处理机制，指出 ZigBee 需在加密模式、密钥建立等方面加强安全性。文献[5]针对链接密钥建立过程的安全漏洞改进了点对点对称密钥建立(Symmetric-Key Key Establishment, SKKE)协议，但方案执行时仍存在主密钥的预分配过程。Blaser[6]提出一种利用公钥密码体制进行 ZigBee 密钥分配的思路，并指出选取计算复杂度低、资源占用少的轻量级公钥密码算法进行密钥分配，可以在实现认证功能的同时避免主密钥的预分配过程。

目前基于公钥密码体制的 ZigBee 密钥分配方案研究仍不够完善，文献[7]指出基于身份的密码体制(Identity-Based Cryptography, IBC)是最适合此类无线传感器网络的公钥体制。文献[8]提出了基于身份的加密算法 IBE，此后出现了一些适用于无线传感网络的 IBC 方案[9–11]，但传统的 IBC 基于双线性对运算计算开销较大[11]。文献[12]提出了基于椭圆曲线的 IBS 方案(BNN-IBS)，该方案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。椭圆曲线密码体制在相同安全强度要求下具有密钥长度短、算法速度快、占用内存少和抗攻击能力强等优点；而点乘运算与双线性对运算相比能够带来更小的计算开销，这对于资源受限的 ZigBee 节点是非常重要的。

2012-02-10 收到，2012-05-31 改回
*通信作者：杨同豪 youngtonghao@163.com

综上所述，本文以 BNN-IBS 签名方案为基础，设计 ZigBee 安全增强模型，提出一种基于身份的无双线性对运算的节点身份认证及密钥分配方案。方案能够解决主密钥预分配带来的安全隐患，同时，运用椭圆曲线密码体制解决了 ZigBee 节点容量小、计算能力弱的问题。

2 方案总体设计

ZigBee 规范中，密钥分配及管理服务主要由网络层以上各层提供，本文提出的方案主要通过为应用层相关子层增加身份认证服务及改进密钥建立、密钥传输等服务增强密钥分配的安全性。据此，依托 ZigBee 协议栈，设计 ZigBee 安全增强模型如图 1 所示。

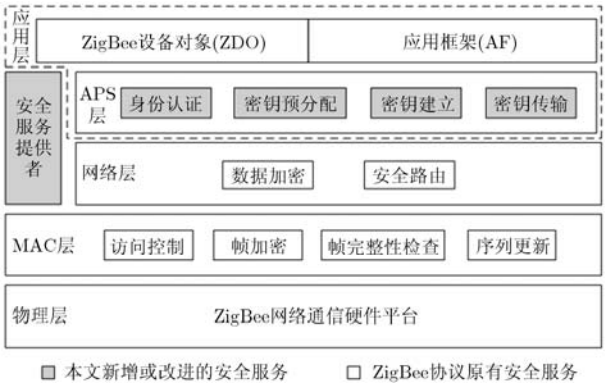

图 1 ZigBee 安全增强模型

其中，物理层以 ZigBee 网络通信硬件平台为基础，保证数据可靠传输。MAC 层和网络层负责本层原有的各类安全服务，应用层主要利用 ZigBee 设备对象及应用层构架通过应用支持子层(APS)管理实体服务访问接口对身份认证及密钥分配相关服务进行调用。

安全服务提供者作为提供安全服务的主体，需要为 APS 层安全管理和网络层安全管理提供服务接口。该模块主要实现椭圆曲线等相关算法，同时还需要执行网络公共参数及节点公私钥对等 ZigBee 节点参数的合理存储和调用。

身份认证服务实体作为新增的安全模块向上层具体应用提供身份认证服务，本文通过在 ZigBee 协议栈 APS 层添加对数据发送和接收的处理接口来实现 ZigBee 节点签名验证，并以此实现节点的双向身份认证。

密钥建立、密钥传输及密钥请求等服务实体则是在 ZigBee 协议原有安全模块的基础上进行的安全增强设计。其中，密钥建立服务实体主要实现链接密钥的生成功能，节点身份认证成功的同时，该模块调用安全服务提供者提供的算法库运算得出相邻节点间共享的链接密钥。在初始链接密钥建立完成的基础上，通过调用密钥传输及密钥请求服务实体，ZigBee 网络中各节点能够保证执行网络密钥传输、链接密钥更新等操作的安全性。

3 协议流程设计

依据图 1 设计的 ZigBee 安全增强模型，本节改进 BNN-IBS 方案，设计带认证的密钥分配协议，协议中所使用的符号及其含义如表 1 所示。

表 1 协议中所使用的符号及含义

符号	含义
$\mathrm{GF}(2^n)$	二元有限域
E/F_{2^n}	椭圆曲线
$E(F_{2^n})$	椭圆曲线上的点构成的群
P	椭圆曲线上阶为 p 的点
G	P 生成的加法群
$H(\ )$	哈希函数

ZigBee 节点组网之前，离线服务器需首先选取满足安全要求的 $\{E/F_{2^n}, p, G, P\}$ 和主密钥 $x \in Z_p^*$，计算系统公钥 $Q = xP$；并选择两个密码学哈希函数 $H_1: \{0,1\}^* \times G \to Z_p^*$ 和 $H_2: \{0,1\}^* \times G \times G \times G \to \{0,1\}^k$，其中，$H_1$ 是一个将节点身份信息映射为密钥空间中某个元素的单向钥控哈希函数，用于实现节点身份信息的签名验证，H_2 用于实现 ZigBee 节点签名和共享密钥的生成。然后，离线服务器选择 $r_U \in Z_p^*$ 为 ZigBee 节点 U 生成节点公私钥对 (R_U, s_U)。完成网络公共参数及节点公私钥对的生成后，离线服务器将其注入 ZigBee 节点。令 A 为 ZigBee 网络新加入节点，B 为网络合法节点，协议流程具体设计如图 2 所示。

由图 2 所示，离线服务器首先为新节点 A 预置网络公共参数和公私钥对，A 生成签名验证信息并发送至网络中的可信路由节点 B。节点 B 收到签名验证信息后与节点 A 进行双向身份认证，若节点 A 或 B 中任一方的身份认证出现错误，则终止密钥分配过程，新节点 A 入网失败。若身份认证成功，节点 A 获得与节点 B 进行通信的链接密钥。此链接密钥可应用于 ZigBee 应用层及其子层，用于提供密钥传输服务和数据帧安全服务。其中，密钥传输服务用于安全传输 ZigBee 网络密钥；数据帧安全服务主要用于提供应用层点对点的安全数据传输。至此，ZigBee 节点完成身份认证及密钥分配过程，节点 A 安全加入 ZigBee 网络。

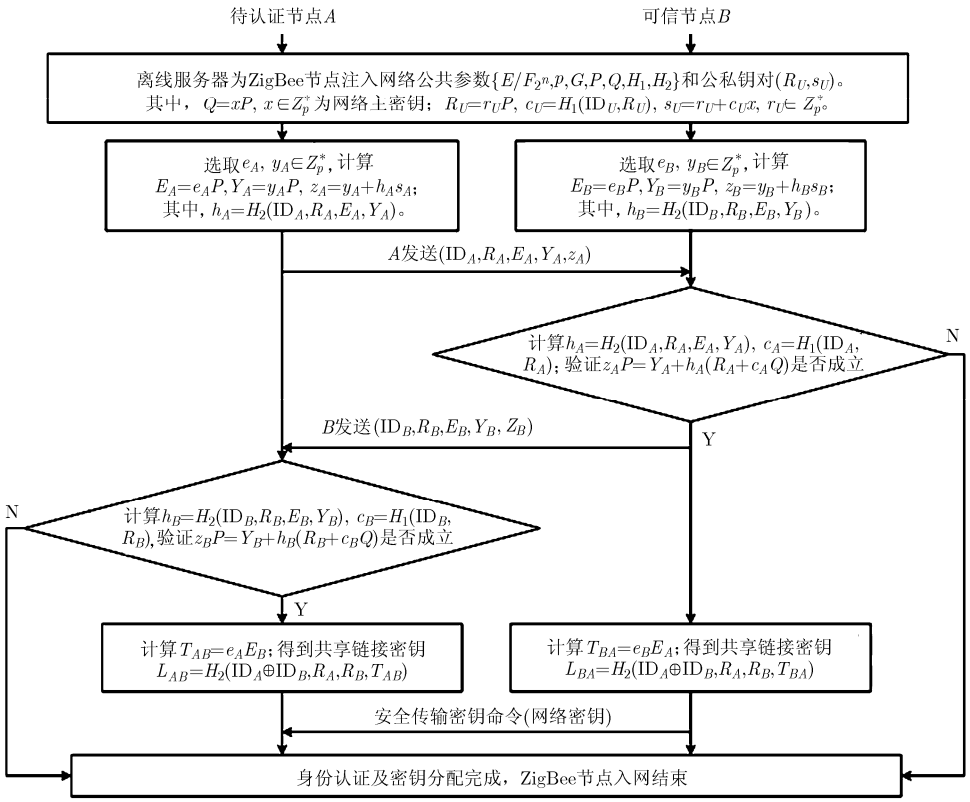

图 2 ZigBee 节点密钥分配协议流程

4　安全性分析

本节对上文提出的带认证的 ZigBee 密钥分配方案进行安全性分析，此方案的安全性主要基于椭圆曲线上的离散对数问题，在椭圆曲线加法群 G 上，有如下安全性假设成立：

假设 1　计算性 Diffie-Hellman(CDH)：对未知的 $a,b\in Z_p^*$，给定 (aP,bP)，计算 abP 是困难的。

假设 2　除法性计算性 Diffie-Hellman(DCDH)：对未知的 $a,b\in Z_p^*$，给定 (aP,bP)，计算 $ab^{-1}P$ 是困难的。

基于以上安全性假设，得出本文方案具有以下安全性结论：

结论 1　认证过程能够有效抵抗中间人攻击。

ZigBee 节点身份认证采用的是基于身份的双向认证方案，方案的实现在椭圆曲线加法群上完成。节点 A 基于身份信息生成签名 $(\mathrm{ID}_A,R_A,E_A,Y_A,z_A)$ 并发送至节点 B 后，B 通过检查 $z_AP=Y_A+h_A(R_A+c_AQ)$ 是否成立来验证节点 A 的真实性。若攻击者欲伪造此签名信息，必须攻破节点 A 的私钥 s_A，而由 DCDH 假设可知由 R_A 计算得出 s_A 是困难的。

结论 2　密钥分配方案满足完善前向保密性。

基于 CDH 假设，即使攻击者截获消息 $E_A=e_AP$ 和 $E_B=e_BP$，也无法由此获得 e_Ae_BP。由此攻击者也无法得到节点之间的共享链接密钥。此外，由于 ZigBee 节点 A 和 B 之间链接密钥的确定还需要随机数 e_A,e_B 的参与，因此即使 ZigBee 网络主密钥或节点私钥泄露均可以保证之前建立的链接密钥的安全。此密钥分配方案具有完善的前向保密性。

结论 3　方案为 ZigBee 网络提供最佳的网络免疫力。

每对 ZigBee 节点之间的链接密钥对是唯一的，任何节点的被俘都不会向攻击者透露除与自身直接通信的节点之外的任何节点信息。而且不论被俘节点的数目为多少，攻击者都很难得到未俘节点的秘密信息。这是因为 ZigBee 网络的公开信息均为 BNN-IBS 方案的系统参数，攻击者欲通过公开信息和俘获节点的秘密信息来获取未俘节点 A 的私钥 s_A，仍需面对攻破椭圆曲线上的离散对数问题，而由 CDH 假设和 DCDH 假设，此攻击是困难的。

5　实验及结果分析

5.1　方案实验

依据设计的 ZigBee 安全增强模型及密钥分配协议流程，本文改进了 ZigBee 2007 协议栈，并在 ZigBee CC2530 硬件平台上进行 ZigBee 密钥分配实验。其中，硬件节点使用自制 ZigBee 网络通信平台，其主芯片为 CC2530(8 bit, 8051MPU, 32 MHz，电

压 3 V，无数据收发时 MPU 正常工作电流 6.5 mA)[13]。

实验选用普通 PC 机作为 ZigBee 网络离线服务器用于密钥参数的生成和预置。ZigBee 节点 ID 长度为 64 bit(物理地址的长度)，选取椭圆曲线上点的坐标长度为 64 bit，即 $n=|p|=64$。ZigBee 节点中网络公共参数和对应公私钥对的注入均通过离线服务器改进 ZigBee 协议栈程序并编译下载至 CC2530 芯片中完成。固件程序下载完成后，ZigBee 协调器上电初始化网络，其它节点在加入网络的同时即可实现节点之间双向身份认证和密钥分配功能。

5.2 结果分析

本节主要讨论方案的开销与能耗分析，并与 ZigBee 规范中原有密钥分配方案和文献[11]中基于双线性对运算的方案进行对比。

(1)存储开销　以主密钥所需的存储空间为 1, ZigBee 网络容量为 N，原规范中每个节点存储主密钥的开销为 N-1，此外节点中还需保存用于进行链接密钥建立的 SKKE 协议相关参数等。而本文方案中避免了原有 ZigBee 规范中主密钥预分配过程，因此，不必预置主密钥而只需存储 ZigBee 网络公共参数和节点公私钥对等信息。文献[11]中的存储开销与本文方案的存储开销处于同一层次。图 3 为本文方案和 ZigBee 规范中原有密钥分配方案的存储开销示意图。

由图 3 可知，在 ZigBee 网络容量不大的情况下，ZigBee 规范中原有密钥分配方案和本文方案均能保持较小的存储开销；但随着网络容量的增大，原方案所占用的存储开销逐步增加，这是由于节点中所预存储的主密钥有冗余造成的。而本文方案由于认证和密钥分配过程是基于身份进行的，因此并不会因 ZigBee 网络容量的增大而使存储开销增加，同时还保证了 ZigBee 网络具有良好的扩展性。

(2)通信开销　以双方节点链接密钥分配完成所需的通信数据量来表示通信开销，ZigBee 规范中原有链接密钥的建立需进行 4 次 SKKE 命令传输，总数据长度为 768 bit[1]。本文方案中，进行链接密钥分配的节点之间需要进行 2 次消息传输，传输的总数据长度为 2×5×64 bit＝640 bit。本文方案与文献[11]中基于双线性对运算的方案相比在通信开销上是相同的。设 ZigBee 节点的邻居节点数为 m，本文方案和 ZigBee 规范中原有密钥分配方案的通信开销如图 4 所示。

(3)计算开销　表 2 列出了 3 种方案的计算开销。其中，H 表示哈希运算；S 表示椭圆曲线上的点乘运算；P 表示双线性对运算。

表 2 ZigBee 密钥分配方案计算开销分析

运算方法	本文方案	原 ZigBee 方案	文献[11]方案
H	3	4	2
S	4	0	2
P	0	0	1

双线性对运算、哈希运算的计算复杂度分别是椭圆曲线上的点乘运算的 20 倍和 1 倍[11]，因此在计算开销上本文方案与文献[11]中方案相比有很大的改善。虽然本文方案比原 ZigBee 规范中的密钥分配方案的计算开销要大，但是 ZigBee 规范中原有方案并不具备身份认证的能力，其安全性也弱于本文方案。

(4)综合能耗分析　假设与 MICA2 节点类似[14]，CC2530 节点发送与接收一个字节的能耗分别为 0.0592 mJ 和 0.0286 mJ，设 ZigBee 网络中节点的平均邻居节点数为 m，则本文方案、ZigBee 规范中原有方案和文献[11]中方案的通信能耗分别为 $3.512m$ mJ, $4.2144m$ mJ 和 $3.512m$ mJ。为简化分析，设双线性对运算和哈希运算所消耗的能量分别为椭圆曲线上的点乘运算的 20 倍和 1 倍，而在 CC2530 节点上，进行一次椭圆曲线上的点乘运算需 0.21 s，能耗约为 0.21 s×3 V×6.5 mA=4.095 mJ。则本文方案、ZigBee 规范中原有方案和文献[11]中方案的计算能耗分别为 28.665 mJ, 16.38 mJ 和 98.28 mJ。3 种方案的综合能耗对比如图 5 所示。

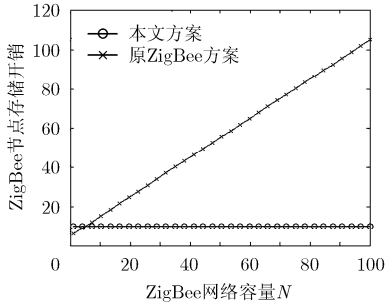

图 3 存储开销

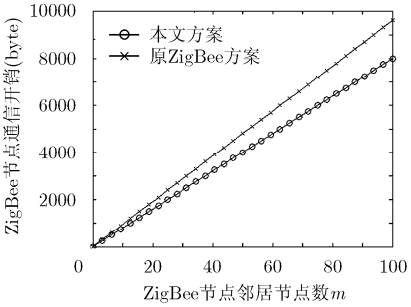

图 4 通信开销

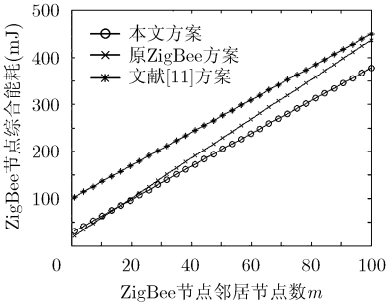

图 5 综合能耗

由图 5 可知，在 ZigBee 节点的邻居节点数目不多的情况下，3 种方案的综合能耗均较小，但当邻居节点的数目增多的情况下，本文方案的综合能耗对比 ZigBee 规范中原有方案和文献[11]中方案具有比较明显的优势。

6　结束语

本文在深入研究各种基于身份的认证及密钥分配方案的基础上，利用椭圆曲线加法群构造了一种无双线性对运算的带认证的 ZigBee 密钥分配方案。该方案具有基于身份的密钥分配方案的优点，网络的安全性高，免疫力强，扩展性好。相比 ZigBee 规范中原有密钥分配方案，本文方案在实现 ZigBee 链接密钥分配的同时完成了节点的身份认证，保证了 ZigBee 密钥分配安全性，并且能够有效减少存储开销和能耗，适合大规模 ZigBee 网络的应用。

参 考 文 献

[1] ZigBee Alliance. ZigBee specifications[EB/OL]. http://www.zigbee.org, 2008.

[2] ZigBee Alliance. ZigBee security specification overview[EB/OL]. http://www.zigbee.org, 2010.

[3] Yüksel E, Nielson H R, and Nielson F. ZigBee-2007 security essentials[C]. Proceedings of the 13th Nordic Workshop on Secure IT Systems, Copenhagen, 2008: 65–82.

[4] Lee Kyung hwa, Lee Jooh yun, Zhang Bong duk, *et al*.. An enhanced trust center based authentication in ZigBee networks[C]. Advances in Information Security and Assurance, Lecture Notes in Computer Science, Seoul, 2009, 5576: 471–484.

[5] Yüksel E, Nielson H R, and Nielson F. A secure key establishment protocol for ZigBee wireless sensor networks[J]. *Computer Journal*, 2011, 54(4): 589–601.

[6] Blaser M. Industrial-strength security for ZigBee: the case for public-key cryptography[J]. *Embedded Computing Design*, 2005, 3(3): 48–52.

[7] Oliveira L B, Dahab R, Lopez J, *et al*.. Identity-based encryption for sensor networks[C]. Proceedings of the 5th Annual IEEE Internationa1 Conference on PerCom Workshops, New York, 2007: 290–294.

[8] Shamir A. Identity-based cryptography and signature schemes[C]. Advances in Cryptology, Lecture Notes in Computer Science, California, 1984, 196: 47–53.

[9] 刘文琦, 顾宏, 杨建华. 基于身份的同时生效签密体制研究[J]. 电子与信息学报, 2011, 33(7): 1582–1588.
Liu Wen-qi, Gu Hong, and Yang Jian-hua. Identity-based concurrent signcryption scheme[J]. *Journal of Electronics & Information Technology*, 2011, 33(7): 1582–1588.

[10] Sun Zhong-wei and Wu Ju-ying. Identity-based access control for distribution automation using EPON[J]. *Chinese Journal of Electronics*, 2011, 20(3): 443–446.

[11] Chen L, Cheng Z, and Smart N P. Identity-based key agreement protocols from pairings[J]. *International Journal of Information Security*, 2007, 6(4): 213–241.

[12] Bellare M, Namprempre C, and Neven G. Security proofs for identity-based identification and signature scheme[J]. *Journal of Cryptology*, 2009, 22(1): 1–61.

[13] Texas Instruments. CC2530_datasheet[EB/OL]. http://www.ti.com, 2011.

[14] Wander A, Gura N, Eberle H, *et al*.. Energy analysis of public-key cryptography on small wireless devices[C]. Proceedings of the 3rd Annual IEEE Internationa1 Conference on PerCom Workshops, Hawaii, 2005: 324–328.

郁　滨：　男，1964年生，教授，博士生导师，主要研究方向为信息安全、无线网络安全技术和视觉密码等.

杨同豪：　男，1987年生，硕士生，研究方向为信息安全、无线网络安全技术.