DOI: 10.3976/j.issn.1002-4026.2012.02.013

ZigBee 协议栈的安全体系综述

黄太波[1,3],赵华伟[2,3],潘金秋[1],聂培尧[1],杨泽军[3,4]

(1. 山东财经大学管理科学与工程学院,山东 济南 250014;2. 山东财经大学计算机科学与技术学院,
山东 济南 250014;3. 山东省计算中心,山东省计算机网络重点实验室,山东 济南 250014;
4. 山东师范大学信息科学与工程学院,山东 济南 250014)

摘要:ZigBee 技术作为无线传感网络领域的新兴技术获得广泛应用,其安全性日益重要。本文从现存的 ZigBee 安全体系入手,针对 ZigBee 的安全结构、安全服务、安全模式、安全组件、安全密钥和信任中心以及各层的安全措施展开论述,并具体介绍了 ZigBee 实现安全的步骤,最后提出一种可以提高 ZigBee 安全性的密钥管理方案的新思路。

关键词:ZigBee 技术;无线传感网络;安全结构;信任中心

中图分类号:TN926+.23;TP393.08 **文献标识码**:A **文章编号**:1002-4026(2012)02-0059-08

A survey of security architecture of ZigBee protocol stack

HUANG Tai-bo[1,3], ZHAO Hua-wei[2,3], PAN Jin-qiu[1], NIE Pei-yao[1], YANG Ze-jun[3,4]

(1. School of Managment Science and Engineering, Shandong University of Finance and Economics, Jinan 250014, China;
2. School of Computer Science and Technology, Shandong University of Finance and Economics, Jinan 250014, China;
3. Shandong Provincial Key Laboratory of Computer Networks, Shandong Computer Science Center, Jinan 250014, China;
4. School of Information Science and Engineering, Shandong Normal University, Jinan 250014, China)

Abstract: ZigBee, an emerging wireless sensor network technology, has wide application and its security is increasingly significant. This paper presents its security architecture, security service, security model, security components, security keys and trust center and security policy of each layer. The paper also gives its security implementation steps. The paper eventually proposes a new idea for its key management, which is favorable to its security enhancement.

Key words: ZigBee; wireless sensor network; security architecture; trust center

随着无线通信技术的发展和进步,无线网络取代有线网络的趋势越来越明显。其中,在短距离的无线控制、监测、数据传输领域,ZigBee 技术基于 IEEE802.15.4,工作在 2.4 GHz 的 ISM 频段上,传输速率为 20~25 kb/s,传输距离为 10~75 m,具有低成本、低功耗、低速率、低复杂度的特点和可靠性高、组网简单且灵活的优势,受到更多的关注。目前对于 ZigBee 的使用案例也逐渐增多,因此对其安全通信的研究也提上了日程。

本文对 ZigBee 技术的整个安全体系结构进行了全面剖析,以期能促进其安全技术的进一步发展。

1 ZigBee 技术简介

根据 ZigBee 协议的定义,在网络中有三种逻辑设备类型:协调器,路由器和终端设备,根据性能不同可

收稿日期:2011-10-20

基金项目:国家自然科学基金(60802030);山东省自然科学基金(ZR2011FI027);山东省自然科学基金(ZR2011FM022);山东省博士后创新项目专项资金(201003016)

作者简介:黄太波(1985-),男,硕士研究生,研究方向为信息安全。

分为两种类型的设备[1],一种是全功能设备 FFD(Full Function Device),称为主设备,承担了网络中协调器的功能。如果网络启用了安全机制,网络协调器又可成为 TC(Trust Center)。另一种是简化功能的设备 RFD(Reduced Function Device),称为从设备。它不能作为网络协调者,只能与网络协调器进行通信。根据应用的需求,ZigBee 技术网络有两种网络拓扑结构,即星形拓扑结构和对等的拓扑结构[2],见图 1。

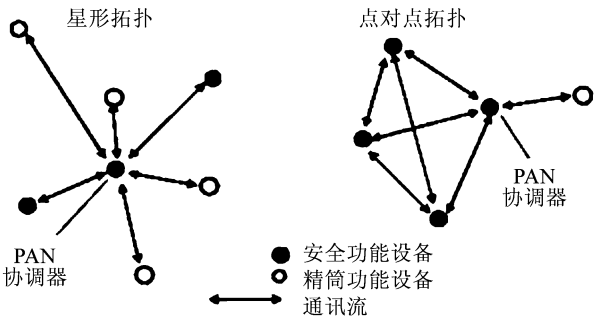

图 1 ZigBee 拓扑结构图

Fig. 1 ZigBee network topology

ZigBee 协议栈由一系列叫做层的模块组成。每一层都为它的上一层提供特定的服务。数据实体提供数据传输服务,管理实体提供所有的其他服务。每一个服务实体通过一个服务接入点(Service Access Point,SAP)为下层提供了接口,并且每一个 SAP 提供了一定数目的服务单元来达到要求的功能[3]。

ZigBee 协议栈共有 4 层,见图 2。PHY 层提供物理无线设备的基础通信能力;MAC 层提供在设备之间可靠的、单跳通信链路服务;NWK 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;APL 包括应用支持子层(APS)、Zigee 设备对象(ZDO)和应用软件;ZDO 负责整个设备的管理,APS 提供对 ZDO 和 ZigBee 应用的服务[4-5]。

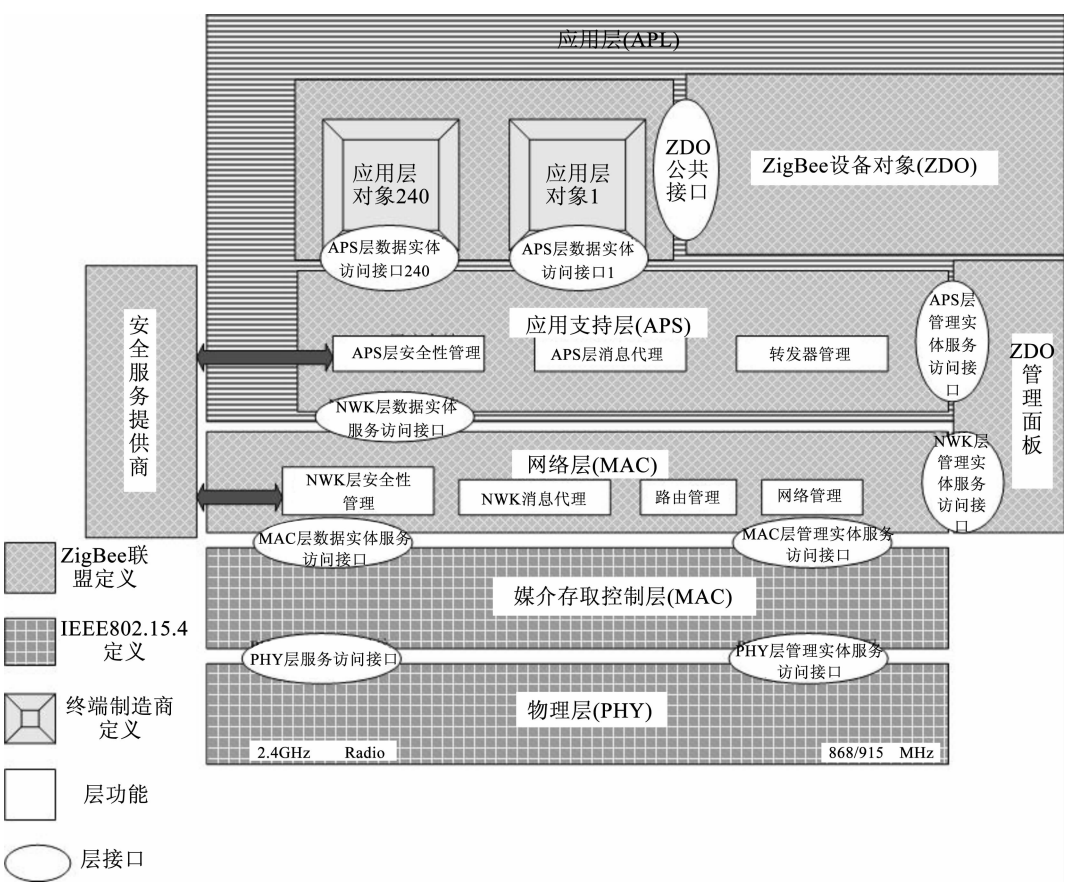

图 2 ZigBee 协议栈架构图

Fig. 2 Architecture map of ZigBee protocol stack

2　ZigBee 的安全要素

2.1　安全服务

IEEE 802.15.4 标准规定了 ZigBee 协议栈的 MAC 层可以提供设备之间基本的安全服务和互操作。其中,基本的安全服务包括维护一个接入控制列表(Access Control List, ACL),以及使用对称加密算法保护传输的数据[6]。MAC 的上层决定 MAC 层是否使用安全措施,并提供该安全措施所必须的关键资料信息。此外,上层还负责对密钥的管理、设备的鉴别以及对数据的保护、更新等。其主要的安全服务有:

(1)接入控制:每个设备通过维护一个接入控制表(ACL)来控制其他设备对自身的访问。

(2)数据加密:采用基于 128 位 AES 算法的对称密钥方法保护数据。在 ZigBee 协议中,信标帧净载荷、命令帧净载荷和数据帧净载荷要进行数据加密。

(3)数据完整性:数据完整性使用消息完整码 MIC(Message Integrity Code),可以防止对信息进行非法修改。

(4)序列抗重播保护:使用 BSN(信标序列号)或者 DSN(数据序列号)来拒绝重放的数据的攻击[2-3]。

2.2　安全模式和安全组件

MAC 层允许对数据进行安全操作,但是并不是强制安全传输,而是根据设备的运行模式及所选的安全组件,对设备提供不同的安全服务。ZigBee 协议栈中提供了 3 种安全模式[4]:

(1)非安全模式:在 MAC 层中,该模式为缺省安全模式,不采取任何安全服务;

(2)接入控制(ACL)模式:这种模式仅仅提供接入控制,作为一个简单的过滤器只允许来自特定节点发来的报文;

(3)安全模式:同时使用接入控制和帧载荷密码保护,提供了较完善的安全服务[7]。只有在该模式下,才使用 2.1 中所提及的 4 种安全服务,并使用表 1 提及的安全组件。

安全组件的标识包括对称密钥算法、模式以及完整性校验码的长度等信息。ZigBee 的安全机制是在 MAC 层实现的,应用程序通过在协议栈中设置恰当的参数调用某一级别安全组件,默认为无安全措施。IEEE802.15.4 提供了 8 种可选的安全组件[8],应根据需要选择安全组件中的任意 1 种,每个安全组件提供不同类型的安全属性和安全保证,见表 1。

表 1　ZigBee 安全组件表

Table 1　The table of ZigBee security components

标示符	安全级别子域	安全组件	安全属性	安全服务				数据完整性
				接入控制	数据加密	帧完整性	序列更新(可选)	
0x00	000	None	无					M=0
0x01	001	AES-CTR	ENC	X	X		X	M=0
0x02	010	AES-CCM-128	ENC-MIC-128	X	X	X	X	M=16
0x03	011	AES-CCM-64	ENC-MIC-64	X	X	X	X	M=8
0x04	100	AES-CCM-32	ENC-MIC-32	X	X	X	X	M=4
0x05	101	AES-CBC-MAC-128	MIC-128	X		X		M=16
0x06	110	AES-CBC-MAC-64	MIC-64	X		X		M=8
0x07	111	AES-CBC-MAC-32	MIC-32	X		X		M=4

注:M 代表 MIC 的字节数,MIC 字节数越长,攻击者成功伪造 MAC 的可能性越小。“X”表示该安全组件可以提供此项安全服务。

3　ZigBee 安全密钥和信任中心

3.1　安全密钥

ZigBee 设备在网络中利用一个 128 位的对称密钥提供安全服务,其中在数据加密过程中可以使用 3 种基本密钥[9]:主密钥(Mast Key,MK)、链接密钥(Link Key, LK)和网络密钥(Network Key, NK)。MK 用来建立密钥并且为网络中的设备两两共享,是 2 个设备长期安全通信的基础,也可以作为一般的 LK 使用。所以,必须维护主密钥的保密性和正确性。LK 是为网络中的 2 个设备共享,用来保证一组应用层对等实体间的单播通信的安全,可以应用在 MAC、NWK 和 APL 层[10]。LK 在高安全模式(High Security, HS)中用作安全服务(例如密钥传输鉴权等服务)的基础。NK 为网络中所有设备共享,用来保护一个网络中的广播通信。NK 在标准安全模式(Standard Security, SS)中用作安全服务(例如鉴权和帧安全服务)的基础。LK 和 NK 都不断地进行周期性更新(高安全模式下)。因此在高安全模式下,TC 的内存是要随着网络中设备数目的增加而不断增大的,但是在标准安全模式下却不是这样的。当 2 个设备同时有 LK 和 NK 时,采用 LK 通信。虽然存储 NK 的开销小,但是降低了系统的安全性,不能阻止内部攻击[11]。预期的接收者都知道保护帧中的密钥类型。

安全密钥可以通过多种方式获得,不同类型的密钥获得方式不同,见表 2。密钥传输是指网络中的 TC 发送密钥给设备。基于一个预共享密钥(MK)的密钥建立方法可以用来建立一对两个设备共享的密钥。预安装是指在设备加入网络前就获得了密钥。

在 ZigBee 中,NK 有两种类型,即标准(SNK)和高安全(HSNK)[12]。NK 的分发和帧计数器的初始化依赖于 NK 的类型,但是这两种类型的 NK 都以同样的方式保护数据。安全密钥在不同层和不同安全模式下的可用性见表 3。一些密钥类型对于一些安全模式来说是可选的,在表中都用“O”作了标注。此外所有的层必须共享主动网络密钥和相关联的接收帧计数器或者发出帧计数器。

为了在不同安全服务中避免密钥的重用,从 LK 中生成不同的密钥是必需的。可以利用 LK 单向函数得到无关联密钥,这样可以使得不同安全协议的执行在逻辑上分开。三种类型的安全密钥可以从 LK 中派生出来,如表 4 中列出的情况。除了数据密钥,其他密钥都需要对应于消息验证码的密钥哈希函数的计算而派生得到。所有派生出的密钥都必须共享联合帧计数器。

表 2 密钥的获得方法

Table 2 Key acquirement schemes

获得方法\密钥类型	NK	MK	LK
密钥传输	是	是	是
密钥建立	否	否	是
预安装	是	是	是

表 3 安全密钥的可用性

Table 3 Availability of key types

密钥	层		模式	
	网络层	应用层	安全模式	高安全模式
网络密钥	YES	YES	YES	YES
主密钥	NO	YES	NO	YES(O)
链接密钥	NO	YES	YES(O)	YES(O)

表 4 密钥派生方式

Table 4 Derived key types

密钥类型	派生方式	用途
密钥传输密钥	$HMAC(0x00)_{LK}$	保护传输的 NK
密钥装载密钥	$HMAC(0x02)_{LK}$	保护传输的 MK 和 LK
数据密钥	LK	和 LK 相同作用

注:1. HMAC:密钥 HASH 消息鉴权机制 2. 0x00/0x02 指在链路密钥之下带有输入字符串”0x00”或者”0x02”

3.2 信任中心

在每一种 ZigBee 网络的安全应用中,必有一个网络中的设备都必须信任的信任中心(Trust Center, TC)[10]。TC 作为网络中的一部分,负责密钥分发和端对端的应用配置管理。在高安全模式(商业模式),应用设备都用 MK 来初始化与 TC 的安全通信,而在标准安全模式下,则用 NK。在表 2 各种密钥获得方法的对比中,可知 MK 和 NK 都可以通过预安装

表 5 密钥的分发

Table 5 Key distribution

目的	设备从 TC 接收内容	途径
信任管理	初始 MK 或者活跃 NK	不安全密钥传输
网络管理	初始活跃 NK 或更新的 NK	安全密钥传输
配置管理	MK 或 LK	安全密钥传输

或者通过一种叫做带内不安全密钥传输的方式获得。毫无疑问,后一种选择在不安全环境中是不可以接受的。在表 5 中给出了 ZigBee 设备和 TC 在不同目的中的相互操作。TC 不是一种设备类型,而是一种应用,一般由协调器充当。

在 ZigBee 协议栈版本(ZigBee PRO)中还定义了两种安全模式:高安全模式(High Security, HS)和标准安全模式(Standard Security, SS),在标准安全模式或高安全模式中,TC 是否配置为操作状态是可选的[9]。标准安全模式设计为居住应用。在这种模式下,TC 维护 SNK 和控制网络准入政策。高安全模式设计为商业应用,在这种模式下,TC 需要维护网络中所有设备的列表(在标准安全模式下这一应用是可选的)、所有的相关密钥(MK、LK 和 HSNK)和控制网络准入政策。此外,在高安全模式下,对称密钥密钥交换协议和多实体鉴权要强制实现[12]。

3.3　ZigBee 密钥管理的不足

目前大多数 ZigBee 应用的密钥有 NK 和 LK,若使用 NK,虽然可以节省节点的存储资源,但是当某一节点被捕获后,整个网络就会受到威胁。若使用 LK,当网络中某一节点被捕获后,只有很少一部分节点受影响,但是增加了系统开销。无论采用预置的方式,还是采用基于 MK 的密钥传输方式,密钥都存在着很大的泄露风险。

当今 ZigBee 技术的主流应用的密钥管理仍然是采用对称密码体制,因为对称密码体制的局限性,使得 ZigBee 的安全性得不到明显的提升。虽然非对称密码体制的引入可以大大提高 ZigBee 的安全性,但是又因为其对资源的要求较高而得不到大规模的应用。将对称密码体制和非对称密码体制结合起来,应用于 ZigBee 的密钥管理中可以得到一个比较好的资源和安全的均衡,所以提出一个可以将两种加密体制完美结合的密钥管理方案是亟待解决的问题。

总之,一个安全系统的强度取决于其最弱的一环。ZigBee 最弱的一环在于安全密钥在所有设备中的分发和存储[10]。因此密钥管理方案的完善与否决定了 ZigBee 的安全强度,也就在很大程度上决定了其使用范围。

4　ZigBee 的安全实现

4.1　共同安全因素

ZigBee 协议栈实现安全保护,有些用了很多的安全相关特征,如 NWK 层和 APS 层都用的辅助帧头、安全参数和执行方针等。

4.1.1　辅助帧头

辅助帧头包括一个安全控制域、一个帧计数器域、源地址域和密钥序列数域。安全控制域由安全级别子域、密钥识别符、延长现时和保留域组成。辅助帧头的帧计数器可以提供帧刷新功能,预防帧重发。安全级别子域的安全级别标识符显示了使用哪个安全组件来保护输出帧和输入帧,表 1 中列出了安全级别子域的可用安全组件。

4.1.2　安全参数

ZigBee 的帧保护机制使用 AES-128,CCM* 安全操作模块。CCM* 模式是 CCM 模式的拓展,既包含 CCM,又可单独使用 CTR 和 CBC-MAC 模式来实现加密或者鉴权。最主要的是 CCM* 模式对于所有CCM* 安全级别只使用一个密钥,就是说,由于 ZigBee 使用 CCM* 模式,MAC、NWK 和 APL 层可重复使用相同密钥[9]。

CCM* 现时输入用于 CCM* 模式的加密和鉴权传输,也用于 CCM* 加密和鉴权校验传输。表 6 说明了 CCM* 现时子域的顺序和长度。现时的安全控制域和帧计数器域应与正在处理的帧的辅助帧帧头的

表 6　CCM* 现时子域的顺序和长度

Table 6　The sequence and size of CCM* nonce

字节:8	4	1
源地址	帧计数器	安全控制

安全控制域和帧计数器域相同。现时的源地址域设置为发起帧安全保护的设备的延长 64bit MAC 地址。当辅助帧中的延长现时子域为 1 时,发起帧安全保护的设备的延长 64bit MAC 地址将与正在处理的帧的辅助帧帧头的源地址域保持一致[9]。

4.2 MAC 层安全

MAC 层负责自身的安全进程,而上层应决定使用哪个安全级别。

在 ZigBee 网络中,应根据 MAC 个域网信息库(Personal area network Information Base, PIB)中的 macDefaultSecurityMaterial和 macACLEntryDescriptorSet 两个参数的安全资料对安全进程进行处理。上层(如应用层)应将 macDefaultSecurityMaterial 的值与来自 NWK 层的共享邻居设备的 APS 的 LK 密钥的值一致,设置 macACLEntryDescriptorSet 的值与来自 NWK 层的主动网络密钥、计数器的值一致。安全组件应该为 CCM*,安全级别应该为 NIB 中的 nwkSecurityLevel 标识的值。

对于 MAC 层,LK 密钥应该是首选,如果未能获得,则应用缺省密钥(即:macDefaultSecurityMaterial 标识的值)。

4.3 NWK 层安全

NWK 层为 MAC 层的正确操作提供保障,为 APL 层提供合适的服务接口。当一个 NWK 层帧需要安全保护时,NWK 层利用带有 CBC-MAC 操作模式的增强计数器中的 AES 加密和鉴权保护帧安全。上层(例如:应用层)通过设置安全密钥,帧计数器和安全级别来控制安全进程操作。

安全 NWK 层帧格式见表 7,辅助帧帧头位于 NWK 帧头和净载荷域之间。表中的安全 NWK 净载荷不是必须要是一个加密的净载荷,只是进行了完整性保护。安全级别域可以是表 1 中的任意一个。NWK 层输入帧和输出帧的安全操作见表 8。

表 7 安全 NWK 层帧格式

Table 7 Secured ZigBee NWK layer frame form

字节:可变	14	可变的
源 NWK 帧头	辅助帧帧头	加密净载荷 加密信息完整性码(MIC) 安全帧净载荷 = CCM* 的输出
整个 NWK 帧头		安全 NWK 净载荷

表 8 NWK 层输入输出帧安全操作

Table 8 Security operation of NWK layer input and output frame

输出帧保护	输入帧保护
1. 从 NWK 中的 NIB 中检索主动 NK,输出帧计数器,密钥序列数和安全级别等属性参数。 2. 用 1 中的参数设置辅助帧帧头。 3. 利用下面参数进行 CCM* 操作模式的加密和鉴权,参数:MIC 的长度(从安全级别中获得),NK 和 CCM* 现时(CCM* 现时用辅助帧帧头中的值,组成如下形式:源地址 ‖ 帧计数器 ‖ 安全控制)。 4. 根据加密条件,构成输出帧。 5. 增加 NIB 中输出帧计数器的值。 6. 设置辅助帧头安全级别子域为"000"。	1. 判断来自 NIB 中的安全级别,并且重写到安全级别子域中。 2. 判断来自辅助帧帧头中的密钥序列数,发送地址和接受帧计数器。 3. 从 NIB 中获得与密钥序列数相对应的安全资料,如果接受帧计数器比帧计数器小,则丢掉。 4. 利用与输出帧一样的参数执行 CCM* 模式加密和鉴权。 5. 设置帧计数器为:接受帧计数器 +1,将帧计数器和发送地址存入 NIB 中。

注:表中的 ‖ 表示级联。

4.4 APL 层安全

4.4.1 APL 帧安全

APS 帧格式由 APS 帧头和 APS 负载域组成。APS 帧头包括帧控制域和地址域。当一个安全策略应用到一个 APDU 时,APS 帧控制域的安全子域设置为 1,用来标识辅助帧帧头的存在。安全 APS 帧格式与安全 NWK 帧(表 7)的格式相同。APS 层输入输出帧的安全操作见表 9。

表 9　APS 层输入输出帧安全操作

Table 9　Security operation of APS sub-layer input and output frame

输出帧保护	输入帧保护
1. 获得密钥标识符,从 NIB 或 AIB 中获得安全资料。如果密钥标识符为主动 NK,APS 层或 NWK 层将应用安全策略(不是两者都用)。 2. 从安全资料中提取输出帧计数器(如果密钥标示符标识为主动 NK,也提取密钥序列数)。 3. 从 NIB 中获得安全级别,根据得到参数设置辅助帧帧头。利用下面参数进行 CCM* 操作模式的加密和鉴权,如下形式组成CCM* 现时:CCM* 现时用辅助帧帧头中的值,组成如下形式:源地址 ‖ 帧计数器 ‖ 安全控制)。 4. 根据加密条件,构成输出帧。 5. 增加 NIB 中输出帧计数器的值。 6. 设置辅助帧头安全级别子域为“000”。	1. 判断来自辅助帧帧头的序列数,密钥标识符和输入帧计数器值。 2. 根据密钥标识符从 NIB 或 AIB 中获得相应的安全资料。如果输入帧计数器比帧计数器小,则丢掉。 3. 判断来自 NIB 中的安全级别,并将其重写到安全级别子域中。 4. 利用与输出帧一样的参数执行 CCM* 模式加密和鉴权。 5. 利用 CCM* 模式的输出结果构成不安全的 APS 帧。 6. 设置帧计数器为:接受帧计数器 + 1,将帧计数器和发送地址存入 NIB 中。

注:表中的 ‖ 表示级联

4.4.2　APS 子层安全

(1)密钥建立:APSME(应用支持子层管理实体)提供允许两个设备相互建立 LK 的服务,初始信任信息(如 MK)必须在运行密钥建立协议之前安装在每一个设备里;

(2)密钥传输服务:通过安全或者非安全的方式为设备传输 NK、LK 或者 MK;

(3)设备更新服务:当 ZigBee 路由器的一个节点设备发生状态改变(如:加入或者离开网络)时,为其提供安全的方式将设备状态改变的消息通知 TC(信任中心);

(4)设备移除服务:为 TC 提供安全的方式,通知路由器其一个子设备需要移除网络;

(5)请求密钥服务:为一个 ZigBee 设备提供安全的方式从另一个设备(如:TC)请求获得一个主动 NK 或者一个端到端应用 MK;

(6)交换密钥服务:为 TC 提供安全的方式通知一个设备交换相互的 NK。

4.5　安全进程

安全的实现进程包括加入安全网络、鉴权、NK 更新、端对端应用密钥建立和离开网络。其需要的安全服务是由以上提到的所有安全操作共同配合完成的。我们设想出的在一个网络中的安全进程[8],见图 3。

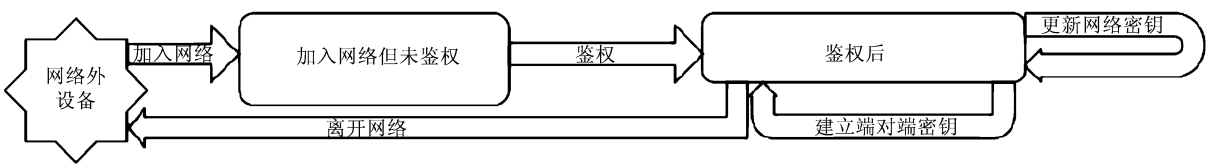

图 3　安全进程图

Fig. 3　Security procedures of ZigBee

5　结语

ZigBee 是一项新兴的短距离无线通信技术,在继承 IEEE802.15.4 的基础上,又采用了诸多的安全体制和安全措施,例如:AES-128 加密算法、CCM* 操作模式、TC 等。但是 ZigBee 因为其自身的内存小、易被捕获的特点,仍然存在一些安全隐患,例如密钥管理问题、安全定位问题、安全路由问题等。通过对 ZigBee 的安全体系的论述可以得出,提出一种恰当的引入一个参数(例如躯感网中引入的 PV)的两种加密体制组合使用的密钥管理方案可以大大提高 ZigBee 的安全性,拓宽 ZigBee 的使用范围。

参考文献:

[1]KINNEY P. ZigBee technology:Wireless control that simply works[DB/OL]. [2011 -07 -12]. https://docs. zigbee. org/zigbee -docs/dcn/03 -1418. doc.

[2]蒋挺,赵成林. 紫峰技术及其应用(IEEE 802. 15. 4)[M]. 北京:北京邮电大学出版社,2006.

[3]ZigBee Alliance,Inc. ZigBee Specification,ZigBee Document 053474r06 ,Version 1. 0[EB/OL]. (2005 -06 -27) [2011 -08 -12]. http://www. nd. edu/ ~mhaenggi/ee67011/zigbee. pdf.

[4]金纯,罗祖秋,罗凤,等. ZigBee 技术基础及案例分析[M]. 北京:国防工业出版社,2008.

[5]任秀丽. 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.

[6]徐小涛,高泳洪,章炜,等. 基于 IEEE802. 15. 4 的 ZigBee 无线网络数据传输安全的研究与探讨[J]. 信息网络安全, 2009 (6): 10 -12.

[7]徐健,李小珉. ZigBee 的 MAC 层安全研究[J]. 网络与通信, 2009(18): 36 -42.

[8]孙静. ZigBee 网络安全性分析[J]. 电脑与电信, 2010(11): 38 -40.

[9]ZigBee Alliance. ZigBee Specification , Document 053474r17[EB/OL]. (2008 -01 -17) [2011 -08 -12]. http://people. ece. cornell. edu/land/courses/ece4760/FinalProjects/s2011/kjb79_ajm232/pmeter/ZigBee%20Specification. pdf.

[10]HYNCICA O, KACZ P, FIEDLER P, et al. On security of PAN wireless systems[J]. LNCS, 2006(4017): 178 -185.

[11]覃志松,黄廷磊. ZigBee 无线传感器网络安全研究及改进[J]. 微计算机信息,2010(8):53 -54.

[12]YUKSEL E, NIELSON H R, NIELSON F. ZigBee-2007 security essentials[C]//Proceedings of the 13th nordic workshop on secure IT systems. Denmark: DTU Informatics ,2008 : 65 -82.

[13]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(7): 42 -45.

[14]ZHOU Y, LING Z, WU Q. ZigBee wireless communication technology and investigation on its application[J]. Process Automation Instrumentation, 2005(6): 5 -9.

[15]周公博, 韩振铎, 胡宁宁. ZigBee 标准的密钥协商机制分析[J]. 电子技术应用, 2007(10): 158 -160, 164.

[16]胡江. Zigbee 无线传感器网络安全性分析[J]. 科协论坛, 2007(9): 103.

[17]吕治安. ZigBee 网络原理与应用开发[M]. 北京:北京航空航天大学出版社, 2008.

[18]聂晓培. ZigBee 标准的安全服务体系结构分析[J]. 网络安全技术与应用, 2009(1): 43 -45.

[19]虞志飞, 邬家炜. ZigBee 技术及其安全性研究[J]. 计算机技术与发展, 2008(8): 144 -147.

[20]杨斌. 基于 TC 和 AES 的 ZigBee 标准安全性分析[J]. 计算机工程与设计, 2010 (11): 40 -43.

[21]VENKATASUBRAMANIAN K K,GUPTA S K S. Security for pervasive health monitoring sensor applications[EB/OL]. [2011 -08 -09]. http://www. cis. upenn. edu/ ~vkris/papers/ICISIP2006. pdf.