• 信息安全技术 •

基于 TC 和 AES 的 ZigBee 标准安全性分析

杨 斌

(顺德职业技术学院 计算机技术系, 广东 顺德 528300)

摘 要:ZigBee 是一种新兴的无线传感网络标准,由于功耗、成本较低得到广泛应用。为研究 ZigBee 标准的安全性,分析了 ZigBee 标准协议栈体系结构,并对其定义的信任中心(trust center,TC)和所采用安全机制进行了分析。ZigBee 信任中心有住宅模式与商业模式两种安全模式,定义了比较完整的加密和认证方法。ZigBee 安全机制采用基于 AES-128 算法的 CCM*操作模式,有多种安全方案,因此,ZigBee 标准是一种比较安全的无线传感网络标准。

关键词:信任中心; 住宅模式; 商业模式; AES; CCM*

中图法分类号:TP393.08 **文献标识码**:A **文章编号**:1000-7024 (2010) 11-2439-03

Security analysis of ZigBee standard based on TC and AES

YANG Bin

(Department of Computer Technology, Shunde Polytechnic, Shunde 528300, China)

Abstract: ZigBee is a new standard for wireless sensor networks, which is widely used because of the low power consumption and low cost. In order to research the security of the ZigBee standard, the protocol stack architecture of ZigBee standard, the defined trust center (TC) and the security mechanisms are analyzed. The ZigBee trust center has residential and commercial safety models, which defines a relatively full encryption and authentication methods. There are several security schemes in the ZigBee security mechanism based on the CCM* mode of the AES-128 algorithm. Therefore, ZigBee standard is a more secure standard of wireless sensor network.

Key words: trust center; residential model; commercial model; AES; CCM*

0 引 言

ZigBee 是新一代的无线传感器网络标准。Zigbee 网络可由多达 65 000 个无线数传模块组成,每个 Zigbee 网络数传模块类似移动网络的一个基站,在整个网络范围内,它们可以相互通信,也可与现有的其它各种网络连接,范围最大达几公里。

ZigBee 为固定、便携或移动设备提供低成本、低功耗、低速率和低复杂度的无线连接,适合于工业控制自动化、无线远程监控、医疗健康、智能建筑等领域,提高工业化、信息化程度。

1 ZigBee 协议栈结构

ZigBee 协议栈包含物理层、媒体访问控制层、网络层、应用层,并定义了安全服务提供机制,其结构如图 1 所示。

物理层、媒体访问控制层采用IEEE802.15.4 标准,定义了 3 种拓扑结构,分别是:星型结构(Star)、簇状结构(cluster tree)和网状结构(Mesh),采用 CSMA/CA 媒体访问控制机制;网络层包含安全管理、消息代理、路由管理、网络管理等功能;应用层分为应用支持子层 (APS)、应用层架构、ZigBee 设备对象(ZDO),应用支持子层包含 APS 层安全管理、APS 层消息代理、转发器管理等功能,ZigBee 设备有协调器、全功能器件(FFD)和简化功能器件(RFD)3 种。

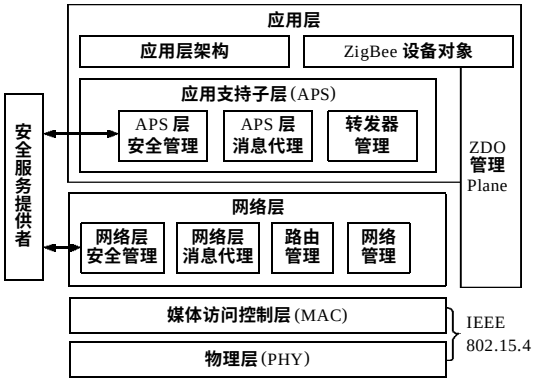


图 1 ZigBee 协议栈结构

ZigBee 协议栈提供的安全服务有数据加密、完整性校检和鉴权等功能,可以施加在网络层或应用层上,采用 AES-128 加密技术保证秘密性,并基于 AES 算法生成一系列的安全机制,用来保证完整性和真实性。安全机制为设备入网认证、数据传输、密钥建立、密钥传递以及设备管理等提供安全服务。

收稿日期:2009-04-11;修订日期:2009-10-09。

基金项目:广东省科技计划基金项目(2006A10203004);粤港关键领域重点突破招投标项目佛山专项基金项目(2006Z1);顺德职业技术学院科技基金项目(2006-kj20、2008-kj010)。

作者简介:杨斌(1968-),男,江西南昌人,硕士,副高级工程师,研究方向为通信与网络信息系统。E-mail:yangbby@126.com

2 ZigBee 信任中心

ZigBee 定义了信任中心，信任中心是一种在网络中建立与分配安全密钥的可信任设备，它允许设备进入网络，然后分配密钥(有网络密钥、链接密钥和主密钥 3 种)，从而确保设备之间端到端的安全性。信任中心有住宅模式与商业模式两种安全模式(在 ZigBee Pro 中叫标准模式与高安全模式)，住宅模式消耗资源少，但不建立密钥或随着网络规模而扩展。商用模式建立并维护密钥，且有良好的扩展性，但需要较多的存储器，为了降低存储要求，也可共享安全密钥，用于高安全的应用。但是在认证 ZigBee 2006 及之前版本的商业产品中，并未有商业安全模式相关的认证产品，因此，大部分商业化协议栈产品并未支持，而在 ZigBee Pro 产品认证中，则要求必须支持商业安全模式。

2.1 住宅模式

住宅模式以网络密钥为基础提供安全服务，网络密钥可在设备制造时由工厂安装，也可在密钥传输中得到，住宅模式中的密钥及其功能如图 2 所示。

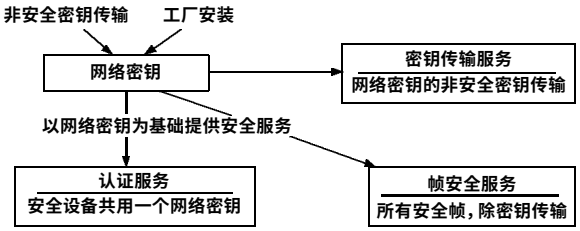


图 2 住宅模式中的密钥及其功能

住宅模式中，所有网络设备应用网络密钥加密传输数据、认证其它设备，住宅模式中新加入设备的认证过程如图 3 所示。

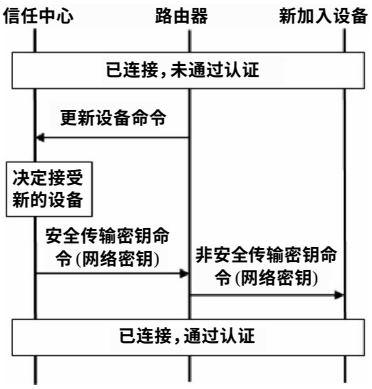
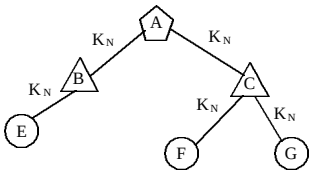


图 3 住宅模式中新加入设备的认证过程

为实现加密和认证，所有设备需要保存网络密钥和帧计数器，帧计数器包括发送帧计数器和接收帧计数器 接收帧计数器个数与设备类型有关，FFD 的接收帧计数器个数为其子节点个数，RFD 只需一个。住宅安全模式网络中的密钥见图 4 所示。

2.2 商业模式

商业模式中，网络密钥可以在媒体访问控制层、网络层和应用层中应用，主密钥和链接密钥则应用在应用层及其子层，



A :协调器； B、C :路由器； E、F、G :终端； K_N :网络密钥

图 4 住宅模式网络中的密钥

一个高层应用可以灵活地指定所用的安全套件。主密钥可在设备制造时由工厂安装，也可在非安全密钥传输中得到，也可以从信任中心采用安全密钥传输方式分配给新加入设备。链接密钥则通过主密钥使用 SKKE 协议或密钥传输方式由新加入设备与其它设备分别协商建立。网络密钥则由链接密钥加密产生。商业模式中的密钥及其功能如图 5 所示。

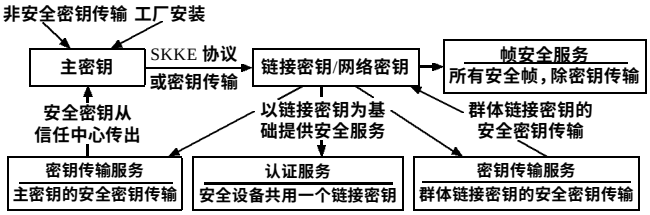


图 5 商业模式中的密钥及其功能

商业模式中，主密钥是整个系统的安全基础，但主要提供安全服务的则是链接密钥，链接密钥可用于主密钥的安全传输服务，也可在群体链接密钥传输中提供安全传输服务，还可在两个设备发起通信时提供认证服务。

商业模式中，新加入设备通过路由器向信任中心请求认证，信任中心应用主密钥认证新加入设备，认证过程如图 6 所示。

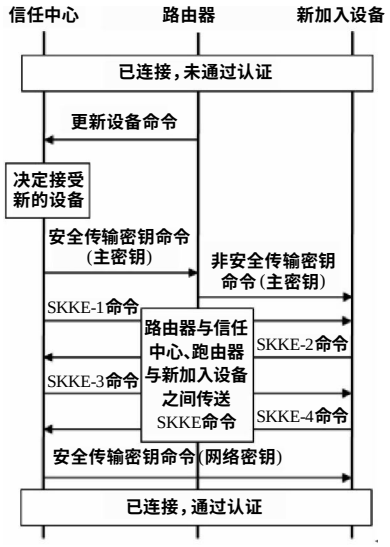
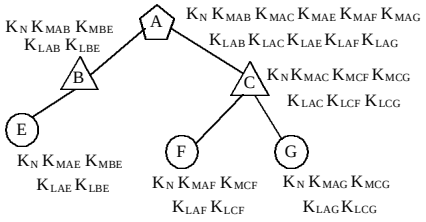


图 6 商业模式(ZigBee 2006)中新加入设备的认证过程

商业模式网络中的密钥如图 7 所示。

2.3 SKKE 协议

SKKE(symmetric-key key establishment)协议是对称密钥密钥建立协议，发起设备使用主密钥通过 SKKE 协议与响应设



A：协调器； B、C：路由器； E、F、G：终端； K_N：网络密钥；
K_{MXY}：X、Y 设备间主密钥； K_{LXY}：X、Y 设备间链接密钥

图 7　商业模式网络中的密钥

备建立链接密钥，主密钥可由工厂预装，也可由信任中心安装，或可根据用户输入的数据(例如：PIN 码，密码或密钥)生成。主密钥的秘密性和真实性是商业模式网络系统安全的基础。通过 SKKE 协议建立链接密钥的操作过程如图 8 所示。

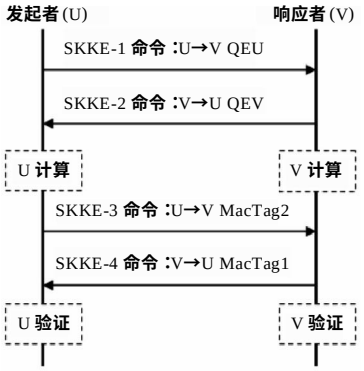


图 8　SKKE 协议操作过程

图 8 中 U 计算过程如下：

$Z = MAC\{U \parallel V \parallel QEU \parallel QEV\}_{MK}$

KKeyData = kdf(Z, 256)

MacKey = Leftmost 128bits of KkeyData

= H(Z ‖ 0x00000001)

KeyData = Rightmost 128bits of KKeyData

= H(Z ‖ 0x00000002)

$MacData2 = 0x03 \parallel U \parallel V \parallel QEU \parallel QEV$

$MacTag2 = MAC(MacData2)_{MacKey}$

图 8 中 V 计算过程如下：

$Z = MAC\{U \parallel V \parallel QEU \parallel QEV\}_{MK}$

KKeyData = kdf(Z, 256)

MacKey = Leftmost 128bits of KKeyData

=H(Z ‖ 0x00000001)

KeyData = Rightmost 128bits of KKeyData

= H(Z ‖ 0x00000002)

$MacData1 = 0x02 \parallel V \parallel U \parallel QEV \parallel QEU$

$MacTag1 = MAC(MacData1)_{MacKey}$

图 8 中 U 验证过程如下：

$MacData2 = 0x03 \parallel U \parallel V \parallel QEU \parallel QEV$

使用 MacData2 验证 MacTag2。

图 8 中 V 验证过程如下：

$MacData1 = 0x02 \parallel V \parallel U \parallel QEV \parallel QEU$

使用 MacData1 验证 MacTag1。

以上计算中，H 表示 Hash 函数，MAC 表示 HMAC 函数，‖表示右连接，0x 表示 16 进制。

则发起设备与响应设备建立的链接密钥是：$H(MAC\{U\|V\|QEU\|QEV\}_{MK}\|0x00000002)$。

3　ZigBee 中 AES 的应用

AES(advanced encryption standard)是美国联邦政府采用的一种高级加密标准。ZigBee 采用 AES-128(密钥和数据块长度均为 128 位)的 CCM*加密模式。

CCM*加密模式是 CCM(counter with cipher block chaining-message authentication code)加密模式的扩展，他包含 CCM 加密模式，同时又可单独使用 CTR 模式(counter mode)和 CBC-MAC 模式(cipher block chaining-message authentication code)。可利用 CTR 模式保证秘密性，利用 CBC-MAC 模式保证数据完整性，以及以上两者均使用既保证秘密性又保证完整性，可提供多种安全方案，并可根据安全需求选择消息完整性代码(MIC)的长度(32、64、128 位)，形成多达 8 级的安全级别。CCM*组合 CTR 模式和 CBC-MAC 模式的实现过程如图 9 所示。

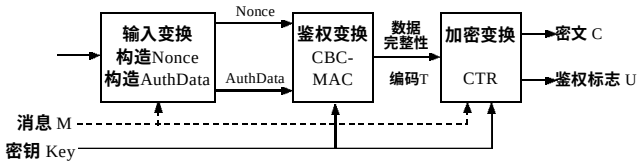


图 9　CCM*加密模式操作过程

图 9 中 3 种变换要用到如下参数：128 位密钥 Key、消息域长度 L(2-8 的整数)、鉴权域长度 M(0、4、6、8、10、12、14 和 16)、随机值 Nonce N(长度为 15-L)；鉴权数据 a 和加密数据 m，均为字节串，其长度分别为 l(m)、l(a)字节，且满足 $0 \le l(m) < 2^{8L}$、$0 \le l(a) < 2^{64}$ 条件。

随机值 Nonce N 包含设备源地址、帧计数、安全控制 3 个字段，长度分别为 64 位、32 位、8 位。安全控制字段又包括安全级别(3 位)、密钥标识(2 位)、扩展 Nonce(1 位)3 个数据域，另有两位作为保留使用。安全级别对应无加密、MIC-32、MIC-64、MIC-128、ENC、ENC-MIC-32、ENC-MIC-32、ENC-MIC-32 共 8 个安全级别；密钥标识对应数据密钥、网络密钥、密钥传输密钥、密钥装载密钥 4 种类型；扩展 Nonce 表明发送者地址是否设置在帧辅助头(auxiliary header)。

3.1　输入变换

输入变换的目的是输入 a 和 m，形成 AuthData 和 PlainText-Data，用于鉴权变换和加密变换，步骤如下：

(1)对 a 形成 L(a)字节串：如果 l(a)=0，则 L(a)为空；如果 $0 < l(a) < 2^{16}-2^8$，则 L(a)是 l(a)的 2 个字节编码；如果 $2^{16}-2^8 \le l(a) < 2^{32}$，则 L(a)是 0xff、0xfe 和 l(a)的 4 个字节编码的右连接；如果 $2^{32} \le l(a) < 2^{64}$，则 L(a)是 0xff、0xff 和 l(a)的 8 个字节编码的右连接(以下用“‖”表示)。

(2)增补鉴权数据 AddAuthData=L(a) ‖ a ‖ 0，该数据能整除 16。

(3)增补消息数据 PlaintextData= m ‖ 0，该数据能整除 16。

(下转第 2481 页)

[3] Atmel Inc. ATmega8L data sheet[EB/OL]. http://www.at-me1.com/dyn/resources/proddocuments/2486S.pdf,2008.

[4] 袁刚强,邓世建,吴玉康.基于 AVR 的新型防汽车追尾安全装置设计[J].电子设计工程,2009,17(10):61-65.

[5] 张帅,谈国新,伍传敏.基于过程化处理的 Flash 动画制作方法[J].计算机工程与设计,2008,29(11):5598-5600.

[6] Penner R. Programming Macromedia Flash MX[M]. Berkeley, CA,USA:Brandon A.Nordin,2002.

[7] 李康满,刘朝晖.在 VC++中使用 Flash 动画技术[J].衡阳师范学院学报,2005,26(6):86-88.

[8] 张志会.基于 Flash 的车站作业可视化仿真[J].铁道运输与经济,2009,31(10):21-26.

(上接第 2441 页)

(4)鉴权数据 AuthData=AddAuthData ‖ PlaintextData。

3.2 鉴权变换

鉴权变换的目的是生成消息完整性编码，使用CBC-MAC模式，其输入参数是随机值 Nonce N 和鉴权数据 AuthData，消息完整性编码 T 计算过程如图 10 所示。

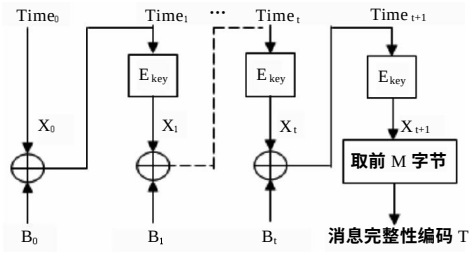


图 10 CBC-MAC 模式操作过程

B_0 :=Reserved ‖ Adata ‖ M ‖ L ‖ Nonce N ‖ l(m)

//Reserved 是 1 位扩充位，作为将来扩充之用，被设置为 0；Adata 为 1 位，当 l(a) =0 时，值为 0，否则为 1；L 为 3 位，代表整数 L -1；M 为 3 位，当 M >0 时，值为(M - 2) /2，否则为 0。

$X_0 := 0^{128}$; //0^{128} 代表 16 个字节全 0。

X_{i+1}:= E(Key, $X_i \oplus B_i$) for i=0, ...,t.

//先把 AuthData 分解为 B_1 ‖ B_2 ‖ … ‖ B_t，每个 B_i 均为 16 个字节，再把 X_i 和 B_i 进行异或，然后用密钥 Key 加密，形成 X_{i+1}。

消息完整性编码 T: = left(1,M,X_{i+1})//取密文 X_{i+1} 前 M 个字节。

3.3 加密变换

加密变换使用 CTR 模式，加密过程如图 11 所示。

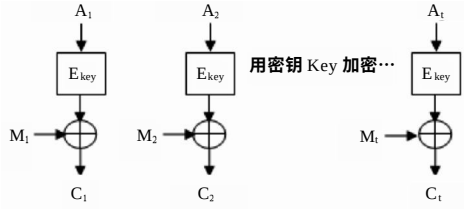


图 11 CTR 模式操作过程

密文块 C_i:= E(Key, A_i)⊕M_i,for i=1,2,…,t//计数域 A_i = Reserved ‖ Reserved ‖ 0 ‖ L ‖ Nonce N ‖ Counter i, for i = 0,1,2,…，消息块 M_i 都为 16 字节。

加密块 S_0:= E(Key, A_0)

加密鉴权标志 U : = T ⊕left(1,M,S_0)

密文 C: = left(1，l(m)，C_1 ‖ C_2 ‖ … ‖ C_t) ‖ U

4 结束语

ZigBee标准是一项新的无线网络技术与传感器技术相结合的无线通信技术，是一种用于无线监测与控制应用的全球性无线通信标准，由于具有低成本、低功耗和低复杂度等优越性，得到广泛应用。ZigBee标准定义了信任中心，采用 AES-128 加密算法的 CCM*操作模式，提供了加密、数据完整性检查和鉴权功能，有较高的安全性。通过对 ZigBee 标准安全性分析，了解 ZigBee 安全机制和安全性能，可促进 ZigBee 标准不断发展，满足人们日益增长的安全性需求。

参考文献:

[1] ZigBee Document 053474r17[S].ZigBee Specifications.

[2] ZigBee Document 053474r13[S].ZigBee Specifications.

[3] ZigBee Document 053474r7[S].ZigBee Specifications.

[4] ZigBee Document 053474r6[S].ZigBee Specifications.

[5] ZigBee Document 02039r0: Security working group requirements definition[S].ZigBee Specifications.

[6] ZigBee Document 053275r03: ZigBee protocol stack settable values (knobs)[S].ZigBee Specifications.

[7] ZigBee Document 074855r01: ZigBee PRO stack profile [S]. ZigBee Specifications.

[8] Yuan Yuxiang.ZigBee IEEE 802.15.4[EB/OL].http://www. sasase.ics.keio.ac.jp/jugyo/2005/zigbee.pdf .

[9] ZigBeeTM Alliance.08045r00ZB_AFG-ZigBee-Technical-Overview[EB/OL].http://203.208.37.132/search? q=cache:vrIn7QHrnRUJ: www.zigbee.org/imwp/idms/popups/pop_download.asp%3FContentID%3D12617+ZigBee+2007+ppt&cd = 1&hl = zh-CN&ct=clnk&gl=cn&st_usg=ALhdy2_5sPeQpokoWPcRBiDx6jO0gj_3MA .

[10] Sinem Coleri Ergen, ZigBee/IEEE 802.15.4 Summary[EB/OL]. http://pages.cs.wisc.edu/~suman/courses/838/papers/zigbee. pdf.

[11] Ender Yuksel, Hanne Riis Nielson, Flemming Nielson. ZigBee-2007 security essentials[C].Proceedings of the 13th Nordic Workshop on Secure IT Systems,2008:65-82.

[12] Fereshteh Amini, Moazzam Khan, Jelena Misic, et al. Performance of IEEE 802.15.4 clusters with power management and key exchange[J].Journal of Computer Science and Technology, 2008,23(3):377-388.

[13] NIST. Advanced encryption standard (AES) [M]. FIPSPUB 197,2001.