一种基于IBE算法的ZigBee网络加密方法

房国志， 李 超

（哈尔滨理工大学 测控技术与通信工程学院，黑龙江 哈尔滨 150040）

【摘 要】ZigBee是一种近距离、低速率、低功耗、低成本的无线传输技术。针对ZigBee网络的对称密钥体系在密钥分配和管理方面仍存在的局限性，提出了基于身份标识加密算法的密钥分配和管理方案。仿真平台TinyOS的实验结果表明基于身份标识加密算法在增强ZigBee网络的安全的同时，减少了密钥数量，为ZigBee网络加密提供了新的手段。

【关键词】紫峰技术；基于身份标识加密算法；网络安全；加密

【中图分类号】TN92 **【文献标识码】**A **【文章编号】**1002-0802(2010)02-0134-03

An Encryption Scheme for ZigBee Networks Based on Identity-Based Encryption

FANG Guo-zhi， LI Chao

(College of Measure-control Technology & Communication Engineering，Harbin Univ. of Sci. & Tech.，Harbin Heilongjiang 150040, China)

【Abstract】ZigBee is a new wireless transmission technology and of such features as low rate, low power consumption and low cost. The ZigBee network currently employs Advanced Encryption Standard, that is, AES128, for encryption. However, there is still exists some application restriction. In this paper, we present an identity-based encryption scheme for ZigBee network is proposed. Experiment on TinyOS platform shows that the proposed scheme is of some advantages in terms of storage requirement and security, and it provides a new approach to the encryption in ZigBee networks.

【Key words】ZigBee；identity-based encryption；network security；encryption

0 引言

近几年来无线传感网络(WSN)研究引起了人们的极大关注[1]。ZigBee技术作为一种新兴的短距离无线通信技术，在无线传感网络中有着良好的应用前景。虽然ZigBee网络中采用了基于AES-128加密算法对称密钥的安全机制，但是其应用没有完全体现出公共密钥体系中的诸如数字签名和无需证书认证的优点。而且在对数据安全性敏感的监控和控制应用中，需要有对ZigBee设备身份鉴别的能力。考虑到ZigBee网络节点具有计算能力低、电源能量有限、易被攻击等特点，本文提出了基于IBE算法的ZigBee网络加密方案。在公共密钥体系上发展而来的基于IBE算法加密方案具有公钥简单、分发简便等优点，适合于短距离ZigBee无线网络的密钥管理、加密和解密。仿真结果表明IBE加密方案在保证网络安全的同时，能够减少资源的需求、降低系统的复杂性。

收稿日期：2008-04-28。

作者简介：房国志（1968-），男，博士研究生，主要研究方向为无线传感网络、测试测量、嵌入式系统；李 超（1984-），男，硕士，主要研究方向为无线传感网络。

1 ZigBee网络安全结构和加密算法分析

ZigBee 技术的物理层和数据链路层协议主要采用IEEE802.15.4 标准，而网络层和应用层由ZigBee 联盟负责建立。数据链路层、网络层和应用层负责在各自层上传输安全的数据，而且应用子层提供安全关系的建立和维护等服务、ZigBee设备对象管理安全策略和设备的安全配置。ZigBee协议提供了一套基于128位AES算法的对称密钥体系，同时还使用了更新计数器和信息完整性检测来阻止对网络的反复攻击和信息的修改。ZigBee网络中存在三种基本密钥：主密钥、链接密钥和网络密钥。链接密钥和网络密钥可以在设备制造时设置，也可以通过主密钥建立，并且它们还可以定期的更新。在整个ZigBee网络中，信任中心负责网络成员管理和密钥分配。信任中心有两种工作模式：住宅模式(Residential Mode)和商业模式(Commercial Mode)。

下页图1描绘了在住宅模式和商业模式中使用的密钥的数量。在图1中，节点A是ZigBee网络的协调者，节点B、C、D是路由节点，节点E、F、G、H是网络的终端节点。在住宅

模式中，整个网络只使用一个密钥K_N。在商业模式中，K_{MXY}是X与Y之间的主密钥，K_{LXY}是X与Y之间的链接密钥。

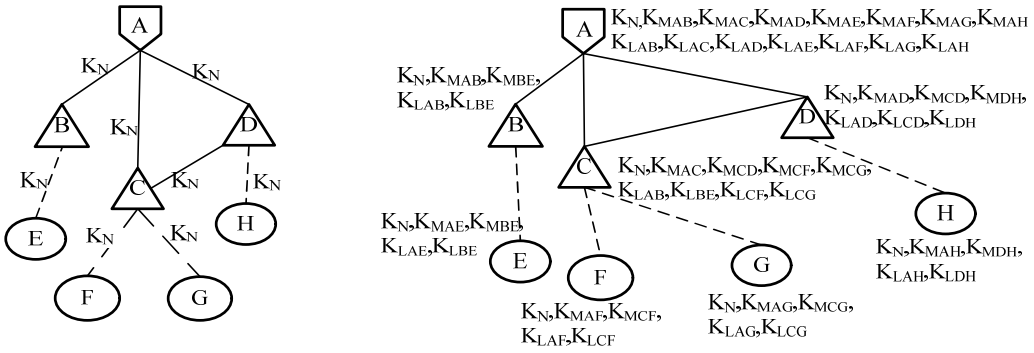
虽然现行的ZigBee安全协议通过用AES算法为信息传输的安全提供有力的保障，但是它还是有一定的局限性：

① 网络中使用的安全密钥的数量。只使用一个密钥的住宅模式虽然能够保证资源的最优化，但不能阻止内部攻击。商业模式是很安全但却需要大量的密钥（主密钥、网络密钥、链接密钥），占用更多的频带资源；

② 这种基于对称密钥加密系统模式不提供数字签名和不可抵赖（Non-repudiation）能力。虽然这种模式能够满足人类日常应用，但是在一些关键性应用中仍需要更强的保护能力；

③ 对称密钥的分配问题。该模式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。同时，在新增加节点和删除节点后，必须建立新的相邻节点的密钥对。

鉴于对称加密系统在密钥管理和安全性方面不足，结合ZigBee网络节点的计算能力低、电源能量有限、易被攻击等特点，本文提出了基于IBE算法的ZigBee网络加密方案。



(a)住宅模式超群　　(b) 商业模式

图1 住宅模式和商业模式中的密钥

2 基于IBE的ZigBee网络密钥理论分析和建立方法

文献[2]研究了一种基于硬件的非对称密钥加密算法。采用优化的参数和算法，其能量消耗可小于20 μW。这使得非对称密钥算法在ZigBee网络中的应用成为可能。文献[3]研究指出椭圆曲线密码系统(Elliptic Curve Cryptography， ECC)在计算量和内存需求方面有一定的优势，使得基于身份标识的加密算法IBE适合应用于ZigBee网络。

基于身份标识的加密算法IBE由Shamir于1984年首先提出的。直到2001年Boneh和Franklin的论文才给出了一个可实际应用的实现方法。在网络中，负责生成并传送用户私钥的可信第三方记为PKG(Private Key Generator)[4]。IBE算法过程如下。

2. 1 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Z_q为素数阶q的加法群，$Z_q=\{0,1,\cdots,q-1\}$，Z^+为正整数，G_1为循环加法群，G_2为循环乘法群，G_1、G_2具有相同的素数阶q。

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：

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；

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

可计算性：有一个多项式时间算法来计算$\hat{e}(P,Q)$。

2.2 Boneh-Franklin IBE算法

基本的Boneh-Franklin IBE算法主要由4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[5]。

算法1：The Basic Boneh-Franklin (BBF) Scheme。

Setup：

Step 1：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$E/GF(p)$，$E/GF(p)$的q阶子群G，G的生成元P，双线性映$\hat{e}G\times G\to GF(p^2)^*$；

Setp 2：PKG随机取$s\in Z_q^*$，计算$P_{pub}=sP$；

Step 3：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：$\pi=\{p,\hat{e},n,P,P_{pub},H_1,H_2\}$，$s\in Z_q^*$为主密钥（Master key）。

Extract：对给定的字符串$Id\in\{0,1\}^*$，生成密钥。

Step 4：计算$Q_{Id}=H_1(Id)\in E/GF(p)$。

Step 5：取密钥为$K_{Id}=(Q_{Id})^3$。

Encrypt：对原文 $m \in M$ 和公钥 Id，加密步骤如下。

Step 6：计算 $Q_{Id} = H_1(Id) \in E / GF(p)$。

Step 7：随机取 $\gamma \in Z_q^*$，加密的密文为：$c = <\gamma P, m \oplus H_2(g_{Id}^{\gamma})>$，其中 $g_{Id} = \hat{e}(Q_{Id}, P_{pub}) \in GF(p^2)$。

Decrypt：设 $c = <U, V>$ 为密文，解密步骤为：

Step 9：应用密钥 $K_{Id} \in E / GF(p)$，计算原文 $m = V \oplus H_2(\hat{e}(K_{Id}, U))$。

2.3 基于身份标识密钥体系的ZigBee网络密钥建立方法

基于BBF算法，本节给出一种应用于ZigBee网络的密钥建立、分配和加密方法。它由3部分组成，具体方法定义如下。

（1）初始化过程

初始化过程由两部分组成，一是计算公共参数，二是计算节点密钥。首先应用Setup函数计算公共参数 $\pi = \{p, \hat{e}, n, P, P_{pub}, H_1, H_2\}$，并选择主密钥 s。

应用Extract函数，根据每个无线节点的标识 $Id \in \{0,1\}^*$，计算 $Q_{Id} = H_1(Id) \in E / GF(p)$ 和相对应的密钥 $K_{Id} = (Q_{Id})^s$。

将 π、Id 和 K_{Id} 写入到无线节点中，使得每个节点都有自己的密钥和相关的公共参数。

（2）加密过程

对一个无线传感器网络中的发送节点A和接收节点B，以及明文m，B的身份 Id 为公钥，随机取 $\gamma \in Z_q^*$。

应用公共参数进行明文加密，密文为：$c = <\gamma P, m \oplus H_2(g_{Id}^4)>$，其中 $g_{Id} = \hat{e}(Q_{Id}, P_{pub}) \in GF(p^2)$。

特别要指出的是，基于IBE算法，可以将加密和认证结合起来，以小的代价同时完成加密和认证。这也是IBE算法可进一步应用于ZigBee网络的优势。

节点 B 收到密文 $c = <U, V>$ 后，应用密钥 $K_{Id} \in E / GF(p)$，计算原文：$m = V \oplus H_2(\hat{e}(K_{Id}, U))$。

2.3 基于身份标识密钥体系的ZigBee网络密钥工作过程

在ZigBee网络中使用各个设备的功能作为它的身份来区分其他的设备。如果多个设备的功能相同，身份信息包含其他信息来区分这些设备，如位置信息或连续信息。为了增强安全性身份信息还可以附加上时间标识（Time-stamp）。总的来说，身份信息可以表示为：

ID = {device_description@domain||time-stamp}。

基于IBE的ZigBee网络加密系统的工作原理与基于身份加密系统模型相类似，其工作步骤如下：

① 信任中心（Coordinator，网络协调器）生成一个主密钥（Master-key），同时把公共参数（Params）广播给所有网络设备；

② 加入ZigBee网络的设备向信任中心注册自己的身份信（Id_{device}）；

③ 信任中心（PKG）授权一个私钥（Pr_{id}）给完成注册的设备，其中包含了该设备的身份信息；

④ 和该设备通信的其他设备，获取该设备的身份信息（Id_{device}），用该信息对发送到该设备的消息加密。发送者也在发送信息中表明自己的私钥（Pr_{sender}）；

⑤ 加密消息通过若干中继到达目的节点。在传输过程中消息是安全的，因为只有拥有相应私钥（Pr_{device}）目的节点才能解密并阅读该信息。

其加密方案如图2，图3所示。

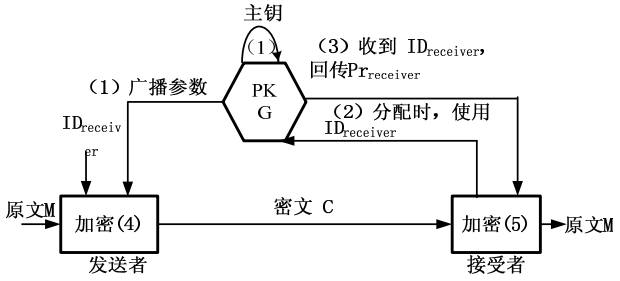


图2 IBE加密方案

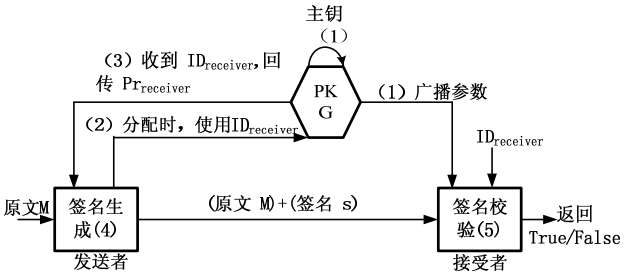


图3 IBE签名方案

2.4 基于身份标识密钥体系的ZigBee网络密钥与其他加密方法比较

TinyOS是UC Berkeley（加州大学伯克利分校）开发的开放源代码操作系统，专为嵌入式无线传感网络设计。它基于一种组件的架构方式，能够快速实现无线传感器网络的仿真，提供运行时的调试和配置，可以实时监测网络状况。实验中随机布置了50个无线传感器节点（见图4）[6-7]，这些节点都有一个唯一的身份标识*Id*。在仿真ZigBee网络过程中，初始化过程在组网之前完成，传感器节点只需进行基于IBE加密和解密工作。实验表明基于IBE算法的加密方法可适用于ZigBee无线传感器网络的密钥管理、加密和解密。下页表1是不同加密方法的对比，其中，*n*为ZigBee网络中网络节点的数量。

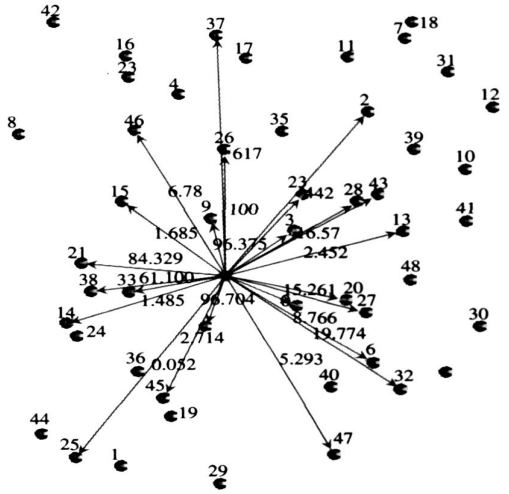


图4 仿真网络拓扑

（下转第140页）

```
void*GetRoutineAddress(char*ModuleName,char*
                        RoutineName)
{
 PIMAGE_DOS_HEADER dos_hdr;
 PIMAGE_NT_HEADERS nt_hdr;
 PIMAGE_EXPORT_DIRECTORY export_dir;
 ULONG *fn_name, *fn_addr, i;
 char* base;
 base=(char*)FindModule(ModuleName);//该函数用来获
得内核模块的基地址
 nt_hdr=(PIMAGE_NT_HEADERS)(base+ dos_hdr->
        e_lfanew);
 export_dir = (PIMAGE_EXPORT_DIRECTORY)(base +
nt_hdr->OptionalHeader.DataDirectory[IMAGE_DIRECTORY
_ENTRY_EXPORT].VirtualAddress);
 fn_name=(ULONG*)(base+export_dir->AddressOfNames);
 fn_addr=(ULONG*)(base+ export_dir->AddressOfFuncti
        ons);
 for (i = 0; i < export_dir->NumberOfNames; i++,
fn_name++, fn_addr++)
 if (strcmp(RoutineName, base + *fn_name) == 0)
 return base + *fn_addr;
 return NULL;
 }
```

3 结语

经分析测试，基于 NDIS-hook 的方法可以取得比在用户层截获包更高的效率，并且不需要手动安装，可以动态地加载或卸载，提高了软件的使用性。这种方法只需对发送、接收的几个函数进行操作，可以不用分析 NDIS 那宏大的体系结构，实现起来也很简单，对系统的兼容性也非常好，现在很多防火墙都采用的这种技术，具有较大的商业价值。总体来说，网络截获包技术已经发展的很完善了，对包的分析匹配的效率还具有很大的提升空间，这也是本文的下一步工作。

参考文献

[1] 高泽胜,陶宏才.基于NDIS-HOOK与SPI的个人防火墙研究与设计[J].计算机应用研究,2003(11):279-281.

[2] 王艳平,张越.Windows 网络与通信程序设计[M].北京:人民邮电出版社,2006:257-256.

[3] 侯功华，赵远东.基于 NDIS 中间层的包过滤的研究与设计[J].微计算机信息,2006(22):141-143.

[4] 朱雁辉.Windows 防火墙与网络封包截获技术[M].北京:电子工业出版社,2002:331-332.

[5] 任建华. 基于主机的实时监控技术的研究与实现[D].南京:南京航空航天大学, 2005:19-22.

（上接第 136 页）

表1 ZigBee各种安全加密方法的比较

性能	加密方法		
	对称加密系统	公钥加密体系	身份标识加密体系
所需密钥总数（网状网络）	$O(n^2)$	$O(n)$	$O(n)$
密钥存储空间	大，每个节点或网络中心节点	较少，网络中心节点	不需要
密钥复杂性和安全性	$O(n)$	$O(n)$	$O(n)+O(lb_2^q)$
计算速度（160 位）	较慢	较快	快

3 结语

与ZigBee协议中的对称加密系统相比，基于IBE算法具有公钥密钥系统的优势，如密钥的管理、建立等，而且与网络的规模无关；与传统的公钥密钥系统相比，如RSA算法，在安全性、计算速度、存储要求、带宽需求等方面具有优势，IBE算法采用的公钥是基于节点的身份标识，相比于RSA加密系统具有更短的密钥长度，减少了计算量和通信开销。基于IBE算法，可以将加密和认证结合起来，以小的代价同时完成加密和认证。本文的理论分析和实验结果表明，基于IBE算法的密钥方法适应用于ZigBee网络，为该类型的网络安全提供了新的加密手段。

参考文献

[1] Akyildiz I F. Wireless Sensor Networks：A survey[J].Computer Networks,2002,38(04):393-422.

[2] Gaubatz G,Kaps J,Sunar B. Public Keys Cryptography in Sensor Networks Revisited[C]//The Proceedings of the 1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS). Heidelberg,Germany,2004:2-18.

[3] Lauter K.The Advantages of Elliptic Curve Cryptography for Wireless Security[J].IEEE Wireless Communications,2004,11(01):62-67.

[4] Blaser M.Industrial-strength Security for ZigBee:The Case for Public-key Cryptography[J].Embedded Computing Design,2005(09):48-52.

[5] A Novel Encryption Scheme for Wireless Sensor Networks Based on Identity-Based Encryption[J].Journal of Nanjing University of Posts and Telecommunications: Natural Science, 2007(27):1-7.

[6] 韩勇,陈强,王建新.移动Ad hoc 网络仿真工具比较[J].通信技术,2008,41(12):305-307.

[7] 文春生. Ad Hoc 网络的复合安全策略研究[J].通信技术,2008,42(05):205-207.

一种基于IBE算法的ZigBee网络加密方法

作者： 房国志， 李超， FANG Guo-zhi， LI Chao
作者单位： 哈尔滨理工大学,测控技术与通信工程学院,黑龙江,哈尔滨,150040
刊名： 通信技术PKU
英文刊名： COMMUNICATIONS TECHNOLOGY
年，卷(期)： 2010，43(2)
被引用次数： 0次

参考文献(7条)

1. Akyildiz I F Wireless Sensor Networks:A survey 2002(4)

2. Gaubatz G. Kaps J. Sunar B Public Keys Cryptography in Sensor Networks Revisited 2004

3. Lauter K The Advantages of Elliptic Curve Cryptography for Wireless Security 2004(1)

4. Blaser M Industrial-strength Security for ZigBee:The Case for Public-key Cryptography 2005(9)

5. A Novel Encryption Scheme for Wireless Sensor Networks Based on Identity-Based Encryption 2007(27)

6. 韩勇. 陈强. 王建新 移动Ad hoc网络仿真工具比较[期刊论文]-通信技术 2008(12)

7. 文春生 Ad Hoc网络的复合安全策略研究[期刊论文]-通信技术 2009(5)