ZigBee技术及其安全性研究

虞志飞,邬家炜
(华南师范大学 计算机学院,广东 广州 510631)

摘 要:ZigBee技术是一种面向无线传感器网络的新技术,在传感器网络广泛应用的情况下,其安全性既要满足高保密性,又要符合低功耗、低复杂性、低成本的要求。因此,研究ZigBee技术的安全性就显得尤为重要。从ZigBee协议栈的安全方面入手,讨论了ZigBee技术的加密技术、安全密钥、网络结构和信任中心方面的安全机制,特别对ZigBee技术存在的一些问题和未来发展进行了分析和总结。

关键词:ZigBee技术;安全;安全密钥;信任中心
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2008)08-0144-04

Research of ZigBee Technology and Its Security

YU Zhi-fei, WU Jia-wei
(School of Computer, South China Normal University, Guangzhou 510631, China)

Abstract: ZigBee is a new technology with wireless sensor networks. With the application of wireless sensor networks, many applications not only have high confidentiality, but also should have low power loss, low complexity and low cost. So the research of the security of ZigBee is becoming very important. From the layers security of ZigBee, mainly discuss the encryption techniques, security key, network structure and the trust center. At last also analyse and conclude some problems to the ZigBee technology and the development of it in the future.

Key words: ZigBee technology; security; security key; trust center

0 引 言

ZigBee是一种短距离、低速率的无线通信技术,是当前面向无线传感器网络的技术标准。其名字来源于蜂群使用的赖以生存和发展的通信方式。虽然存在多种无线网络技术与之竞争,但因其优越特性在其中脱颖而出,主要特性有低速率、近距离、低功耗、低复杂度和低成本,目前适合应用在短距离无线网络通信方面。ZigBee联盟预测主要应用领域包括工业控制、消费性电子设备、汽车自动化、农业自动化和医用设备控制等。在许多应用中,安全性在传感器网络中有很高的要求,因此,安全问题成为制约无线传感器网络发展的一个重要因素。文中主要对ZigBee协议栈体系结构、安全密钥、网络结构以及信任中心使用的安全机制进行分析,使对ZigBee安全技术有详细的了解,并提出安全方面存在的问题以及今后ZigBee技术在安全方面的发展趋势。

收稿日期:2007-11-30
基金项目:广东省科技计划项目(2007B010400068)
作者简介:虞志飞(1984-),男,江西抚州人,硕士研究生,研究方向为网络安全、远程教育;邬家炜,教授,硕士研究生导师,研究方向为计算机网络及应用、远程教育。

1 ZigBee协议栈体系结构安全

ZigBee协议是一种新兴的无线传感器网络技术标准,它是在传统无线协议无法适应无线传感器网络低成本、低能量、高容错性等要求的情况下产生的。ZigBee是在IEEE 802.15.4(无线个人区域网)协议标准的基础上扩展的,IEEE802.15.4标准只定义了PHY层和数据链路层的MAC子层。PHY层由射频收发器以及底层的控制模块构成,MAC子层为高层访问物理信道提供点到点通信的服务接口。ZigBee联盟制定网络层和应用会聚层各高层规范。安全体系结构[1]如图1所示。

ZigBee协议栈由物理层、数据链路层、网络层、应用层组成。物理层负责基本的无线通信,由调制、传输、数据加密和接收构成。链路层提供设备之间单跳通信、可靠传输和通信安全。网络层主要提供通用的网络层功能(如拓扑结构的搭建和维护、寻址和安全路由)。应用层包括应用支持子层、ZigBee设备对象和各种应用对象。

应用支持子层提供安全和映射管理服务,ZDO负责设备管理,包括安全策略和安全配置的管理,应用层提供对ZDO和ZigBee应用的服务。

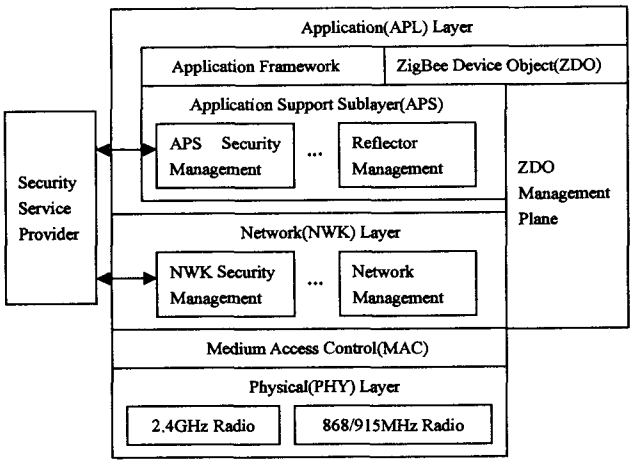


图 1　ZigBee 协议栈安全体系结构

1.1　数据链路层安全

数据链路层通过建立有效的机制保护信息安全。MAC 层有四种类型的帧,分别是命令帧、信标帧、确认帧和数据帧。安全帧格式[2]如图 2 所示。

SYNC	PHY Header	MAC Header	Auxiliary Header	Encrypted MAC Payload	MIC

图 2　数据链路层安全帧格式

其中 AH 是携带的安全信息,MIC 提供数据完整性检查,有 0,32,64,128 位可供选择。对于数据帧,MAC 层只能保证单跳通信安全,为了提供多跳通信的安全保障,必须依靠上层提供的安全服务。在 MAC 层上使用的是 AES 加密算法,根据上层提供的钥匙的级别,可以保障不同水平的安全性。IEEE802.15.4 标准 MAC 层使用的是 CCM 模式,CCM 是一种通用的认证和加密模式,被定义使用在类似于 AES 的 128 位大小的数据块上,它由 CTR 模式和 CBC－MAC 模式组成。CCM 主要包括认证和加密解密,认证使用 CBC－MAC 模式,而加解密使用的是 CTR 模式。然而 ZigBee 技术对数据保护采用一种改进的模式即 CMM * 模式,它是通过执行 AES－128 加密算法来对数据保密,具体实现过程参考文献[3]。

1.2　网络层安全

网络层对帧采取的保护机制同上一样,为了保证帧能正确传输,帧格式中也加入了 AH 和 MIC。安全帧格式[2]如图 3 所示。

SYNC	PHY Header	MAC Header	NWK Header	Auxiliary Header	Encrypted MAC Payload	MIC

图 3　网络层安全帧格式

NWK 层主要思想是首先广播路由信息,接着处理接受到的路由信息,例如判断数据帧来源,然后根据数据帧中的目的地址采取相应机制将数据帧传送出去。在传送的过程中一般是利用链接密钥对数据进行加密处理,如果链接密钥不可用,那网络层将利用网络密钥进行保护,由于网络密钥在多个设备中使用,可能带来内部攻击,但是它存储开销代价更小。NWK 层对安全管理有责任,但其上一层控制着安全管理。

1.3　应用层安全

APL 层安全是通过 APS 子层提供,根据不同的应用需求采用不同的钥匙,主要使用的是链接密钥和网络密钥。安全帧格式[2]如图 4 所示。

SYNC	PHY Header	MAC Header	NWK Header	APS Header	Auxiliary Header	Encrypted MAC Payload	MIC

图 4　应用层安全帧格式

APS 提供的安全服务有钥匙建立、钥匙传输、设备服务管理。钥匙建立是在两个设备间进行,包括四个步骤[4]:交换暂时数据,生成共享密钥,获得链接密钥,确认链接密钥。钥匙传输服务是在设备间安全传输钥匙。设备服务管理包括更新设备和移除设备,更新设备服务提供一种安全的方式通知其它设备有第三方设备需要更新,移除设备则是通知有设备不满足安全需要,要被删除。

2　安全密钥

ZigBee 采用三种基本密钥,分别是网络密钥、链接密钥和主密钥,它们在数据加密过程中使用。其中网络密钥可以在数据链路层、网络层和应用层中应用,主密钥和链接密钥则使用在应用层及其子层。

网络密钥可以在设备制造时安装,也可以在密钥传输中得到,它可应用于多层。主密钥可以在信任中心设置或者在制造时安装,还可以是基于用户访问的数据,例如,个人识别码(PIN)、密码和口令等。为了保证传输过程中主密钥不遭到窃听,需要确保主密钥的保密性和正确性。链接密钥是在两个端设备通信时共享,可以由主密钥建立,因为主密钥是两个设备通信的基础。它也可以在设备制造时安装。

链接密钥和网络密钥要不断进行更新。当两个设备同时拥有这两种密钥时,采用链接密钥来通信。尽管存储网络密钥开销小,但是降低了系统安全。

3　ZigBee 网络结构

ZigBee 规范定义了三种类型的设备,分别是 ZigBee 协调器、ZigBee 路由器和 ZigBee 终端设备。ZigBee 协调器负责启动和配置网络,在一个 ZigBee 网络中只允许一个 ZigBee 协调器。ZigBee 路由器是一种支持关联的设备,一个网络可以有多个路由器,它能够将消息转发到其它设备,但是在星型网络中不支持 ZigBee 路由器。ZigBee 终端设备可以执行相关的功能,并使用网络到达其它需要与其通信的设备。ZigBee 网络结构

如图 5 所示。

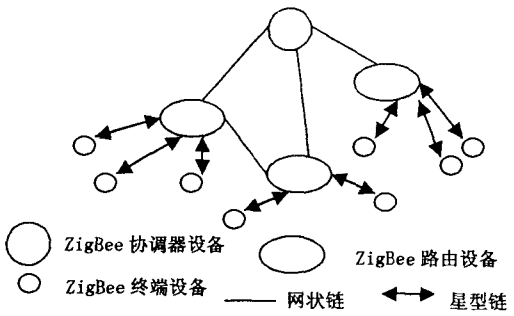


图 5 ZigBee 网络结构

4 信任中心

所谓信任中心是在网络中分配安全钥匙的一种令人信任的设备,它允许设备加入网络,并分配密钥,因而确保设备之间端到端的安全性。在采用安全机制的网络中,网络协调者可成为信任中心。信任中心提供三种功能:

(1)信任管理。任务是负责对加入网络的设备验证。

(2)网络管理。任务是负责获取和分配网络钥匙给设备。

(3)配置管理。任务是确保端到端设备的安全。

信任中心有二种模式:住宅模式和商用模式。对于住宅模式,信任中心要维护一张关于网络中所有设备和钥匙的清单,并采取措施对网络访问和钥匙进行控制管理。同样对于商用模式,信任中心也要维护一张网络中设备和钥匙的清单,并实施策略对网络钥匙的更新和网络访问控制进行管理,但它还要在每个设备中维护一个计数器,此计数器会随着钥匙的产生不断变化,目的是保证顺序更新。商用模式需要维护钥匙并允许更新,具有良好的扩展性,但其要消耗相当多的存储空间,相比之下住宅模式消耗资源少且不需要设置钥匙,因而不要更新,但其网络的扩展性不好。以下针对住宅和商业模式网络的特点,给出了钥匙分布情况和鉴权过程。

住宅模式网络中钥匙分布图如图 6 所示。

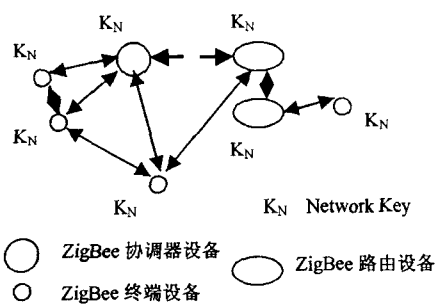
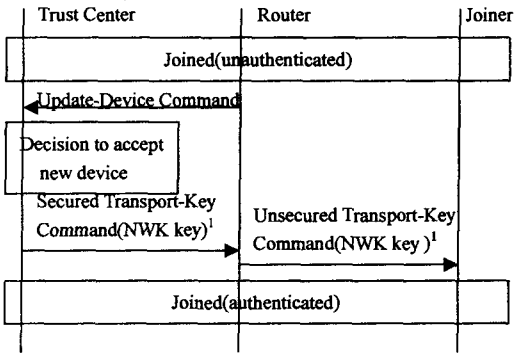


图 6 住宅模式钥匙分布图

住宅模式鉴权过程[5]如图 7 所示。



Note:
1.The trust center sends a dummy all-zero NWK key if the joiner securely joined using a preconfigured network key.

图 7 住宅模式鉴权过程

对于商业模式,网络中钥匙分布和鉴权过程相对来说比较复杂,具体过程参考文献[5]。为了满足安全性需要,ZigBee 标准提供不同的方法来确保安全,概括主要有以下方面:

(1)加密技术。ZigBee 使用 AES-128 加密算法。网络层加密是通过共享的网络密钥来完成,它可以阻止来自外部的攻击。而设备层是通过唯一链接密钥在两端设备间完成加密,它可以阻止内外部的攻击。但是加密技术的有无不会影响顺序更新、完整性和鉴权。

(2)鉴权技术。鉴权可以保证信息的原始性,使得信息不被第三方攻击,有网络层和设备层两种。网络层鉴权可以阻止外部攻击但增加了内存开销,它通过共享网络密钥完成。设备层鉴权是通过设备间唯一链接密钥完成,它可以阻止内外部攻击,但内存开销高。

(3)完整性保护。对信息的完整性保护提供四种可供选择,分别是 0、32、64 和 128 位,其中默认采用 64 位。

(4)顺序更新。通过设置计数器来保证数据更新,通过使用一个有序编号来避免帧重发攻击。在接收到一个数据帧后,将新的编号和最后一个编号比较,如果新的编号比最后一个编号要新,则校验通过,编号更新为最新的;反之,校验失败。这样可以保证收到的数据是最新的,但不提供严格的与上一帧数据之间的时间间隔信息。

ZigBee 标准定义了 8 种安全级别,具体如表 1 所示。

5 存在问题及未来展望

ZigBee 用了多种措施来保证传输安全,采用 AES-128 加密算法、数据完整性检查和鉴权功能。这些措施在某种程度上对安全有一定保障,但是也存在一

些问题。虽然文献[6]认为AES-128加密算法对大部分商业应用来说是足够安全的,而且NIST也预计AES-128加密至少用到2036年是安全的[7],但是文献[8]认为单一的对称加密算法在数据加密和密钥交换中可能带来安全隐患,研究非对称加密在密钥分配中应用具有前景。文献[9]建议将椭圆曲线加密方法作为公钥非对称计划在ZigBee技术中应用。在ZigBee组网方面,基于ZigBee技术组成的网状网只适合数据传输较低的应用,例如工业控制领域,而不适合数据传输量多的应用,因此需进一步加强ZigBee组网的研究,使之应用领域更为广泛。对于无线传感网络中数据安全交换方面,ZigBee联盟只是在理论上对网络层安全协议进行描述,并没有对不同应用应采取具体安全级别有具体的研究,因此加强针对不同应用的具体安全措施还有待进一步发展,同时对数据完整性和认证技术研究以及根据不同的应用情况,进行安全属性的灵活配置研究也很重要。由于IPv6拥有巨大的地址空间,能为每一个ZigBee节点分配一个全球唯一的网络地址,同时还能提供很好的QoS和安全的通信保障,因此,IPv6和ZigBee结合是未来发展的一个亮点,目前国内相应的产品也已经问世。总之,为ZigBee技术有更加广阔的应用空间,ZigBee技术的安全技术,如密钥分配协议的需求与性能指标、密钥管理的方案等,还需进一步深入研究。

表1　ZigBee安全级别

安全级别 Security level	安全属性 Security attribute	数据加密 Data encryption	帧完整性 Frame integrity	完整性代码 Integrity code
0	没有	没有	没有	0 bit
1	MIC-32	没有	有	32 bit
2	MIC-64	没有	有	64 bit
3	MIC-128	没有	有	128 bit
4	ENC	有	没有	0 bit
5	ENC+MIC-32	有	有	32 bit
6	ENC+MIC-64	有	有	64 bit
7	ENC+MIC-128	有	有	128 bit

6　结束语

ZigBee是一种新兴的无线网络通信技术,它因优越的特性在众多技术中脱颖而出,被业界认为是最适合无线传感网络的新技术。在安全方面,ZigBee技术对协议栈各层加强安全保护,采用AES加密算法对数据加密,同时提供数据完整性检查和鉴权措施,还建立信任中心机制对安全钥匙管理,这些安全措施的采用使无线网络通信具有良好安全保护机制。通过对ZigBee技术安全分析,对ZigBee安全优势和不足有一定了解,但是随着许多应用对安全需求的提升,进一步加强安全研究是必要的。

参考文献:

[1] ZigBee Alliance document[EB/OL]. 2004. http://www.zigbee.org.

[2] Paolo B, Prashant P, Vince W, et al. Wireless Sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards[J]. Computer Communication, 2007, 30(7):1655-1695.

[3] 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.

[4] Moazzam K, Fereshteh A, Jelena M. Key Exchange in 802.15 Networks and Its Performance Implications[C]//In Proc of 2nd International Conference on Mobile Ad-hoc and Sensor Networks (MSN 2006), LNCS, Vol. 4325. [s. l.]: Springer-Verlag, 2006:497-508.

[5] ZigBee Alliance. ZigBee Security Specification Overview[EB/OL]. 2005. http://www.zigbee.org/en/events/documents/December2005_Open_House_Presentations/Zigbee_Security_Layer_Technical_Overview.pdf.

[6] Ferguson N, Schneier B. Practical cryptography[M]. New York: John Wiley and Sons, 2003.

[7] Krasner J. Using Elliptic Curve Cryptography(ECC) for Enhanced Embedded Security[EB/OL]. 2004. http://www.embedded-forecast.com/EMF-ECC-FINAL1204.pdf. 2004.

[8] Ondrej H, Peter K, Petr F, et al. On security of PAN wireless systems[C]//In Proc of 6th International Workshop on Embedded Computer Systems(SAMOS 2006), LNCS, Vol. 4017. [s. l.]: Springer-Verlag, 2006:178-185.

[9] Pereira R. ZigBee and ECC Secure Wireless Networks[EB/OL]. 2004. http://www.elecdesign.com.

(上接第133页)

and Systems. Boulder, Colorado, USA: [s. n.], 1999:209-220.

[7] Yuan Chun, Cheng Yu, Zhang Zheng. Evaluation of Edge Caching/Offloading for Dynamic Content Delivery[J]. IEEE Transactions on Knowledge and Data Engineering, 2004, 16(11):1411-1423.

[8] 范国闯,钟　华,黄　涛,等. Web应用服务器研究综述[J]. 软件学报,2003,14(10):1728-1739.