基于非对称密钥体制的 ZigBee 安全改进

冯道水[1]，高泽华[1,3,4]，赵荣华[2]
（1. 北京邮电大学信息与通信工程学院，北京 100876;
2. 北京邮电大学信息光子学与光通信研究院，北京 100876;
3. 泛网无线通信教育部实验室，北京 100876;
4. 光通信与光波技术教育部重点实验室，北京 100876）

摘要：ZigBee 技术是一种新兴的近距离、低功耗、低速率、低复杂度、低成本的双向无线网络技术。本文阐述了 ZigBee 网络的安全机制，分析了 ZigBee 网络在安全性方面存在的问题；通过对网络安全性的分析有针对性的提出了改进方案，使得网络的安全性有了提高并且进一步降低了网络的复杂度和成本，使得 ZigBee 技术的适应场合更加宽广。

关键词：通信安全；ZigBee；非对称密钥；安全改进

中图分类号：TN92

ZigBee security improvements based on Asymmetric key system

Feng Daoshui[1], Gao Zehua[1,3,4], Zhao Ronghua[2]
(1. Schoole Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100876;
2. Institute of optical communication and Optoelectronics, Beijing University of Posts and Telecommunications, Beijing 100876;
3. Key Laboratory of UWC, Beijing 100876;
4. Key Laboratory of OCLT, Beijing 100876)

Abstract: ZigBee tecnology is a newly emerged wireless network, which has a character for close-range, low rate, low power, Low-complexity and low-cost. In this paper, the Security Mechanism of ZigBee is described and analysised in detail. An approved scheme put forward through analysising, then sercurity of zigbee increase by a large margin and make further improvement on cost.

Keywords: Safety of Communication; ZigBee; Asymmetric-key; Improvement of security

0 引言

ZigBee 技术是一种新兴的近距离、低功耗、低速率、低复杂度、低成本的双向无线网络技术，这是一种介于 RFID（射频识别）和 Bluetooth（蓝牙）之间的一种技术方案，主要用于近距离低速率的无线连接，可以在数量众多的网络节点之间进行数据传输的低速率网络。ZigBee 是基于 IEEE802.15.4 的商业应用技术，成本低廉，适用范围非常广泛。可用于工业、家庭和医疗等对数据数率和 QoS 要求不高，但又需要大面积使用无线通信的场合。

目前的 ZigBee 技术已经应用于家庭、工业等场合，完全能够满足用户需求。但是随着物联网的发展，ZigBee 的应用范围和应用领域将日渐广泛，对安全要求也更高。因此需要对 ZigBee 网络的安全性能进行以满足用户和应用场合对安全的需要，使 ZigBee 技术能够更好的应用于物联网领域，提高人们的生产生活水平。

基金项目：国家自然科学基金资助项目（60602005）
作者简介：冯道水（1985-），男，硕士研究生，光网络和物联网. E-mail: fengdaoshui@126.com

1 ZigBee 安全体制

ZigBee 技术的物理层和数据链路层协议主要是采用 IEEE802.15.4 标准，而网络层和应用层由 ZigBee 联盟负责建立。物理层提供基本的无线通信；数据链路层提供设备之间通信的可靠性及单跳通信的链接；网络层负责拓扑结构的建立和维护、命名和绑定服务，它们协同完成寻址、路由及安全这些不可缺少的任务[1]。

ZigBee 协议栈结构如图 1 所示：

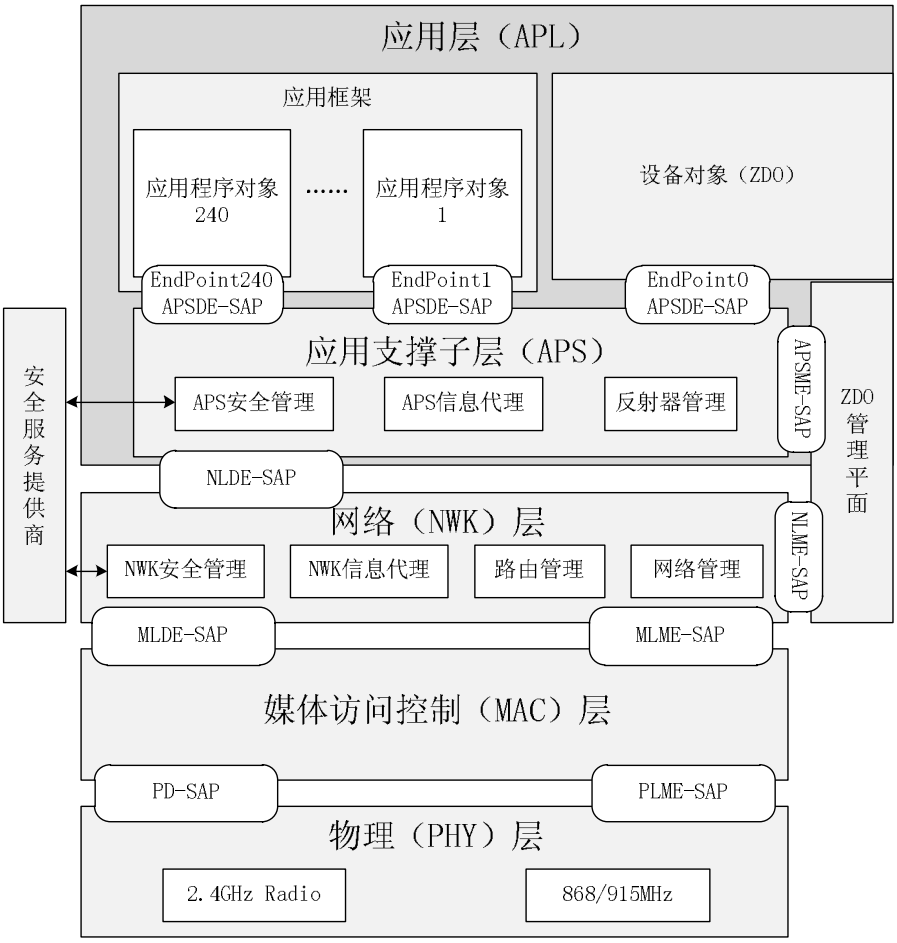

图1 ZigBee 协议栈结构图

从上图可以看出，ZigBee 协议采用的是四层的分层结构，物理层（PHY）和媒体访问控制层（MAC）由 IEEE802.15.4 来指定，网络层（NWK）和应用层（APL）则由 ZigBee Alliance 来进行规范。PHY 层提供基本的物理无线通信能力；MAC 层提供设备间的可靠性授权和一跳通信连接服务；NWK 层提供用于构建不同网络拓扑结构的路由和多跳功能；APL 层包括一个应用支撑子层（APS）、ZigBee 设备对象（ZDO）和应用，ZDO 负责所有设备的管理，APS 提供一个用于 ZDO 和 ZigBee 应用的基础。下面结合 ZigBee 协议栈结构详细说明 ZigBee 的安全机制。

1.1 两种密钥体制

目前加密技术应用广泛，主要可以分为两大类：对称密钥体制和非对称密钥体制[2][3]。

如果一个系统的加密和解密过程中采用的密钥相同，或者虽然密钥不同，但是由其中一个可以很容易得出另一个密钥就说该系统采用的是对称密钥体制。目前广泛应用的对称密钥

算法有 DES、3DES、RC4、RC5 等。

如果一个系统的加密和解密密钥完全不同，且由其中一个无法或者难以推测出另一个密钥，这种系统就是非对称密钥体制。在非对称密钥体制中，密钥是成对出现的，加密密钥和解决密钥，并且可以根据情况把其中一个公开另一个则为私有，因此也称为公钥和私钥。一般来说非对称密钥的使用方式有两种：即公钥加密私钥解密的加密方式和私钥加密公钥解密的验证方式。常用的非对称密钥算法有 RSA、ECC 等。

从这两种密钥体制来看，各有优缺点。对称密钥体制本身比较简单，加密和解密计算速度比较快，容易实现；但是容易被破解，存在着一定的危险性。而非对称密钥体制则由于其计算的复杂而著称，因此计算过程一般比较复杂，实现起来有一定的困难，但是相对于对称密钥体制来说安全性比较高。ZigBee 目前采用的是对称密钥体制，对称密钥体制能够满足目前的应用需要，但是随着物联网的发展和 ZigBee 技术应用范围的越来越广泛，对称密钥体制将不能达到安全要求。

1.2 安全假设

从 1.1 可以看出，在 ZigBee 安全体系结构所提供的安全取决于对称密钥的保管、保护机制的运用以及密钥机制和安全策略的正确执行。因此，在建立 ZigBee 的安全体系结构时，应该满足以下几个假设：

- 所有的协议都正确执行，尤其是安全协议的执行必须正确完整，就是执行与当前协议相关的所有协议都完全正确，且不能有任何遗漏。
- 设备中的随机数产生器正常运行，随机数是产生密钥的原始输入，只有随机数产生器正常才能保证密钥可靠与安全。
- 密钥材料在使用过程中是安全的，即密钥材料不会被非法的获得和使用。

1.3 ZigBee 密钥分类

在 ZigBee 的安全机制中定义了两种不同功能的密钥，一个是连接密钥（Link Key）；另一个是网络密钥（Network Key），它们均是长度为 128 位的对称密钥。

连接密钥应用于应用层（APL）对等实体之间单向通信加密。网络密钥只用于网络内的广播通信加密。设备可以通过密钥建立、密钥传输和预安装等方式来获得连接密钥；可以通过密钥传输或者预安装来获得网络密钥。

1.4 ZigBee 的安全机制

ZigBee 的安全架构涉及到了协议栈的两个层，分别别是网络层（NWK）和应用子层（APS），它们负责安全的传输各自产生的帧。此外，APS 子层提供了建立和维护安全关系的服务，ZDO 设备对象（ZDO）管理一个设备的安全策略和安全配置[4][5]。

1.4.1 分层机制

1) MAC 层

MAC 层负责本层的帧的安全性处理，但是具体的安全决策是由上层来决定。MAC 层根据上层设置安全等级等参数来对本层的帧进行安全处理：包括接发送信息的加密和接收信息的解密，为上层提供通信安全保障。

2) NWK 层

NWK 层负责安全的传输它所产生输出帧和安全接收输入帧所需的处理步骤；或者是根

据更高层的安全属性来对帧进行加密传输，或指示下层进行相应的安全处理。

3) APS 层

APS 层提供了与密钥有关的服务有密钥建立服务、密钥传输服务、请求密钥服务和更换密钥服务四种。

密钥建立服务是用来与通信的目的设备建立即连接密钥所用的。ZigBee 的所有密钥均是由信任中心来负责管理和保存。当源节点向信任中心发起连接密钥建立请求时信任中心计算密钥并利用密钥传输服务把密钥发送给源节点和目的节点。

密钥传输服务一般用来把密钥由信任中心传输给各个节点设备，包括网络密钥和连接密钥。在信任中心收到连接密钥请求或者是网络密钥更新时会使用这项服务功能。当传输网络密钥时会附加一个随机数用来代表这个网络密钥。

请求密钥服务主要用于一个设备向另一个设备请求网络密钥或连接密钥。一般来说这个命令发起于新加入的设备，用于向网络请求网络密钥或者源节点向信任中心请求连接密钥。

更换密钥服务是用来更新网络密钥，密钥传输服务中有一个随机数随着网络密钥一起传输，当需要启用新的网络密钥时信任中心向网络中的所有设备发送更换密钥指令，在指令中附加上代表需要启用的网络密钥的随机数来指明启用哪个网络密钥。

上面的四种密钥服务为 ZigBee 的安全提供了基础，可以完成密钥的建立、传输和更新等功能，为 ZigBee 网络的信息的安全传输提供了保障。但是这些仅仅存在于理论，如果中间出现差错，则不能保障数据的安全。

1.4.2 信任中心

在 ZigBee 网络中，专门定义了一个信任中心，信任中心是一个网络内的设备可以信任的设备，为网络和端到端的应用配置管理分发密钥，也负责网络的建立、运行与维护工作。因此一个 ZigBee 网络中有且只有一个信任中心。一般由协调器自己担当或者由协调器指定。

网络运行的过程中，信任中心负责密钥的分配和管理，包括新设备加入过程中密钥的指定，响应连接密钥请求和计算分配连接密钥，网络密钥的更新等。

2 ZigBee 网络的安全性能分析

从第 1 节的分析可以看出，ZigBee 网络提供了一定的安全解决方案来保障系统安全，但是这种安全是需要前提条件来保证的。ZigBee 的安全假设是所有的协议步骤都已经正确执行而且在网络运行的过程中设备本身是安全的而且在整个网络存在的过程中密钥材料不被泄露。在这个安全假设下 ZigBee 网络是安全的，但是在实际的应用场合中这种安全假设一般是不能满足的，因此 ZigBee 网络的安全性将会大大降低。下面从密钥类型和密钥传输过程详细分析 ZigBee 网络的安全问题[6] [7] 。

2.1 密钥体制分析

由于密钥是由信任中心管理，当源节点设备要和其它设备通信时先向信任中心提出连接密钥建立请求，信任中心接受请求生成密钥，并通过密钥传输服务把密钥同时发送给目的节点和源节点，如图 2 所示。

从密钥体制来看，现有的 ZigBee 网络中虽然使用了分离的连接密钥和网络密钥来提高网络的安全性，但是这两个密钥都是基于对称密钥体制而产生的。而且在连接密钥的使用过程中，一对对称的连接密钥却只能用来对某一对对等实体进行单向的通信加密。当一个设备需要接收多个设备传送来的消息时也需要保存多个密钥材料，根据信息的发送者不同来选择

不同的密钥解密。这就要求目的节点需要保存多个连接密钥，来完成与不同节点的通信。一般来说一个节点即是源节点也同时是其它源节点的目的节点，因此在节点设备中需要保存大量的密钥来完成加密和解密功能。

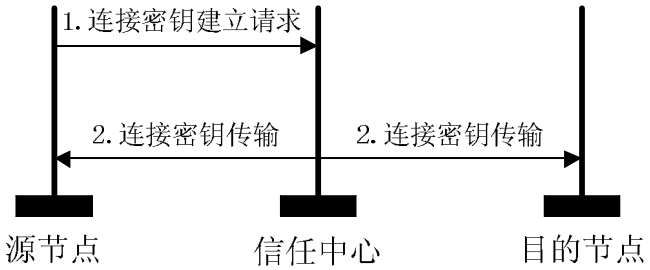

图 2 基于对称密钥的连接密钥请求操作

2.2 密钥分配方式分析

从 ZigBee 网络的密钥的分配方式来看，主要通过两种形式来获得密钥：一是预安装；一是网络传输。预安装是指在设备加入网络之前就把密钥材料安装到设备中，这样设备就可以直接使用密钥加密信息来与网络中的节点设备进行通信，这种方式的优点是密钥材料安全可信，不会产生密钥泄露的问题；但是也存在不足之处，预安装一般是在制造设备的过程中，或者是由信任中心来进行设置，操作过程比较复杂，而且对硬件和技术人员要求比较高，这一点 ZigBee 的低成本、低复杂度的特征相违背，实现难度较大。预安装可以是预装主密钥、网络密钥，甚至是连接密钥。

网络传输是指密钥在新设备加入网络后通过网络传输给新设备。在这种情况下，新设备不可能预先知道网络的安全和密钥安排，无法对密钥传输前的信息包括密钥本身进行任何的加密等安全操作，密钥的传输是明文传输的，如图 3 所示。密钥由信任中心明文传输至新加入设备的过程中可能会经由多跳接力传输，此时是 ZigBee 网络中安全性最脆弱的时候，一旦有密钥被非法设备窃听，这个 ZigBee 网络的安全性就无法保证。

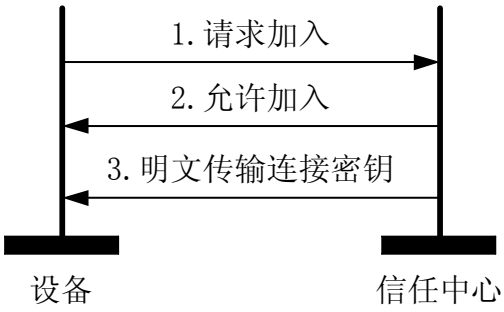

图 3 基于对称密钥的设备加入过程

对于连接密钥来说还有第三种获取方式，这就是密钥建立技术。密钥建立技术是指通过主密钥来接入网络，然后获取连接密钥和网络密钥的技术。这种技术的安全关键在于主密钥的安全。主密钥一般是个人识别码（PIN）、口令、密码等独有的信息，因此安全性和复杂度方面均高于前两种密钥的获取方式。但是对于有些简单的应用场景不需要也没有这些独有信息，因此无法使用主密钥进行密钥建立。

通过上述分析，预安装和密钥传输这两种获取密钥的方式均存在一定的风险。对于预安

装方式来说是操作过程比较复杂；对于密钥传输技术来说是密钥容易泄露，造成安全隐患。

3 安全改进

通过第 2 节的分析可以发现，ZigBee 采用的对称密钥体制需要占用较大的内存空间，而且在加密解密的过程中对密钥的查找会增大传输时延。ZigBee 的密钥分配方式则存在操作过程复杂、对人员要求比较或者密钥容易泄露的问题。

针对上述的问题，需要对 ZigBee 的密钥类型和密钥分配方式进行一定的安全改进，以降低操作要求、增加 ZigBee 网络的安全性和传输质量，满足更高的安全需要，扩大 ZigBee 的应用范围。

3.1 密钥体制的改进

对于网络密钥可以用非对称密钥体制的验证方式来实现，即使用私钥加密、公钥解密。由于私钥是由信任中心自己生成和保管的，因此私钥是不可能泄露，也就不存在非法节点窃听网络密钥然后冒充信任中心的可能性，这样就可以实现所有的网络节点对信任中心的验证功能，从而实现了网络通信的加密和防止非法冒充信任中心的危险。

对于连接密钥，也同样使用非对称密钥，但是与网络密钥不同的是连接密钥使用加密方式，即公钥加密、私钥解密。私钥由目的节点自己保存，而将公钥存储在信任中心对外公开。当某一个节点想与该设备通信时只需要向信任中心提出请求，信任中心则在存储表中查找该节点的加密密钥并发送给请求节点，此时的连接密钥建立过程已经不需要临时生成密钥，所以可以将这一过程重命名为连接密钥如图 4 所示。目的节点在收到信息时只需要用自己的解密密钥来解密即可实现信息的提取。

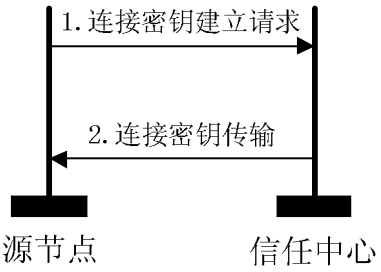

图 4 基于非对称密钥的连接密钥请求操作

经过改进目的节点只需要保存一个解密密钥，解密时也不需要根据源节点再查找密钥，从而节省了存储空间，减少了通信时延；对于信任中心来说也不需要再向目的节点传输对应的密钥从而减少了对无线资源的占用，提高网络的利用率。

3.2 密钥分配方式的改进

针对 2.2 中分析的密钥传输的不安全性和预安装操作的复杂性，对密钥的获取方式在使用非对称密钥的基础上进行相应的改进，这样就可以在降低操作复杂性的同时保证网络的安全性。在设备的加入过程中，密钥会短时间的以明文的方式传输到新加入设备，这样就产生了密钥的泄露问题。在新设备加入网络的过程中，当新加入设备在得到信任中心的确认后加入网络并且得到了网络密钥和信任中心的加密密钥时，新加入的设备可以生成一个随机数当成一个临时密钥，并把临时密钥用信任中心的加密密钥加密后传输给信任中心，信任中心给设备分配设备私有的解密密钥时可以使用这个临时密钥来加密所要传输的密钥，如图 5 所

示。在这一过程中，虽然临时密钥简单，但是临时密钥为单次使用，且只有设备本身和信任中心知道这个临时密钥，所以使用临时密钥来传输设备的解密密钥可以保证密钥的安全性。

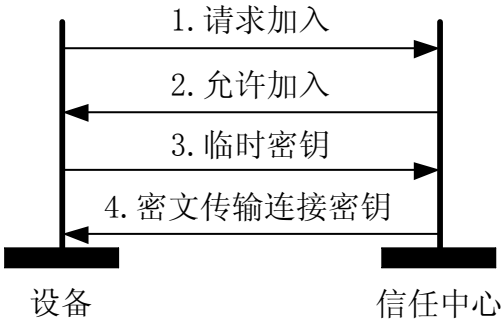

图 5 基于非对称密钥的设备加入过程

经过对密钥分配方式的改进，新设备的加入过程我们可以不使用相对要求比较高的主密钥和预安装方式，而是在设备加入的过程中使用临时密钥加密设备的解密密钥，提高了网络的安全性，降低了网络和设备的复杂度。

4 结论

本文通过对 ZigBee 网络的网络密钥、连接密钥以及两种密钥体制的分析，发现 ZigBee 网络存在安全性问题和对设备复杂度和操作人员知识要求比较高的难题。针对这两个问题分别提出了使用非对称密钥来替代对称密钥、在使用非对称密钥的基础上加入临时密钥使得网络的安全性有大幅的提高，并且在安全性提高的同时减少了密钥的内在占用、降低了网络的复杂度和对操作人员知识的要求，使得 ZigBee 网络更加符合低复杂度、低成本的基本要求，使得网络的适应性得到了提高。本文的主要创新之处在于用非对称密钥代替对称密钥，在设备的接入过程加入临时密钥，经过改进使得 ZigBee 网络的安全性和实用性得到提高，可以适应更宽广的应用场合。

[参考文献]

[1] ZigBee Alliance. ZigBee Document 08006r03-2008. ZigBee-2007 Layer PICS and Stack Profiles[S].
[2] 胡祥义，李岩. 对称密码技术在网络认证系统中的应用[J]. 网络安全技术与应用，2007，3：86~90.
[3] 段晓萍，李燕华. 非对称密码体制 RSA 的原理与实现[J]. 内蒙古农业大学学报，2009，30（1）：304～309.
[4] 李文中，段朝玉. ZigBee2006 无线网络与无线定位实战[M]. 北京：北京航空航天出版社，2008.
[5] 杨斌. 基于 AES 的 ZigBee 标准安全机制分析[J]. 计算机工程与科学，2010，32（7）：42~45.
[6] 吴雨亮. 无线网络信息安全与对策[J]. 安徽电气工程职业技术学院学报，2008，13（1）：102~105.
[7] 任秀丽，于海斌. 基于 ZigBee 技术的无线传感网的安全分析[J]. 计算机科学，2006，33（10）：111~113.