智能家居无线数据的安全传输①

沈永增 杨利亚 (浙江工业大学 信息工程学院 浙江 杭州 310014)

摘 要： 研究了基于 ZigBee 智能家居无线数据的安全传输问题，在简单介绍 ZigBee 技术安全结构和加密算法模式的基础上，通过分析 ZigBee 安全服务特征、数据传输类型，结合智能家居本身的特点来建立安全网络，并对数据进行加密，实现数据安全传输，从而保证智能家居数据的机密性。

关键词： 智能家居；安全；ZigBee；加密；无线数据

Security Transmission of Smart Home Wireless Data

SHEN Yong-Zeng, YANG Li-Ya

(College of Information Engineering, Zhejiang University of Technology, Hangzhou 310023, China)

Abstract: This paper studies the security transmission of Smart Home wireless data based on ZigBee. It briefly introduces ZigBee security structure and encryption algorithm mode, and analyzes the characteristics of ZigBee security service and the mode of data transmission. In view of smart home's characteristics, it sets up a security network. Finally, it achieves data security transmission by encrypting, thus ensuring the confidentiality of smart home data.

Keywords: smart home; security; ZigBee; encrypt; wireless data

1 引言

随着 ZigBee 无线传感器网络技术的发展及智能家居的普及，人们享受着智能家居无线网络带来的便利。但是由于无线网络是“开放”的，只要知道通信频率、调制及编码方式等，任何外界设备都可以收到网络设备发送的数据，同时也可以向这些设备发送数据，因此网络很容易受到外界的攻击。同时，智能家居数据的传输也要保证完整性、机密性，所以智能家居网络中数据的安全传输的研究显得攸关重要。

2 ZIGBEE安全性能

2.1 ZigBee 协议栈

在 ZigBee 网络体系结构中，最低两层(PHY、MAC)使用 IEEE 802.15.4 标准，建立在它们之上的是 ZigBee 联盟负责定义的 NWK 和 APL 层。PHY 层提供最基本的无线通信能力；MAC 层提供设备间单跳和可靠的链路；NWK 层提供多跳、有路由能力的功能，以建立不同拓扑结构网络；APL 层包括应用支持子层(APS)、ZigBee 设备对象(ZDO)和应用程序，APS 为 ZDO 和应用程序提供服务，APL 提供应用程序和 ZDO 密钥的建立、传输、和设备管理服务。ZigBee 安全体系结构使用 IEEE 802.15.4 的安全服务，利用这些安全服务对传输的数据进行加密处理，并提供对接入网络的设备的身份认证、密钥管理等功能。ZigBee 网络体系结构中的 MAC、NWK、APS 都包含该安全体系，它们负责各自帧的安全传输。此外，APS 还提供安全关系的建立和维护，ZDO 负责管理设备的安全策略和安全配置。

2.2 ZigBee 加密算法模式

Zigbee 的 MAC 层使用高级加密标志(AES)的算法进行加密的，算法中采用 128 位的块作为参数，密钥长度也选为 128 位。并按照 IEEE 802.15.4 协议和 Zigbee 扩充的方式进行，来保证 MAC 层帧的机密性、一致性和真实性。MAC 层负责自己的安全处理，

① 基金项目:科技厅面上项目(2007C30008)
收稿时间:2009-11-30;收到修改稿时间:2010-01-01

但其上层能决定其采用的安全级别。Zigbee 提供了一个基于 128 位 AES 算法的安全方案，该方案共定义了 7 种安全套件[1]。其中 CCM-128 和 CBC-MAC-128 支持 128bit 的分组和密钥长度[2]。

MAC 层的安全性有三种模式：利用了 AES 进行加密的 CTR 模式(Counter mode)、利用了 AES 保证一致性的 CBC-MAC 模式(Cipher Block Chaining 密码分组链接)，以及以上两者均使用的 CTR 和 CBC-MAC 模式，被称为 CCM 模式。ZigBee 技术对数据的安全保护是在 CCM*模式下执行 AES-128 加密算法，CCM*模式是 CCM 模式的一种变形，它保留 CCM 模式的所有特点，同时允许不同的安全级别使用同一个密钥。和 CCM 模式相比较，CCM*模式只需要一个密钥，并且可以安全地用于使用可变长度的验证标签的执行环境。CCM*模式的具体实现过程可以参考文献[3]。

3 安全密钥

Zigbee 技术在数据加密过程中，可以使用主密钥、链接密钥、网络密钥这三种基本密钥。主密钥是两个设备长期安全通信的基础，因此必须维护主密钥的保密性和正确性。它可以通过生产厂家预先配置、信任中心设置或是由用户输入(如输入 PIN，口令)得到。链接密钥是网络中两个设备间建立共享的密钥，可以使用主密钥通过密钥建立命令获得，也可以在制造设备时由生产厂家预先配置。网络密钥可以通过信任中心设置、生产厂家预先配置等方法等到。

网络中设备之间的安全是建立在链路密钥和网络密钥之上的。网络密钥可以用在 MAC、NWK、APL 层三个不同的层，因此同一个网络密钥及与其相关的接收、发送帧的计数器可以在这些不同的层中使用。但是链路密钥和主密钥仅能被 APL 子层使用。

4 信任中心

信任中心是负责发布密钥，实现网络或者端对端的应用配置管理的设备，它允许设备加入网络，并分配密钥，从而确保设备间端到端的安全性。ZigBee 网络中必须有一个信任中心，信任中心可以由协调器担任，也可以由协调器指定某一设备担任，信任中心被网络中的所有设备所信任和识别。

信任中心有两种模式：住宅模式和商用模式[4]。商用模式安全性能较高，需要维护钥匙并允许更新，具有良好的扩展性，但是信任中心对设备储存器的需求随着网络中设备数量的增长而增长。而在住宅模式下，信任中心对设备储存器的需求不会随着网络设备数量的增长而增长，不需要设置钥匙，但其网络的扩展性不好。在用于如家庭这一类场合时，ZigBee 可以采用低安全模式[5],所以这里我们选用住宅模式。

5 智能家居数据安全传输的实现

5.1 数据传输类型

ZigBee 技术的数据传输模式分为 3 种数据传输事务类型：第 1 种是从设备向主协调器发送数据；第 2 种是主协调器发送数据，从设备接收数据；第 3 种是两个从设备之间传送数据[3]。在本论文中，我们研究的智能家居网络采用的是星型网络拓扑结构，此结构中只允许在主协调器和从设备之间交换数据，所以，这里我们只需考虑前面两种数据传输事务类型。

5.2 ZigBee 安全网络的建立

在智能家居中，协调器成功建立网络后，还需要通过设置才能建立安全的 ZigBee 网络。协调器通过设置 NIB 属性 nwkSecurityLevel 实现安全级别的配置，通过 AIB 属性 apsTrustCenterAddress 设置信任中心的地址[5]。这里选用协调器作为信任中心，因此设置的信任中心地址就是协调器的地址。选用了住宅模式，还需要把 NIB 属性 nwkAllFresh 设置为 FALSE。这样一个安全的 ZigBee 网络建立好后，新设备要加入此网络，首先发送 NLME-NETWORK-DISCOVERY.request 原语，开始执行主动或被动扫描。在扫描的过程中，新连接设备接收到协调器发送的信标，获得网络的信息，新设备再发送 NLME-JOIN.request 原语与网络建立连接。如果新加入设备已经知道网络密钥，则将命令帧加密后发送出去。协调器接收到请求连接的命令帧后，其 MAC 层发送 NLME-ASSOCIATE.indication 原语到 NWK 层，NWK 层再将连接请求发送到 ZDO。此后，协调器向新连接设备发送连接响应命令，新连接设备接收到连接响应命令后，就向上层发送连接确认原语。新连接设备加入一个安全网络后，要进行认证，住宅模式下认证过程如图 1 所示。

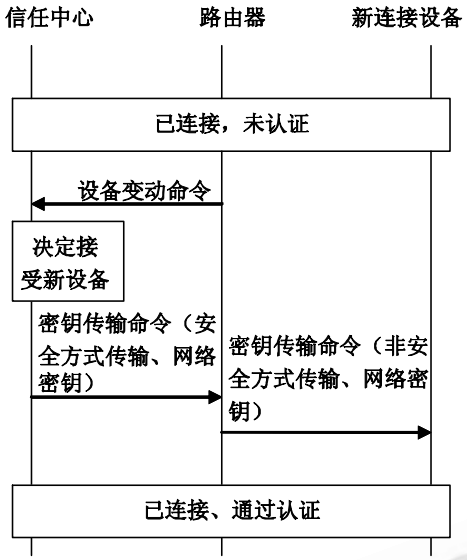

图 1 住宅模式下的认证过程

在安全网络中，如果到了预先规定的时间，新连接设备仍没有通过认证，该设备就将从网络中被移除。新连接设备一旦通过了认证，其在发送网络层帧时总是进行安全处理，除非是与一个已经接入但没有通过认证的设备进行通信。

5.3 数据安全传输实现

在本文中，ZIGBEE 无线模块采用的是 CC2430 无线收发芯片。CC2430 数据加密/解密是由支持高级加密标准 AES 的协处理器完成的。有了 AES 协处理器的加密/解密操作，极大地减轻了 CC2430 内置 CPU 负担，也使得 AES 的安全方案得以轻松实现。

AES 协处理器与 CPU 之间通信的实现主要利用三个 SFR 寄存器：ENCCS(加密控制和状态寄存器)、ENCDI(加密输入寄存器)、ENCDO(加密输出寄存器)，其中状态寄存器 ENCCS 通过 CPU 直接读/写，而输入/输出寄存器必须使用储存器直接存取(DMA)。AES 控制寄存器 ENCCS 的功能描述如表 1 所示。AES 协处理器是各个层次共享的通用源，但是每次只能处理一个实例，所以需要在软件中设置某些标签来安排这个通用源[6]。AES 协处理器的加解密操作流程如图 2 所示。DMA 通道中一个用于数据输入，另一个用于数据输出。在开始命令写入寄存器 ENCCS 之前，DMA 通道必须初始化。根据表 1 所示，寄存器 ENCCS[1:0]输入不同的代码，执行不同的命令，设置寄存器 ENCCS 的 CMD[1:0]为 10，通过 DMA 操作将准备好的 Key 装入 AES 协处理器中。设置寄存器 ENCCS 的 CMD[1:0] 为 11，通过 DMA 操作将准备好的 IV/Nonce 装入 AES 协处理器中。使用 DMA 方式进行数据传输时，数据从 DMA 通道传送数据到 AES 协处理器，需设置 ENCDI 为目的寄存器，而要使 DMA 通道从 AES 协处理器接收数据，就要设置 ENCDO 为源寄存器。寄存器 ENCCS 的 MODE[2:0]中输入不同的代码，就采用不同的加解密的模式，具体如表 1 的 MODE 栏所示。这里 AES 协处理器选用 CCM 模式进行加密与认证，CCM 是 CTR 与 CBC-MAC 的结合。一般来说，首先利用 CBC-MAC 对报文头部和内容提供完整性保护，然后利用 AES-CTR 模式对数据部分和 MAC 进行加密[7]。

表 1 寄存器 ENCCS 的功能描述

位	7	6:4	3	2:1	0
名称	-	MODE[2:0]	RDY	CMD[1:0]	ST
复位	0	000	1	00	0
读写		R/W	R	R/W	R/W
描述	没有使用	加密/解密模式： 000:CBC; 001:CFB 010:OFB; 011:CTR 100:ECB;101: CBC-MAC 110,111 不使用	状态显示： 0:加密、解密正在进行； 1:完成	当 1 写入 ST 时执行命令； 00:加密 01:解密 10:装密钥 11:装入 IV/Nonce	开始执行命令：每个命令或数据块应该分别下达，由硬件自动清除该位

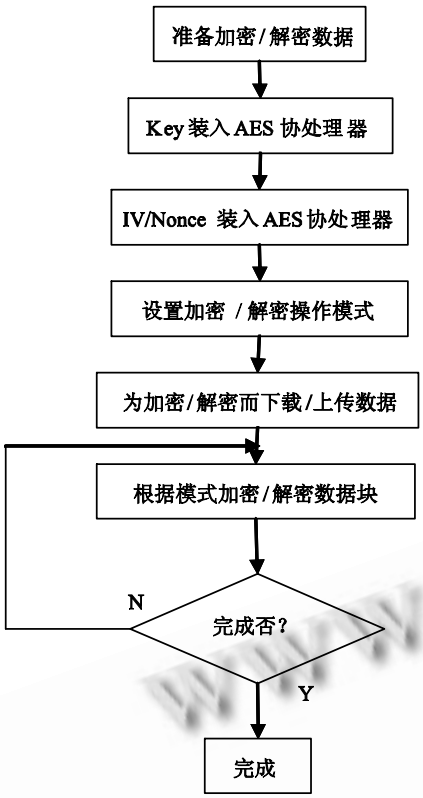

图 2　加解密操作流程

前面已经提到，AES 协处理中运行的是 128 位的数据块。但是，最后一个数据块如果少于 128 位，就必须在写入协调器时，填充 0 到该数据块中。每个数据块装入之前，必须将通用的开始命令送入 AES 协处理器中，数据块一旦装入 AES 协处理器，就通过设置好的加解密操作模式开始加密。当每个数据块加密或解密完成时，就产生一个 AES 中断(ENC)，该中断用于发送一个新的开始命令到寄存器 ENCCS。在处理下一个数据块之前，必须将加密好的数据块读出。

本文采用 128 位的密钥进行加解密，这个密钥(Key)不同，加密出来的内容也不一样，在协议栈中是通过 -DDEFAULT_KEY="{0x01, 0x03, 0x05, 0x07, 0x09, 0x0B, 0x0D, 0x0F, 0x00, 0x02, 0x04, 0x06, 0x08, 0x0A, 0x0C, 0x0D}"这种方式进行密钥定义的。

6　结论

在智能家居中，通过对数据进行加密来提高数据的安全性，可以避开相同设备的干扰，防止被其他设备监听，保证智能家居信息在网络通信中的机密性。通过协议分析仪查看，可以发现监听的数据和发送的数据是不同的，因为我们对数据加了密。

参考文献

1 IEEEHStdJ802.15.4-2003[2009-10-5].http://standards.ieee.org/getieee802/download/802.15.4-2003.pdf.
2 TheoAdvancedKEncryptionKStandardk[2009-10-28].http://en.wikipedia.org/wiki/Advanced-Encryption-Standard.
3 任秀丽,于海斌.基于 ZigBee 技术的无线传感网的安全分析.计算机科学, 2006,33(10):111－113.
4 虞志飞,邬家炜.ZigBee 技术及其安全性研究.计算机技术与发展, 2008,18(8):144－147.
5 吕治安著.ZigBee 网络原理与应用开发.北京:北京航空航天大学出版社,2007.
6 CC2430KDataKSheet[2009.9.18].http://www.chipcon.com.
7 徐小涛,吴延林著.无线个域网(WPAN)技术及其应用.北京:人民邮电出版社,2009.