

ZigBee 技术的无线传感器网络的安全性研究*

任秀丽¹, 于海斌²

(1 辽宁大学信息科学与技术学院沈阳 110036;

2 中国科学院沈阳自动化研究所沈阳 110016)

摘要: 无线传感器网络是自动化、通信工程和计算机科学技术学科中一个新的研究领域, 主要应用在工业、军事、医疗、商业等领域。在大多数应用环境中, 用户对无线传感器网络的安全性有很高的要求, 因此, 安全成为制约无线传感器网络进一步广泛应用的关键。然而, 最新兴起的 ZigBee 无线技术能够很好地解决无线传感器网络的安全问题。本文针对 ZigBee 技术在组网方式、安全结构、加密算法等安全方面进行了全面的剖析。

关键词: 无线传感器网络; ZigBee; 安全; 密钥; 算法

中图分类号: TP393 **文献标识码:** A **国家标准学科分类代码:** 510.50

Study on security of ZigBee wireless sensor network

Ren Xiuli¹, Yu Haibin²

(1 School of Information Science & Technology, Liaoning University, Shenyang 110036, China;

2 Shenyang Institute of Automation, Chinese Academy of Sciences, Shenyang 110016, China)

Abstract: Wireless sensor network is a new research area in automation, communication engineering and computer science. It can be used for various application fields such as industry, military, medical, business and etc. Since most wireless sensor network applications have strict security requirements, security is a critical issue in wireless sensor networks. However, the new ZigBee wireless technique can solve these problems. This paper completely analyzes ZigBee network topology, security structure, encryption algorithm and other techniques.

Key words: wireless sensor network; ZigBee; security; key; algorithm

1 引言

无线传感器网络是自动化、通信工程和计算机科学技术学科中一个新的研究领域, 是一项应用于某一工作区域的信息感知和信息收集技术, 主要应用于工业控制、军事侦察、环境科学、医疗健康、空间探索、智能建筑等各种复杂环境进行检测、诊断、目标定位和跟踪^[1-3]。在大多数应用环境中, 用户对无线传感器网络的安全性有很高的要求, 因此, 安全成为制约无线传感器网络进一步广泛应用的关键。2004年12月, ZigBee 1.0 标准正式公布, 该标准体现了无线组网的安全。ZigBee 协议标准同其他

协议标准一样, 是该项技术发展的阶段性规范的体现, 对该项技术的进展起着重要的推动作用。但是, 它又不可能是完美无缺的, 随着技术的发展和应用的需求, 必然会对其进行改进和完善。要想正确使用标准并对它进行研究, 必须对其有深入、全面的了解。本文针对 ZigBee 技术在组网方式、安全结构、加密算法等安全方面进行了全面的剖析, 以求促进 ZigBee 安全技术的进一步发展。

2 ZigBee 技术和网络体系结构

ZigBee 技术是一种近距离、低复杂度、低功耗、低速率、低成本的无线通信技术。工作在 2.4 GHz 的 ISM 频

段上,传输速率为 20 ~ 250 Kb/s,传输距离为 10 ~ 75 m。主要适用于自动控制、传感和远程控制领域,可以嵌入到各种设备中。它依据 IEEE 802. 15. 4 标准,在数千个微小的传感器之间相互协调实现通信。这些传感器只需要很少的能量,以接力的方式通过无线电波将数据从一个传感器传到另一个传感器,所以它们的通信效率非常高。

为了降低系统成本,ZigBee 网络中定义了 2 种类型的设备^[46]:一种是全功能设备(full function device, FFD),称为主设备,它承担了网络协调者的功能,可与网络中任何类型的设备通信。在网络传输过程中,如果采用安全机制,网络协调者又可成为信任中心;另一种是简化功能设备(reduced function device, RFD),称为从设备,它不能作为网络协调者,只能与主设备通信。

ZigBee 主要采用了 3 种组网方式^[74]:星型网(Star)、网状型网(Mesh)和簇型网(Cluster tree),如图 1 所示。在星型网中,一个功能强大的主设备位于网络的中心,作为网络协调者,其他主设备或从设备分布在其覆盖范围内。网状型网是由主设备连接在一起形成的,网络中的主设备互为路由器。簇型网是由星型网和网状型网相结合形成的,各个子网内部都以星型网连接,其主设备又以对等的方式连接在一起。数据流首先传到同一个子网内的主设备,通过网关节点达到更高层的子网,随后继续上传,最后到达汇集中心设备。

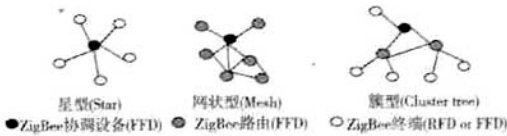


图 1 ZigBee 的 3 种网络结构
Fig. 1 Three kinds of ZigBee network architecture

3 安全结构

ZigBee 技术的物理层和数据链路层协议主要采用 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;应用层包括应用支持子层、ZigBee 设备对象(ZigBee device object, ZDO)和应用,ZDO 负责整个设备的管理,应用层提供对 ZDO 和 ZigBee 应用的服务。数据链路层、网络层和应用层负责在各自层上传输安全的数据,而且应用子层提供安全关系的建立和维护等服务,ZDO 管理安全策略和设备的安全配置,ZigBee 的安全结构^[9]如图 2 所示。

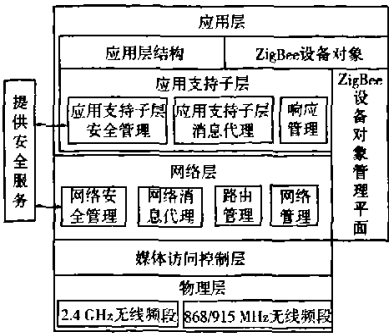


图 2 ZigBee 的 3 种网络安全结构
Fig. 2 Three kinds of ZigBee network security architecture

4 安全特点

ZigBee 技术在安全方面具体表现为如下特点:

(1) 提供了刷新功能

刷新检查能够阻止转发的攻击;ZigBee 设备保持输入和输出刷新计数器,当有一个新的密钥建立时,计数器就重新设置。每秒通信一次的设备,它的计数器值不能超过 136 年。

(2) 提供了数据包完整性检查功能

在传输过程中,这种功能阻止攻击者对数据进行修改。完整性选项有 0、32、64 或 128 位,在数据保护和数据开销之间进行折中选择。

(3) 提供了认证功能

认证保证了数据的发起源,阻止攻击者修改一个设备并模仿另一个设备;认证可应用在网络层和设备层,网络层认证是通过使用一个公共的网络密钥,这阻止了外部的攻击,内存开销很少。设备层认证是在 2 个设备之间使用唯一的链接密钥,能阻止内部和外部的攻击,但需要很高的内存开销。

(4) 提供了加密功能

阻止窃听器侦听数据。它使用 128 位 AES 加密算法,这种加密保护可应用在网络层和设备层上。网络层加密是通过使用一个公共的网络密钥,这阻止了外部的攻击,内存开销很少。设备层加密是在 2 个设备之间使用唯一的链接密钥,能阻止内部和外部的攻击,但需要很高的内存开销。

5 安全密钥

ZigBee 技术在数据加密过程中,可以使用 3 种基本密钥,分别是主密钥、链接密钥和网络密钥。主密钥可以是在设备制造时安装的,也可以通过信任中心设置的,或者是基于用户访问的数据,例如:个人识别码(PIN)、口

令和密码等。主密钥是2个设备长期安全通信的基础,也可以作为一般的链接密钥使用。所以,必须维护主密钥的保密性和正确性。在网络传输过程中,采用主密钥可以阻止窃听;链接密钥是在一个PAN网络中被2个设备共享的,它可以通过主密钥建立,也可以在设备制造时安装;网络密钥可以通过信任中心设置,也可以在设备制造时安装。它可应用在数据链路层、网络层和应用层。

链接密钥和网络密钥不断地进行周期性的更新。当2个设备都拥有这2种密钥时,采用链接密钥进行通信。虽然存储网络密钥的开销小,但它降低了系统的安全性,因为网络密钥被多个设备所共享,所以它不能阻止内部的攻击。

6 加密和解密

ZigBee技术针对不同的应用,提供了不同的安全策略。这些策略分别施加在数据链路层、网络层和应用层上,其对数据的安全保护是在CCM*模式下执行AES-128加密算法。CCM*模式是对CCM模式^[10]的一种改进,CCM模式是由计数器(counter, CTR)模式和密码块链接消息鉴权代码(cipher block chaining-MAC, CBC-MAC)模式相结合构成的。CCM*模式的执行包括输入变换、鉴权变换、加密变换和解密变换,在这4种变换中,通常使用6个参数,分别是:一个位串密钥Key,其长度 $keylen$ 为128位;消息域的长度 $L(2, 3, \dots, 8)$;鉴权域的长度 $M(0, 4, 6, 8, 10, 12, 14, 16)$; N 值的域长度为 $15 - L$,对于在任意一个范围内,使用同一个密钥时, N 值是唯一的; m 个字节串的域长度为 $l(m)$ B,它的取值范围为 $0 \leq l(m) < 2^{31}$; a 个字节串的域长度为 $l(a)$ B,它的取值范围为 $0 \leq l(a) < 2^{34}$ 。

6.1 输入变换

输入变换是要输入鉴权数据 a 和加密数据 m ,通过以下步骤完成:

步骤1 对 a 个字节串的域长度为 $l(a)$ B,形成 $L(a)$ 字节串。

(1) $l(a) = 0$, 则 $L(a)$ 为空串;

(2) $0 < l(a) < 2^{16} - 2^8$, 则 $L(a)$ 是对 $l(a)$ 的2个字节将要加密;

(3) $2^{16} - 2^8 \leq l(a) < 2^{32}$, 则 $L(a)$ 是0xff, 0xfe和 $l(a)$ 的4个将要加密字节进行右连接;

(4) $2^{32} \leq l(a) < 2^{64}$, 则 $L(a)$ 是0xff, 0xff和 $l(a)$ 的8个将要加密字节进行右连接。

步骤2 再进行 $L(a)$ 和 a 本身右连接,形成结果串。

步骤3 将结果串形成一个增补鉴权数据(AddAuth-Data),该数据是通过右连接非负数零形成的,形成的增补数据能整除16。

步骤4 采用同样方法形成一个增补消息数据

(PlaintextData),该数据是将加密数据 m 通过右连接非负数零形成的,形成的增补数据也必须能整除16。

步骤5 最后形成鉴权数据(AuthData),它是由数据AddAuthData和数据PlaintextData构成的,即为 $AuthData = AddAuthData \parallel PlaintextData$ 。

6.2 鉴权变换

数据AuthData构成之后,对它进行加标记变换,具体过程如下:

步骤1 形成一个字节标志域(Flags),它是由1位表示保留(Reserved),1位表示Adata,3位表示 M 和3位表示 L 所组成,即为:

$$Flags = Reserved \parallel Adata \parallel M \parallel L$$

式中:1位Reserved作为将来的扩充,被设置为0;当 $l(a) = 0$ 时,1位Adata将设置为0,否则,将设置为1;3位 L 域代表整数 $L-1$;当 $M > 0$ 时,3位 M 域代表整数 $(M-2)/2$,否则,设置为0。

步骤2 形成16个字节的 B_0 域,它是由上面定义的1个字节标志域(Flags)、 $15 - L$ 个字节的 N 域和用 L 个字节表示的长度 $l(m)$ 域组成,即为:

$$B_0 = Flags \parallel N \parallel l(m)$$

步骤3 分解数据AuthData为 $B_1 \parallel B_2 \parallel \dots \parallel B_t$,式中每个数据块是一个16个字节的串,则CBC-MAC值定义为:

$$X_0 = 0^{128}, X_{i+1} = E(Key, X_i \oplus B_i) \quad (i = 0, \dots, t)$$

式中: $E(K, X)$ 表示使用密钥 K 通过函数 E 对明文 X 进行加密; 0^{128} 代表16个字节全部为0。

再求鉴权标志 T ,它是一个MAC值,通过将密文 X_{i+1} 取前 M 个字节获得的,即为:

$$T = first - M - bytes(X_{i+1})$$

6.3 加密变换

明文数据PlaintextData和鉴权标志 T 都已被建立,使用加密变换进行加密过程如下:

步骤1 形成一个字节标志域(Flags),它是由2个1位表示保留(Reserved),3位表示整数0和3位表示整数 L 所组成,即为:

$$Flags = Reserved \parallel Reserved \parallel 0 \parallel L$$

式中:2个位保留域作为将来的扩充,被设置为0;3位 L 域表示整数 $L-1$;3位0域表示0。

步骤2 形成16个字节的 A_i 域,它是由1个字节标志域(Flags)、 $15 - L$ 个字节的 N 域和 L 个字节表示的整数 i 组成,即为:

$$A_i = Flags \parallel N \parallel Counter \ i \ (i = 0, 1, 2, \dots)$$

步骤3 分解消息数据PlaintextData为 $M_1 \parallel M_2 \parallel M_3 \parallel \dots \parallel M_t$,式中每个消息块 M_i 都是一个16个字节的串,密文块 C_1, \dots, C_t 定被定义为:

$C_i = E(\text{Key}, A_i) \oplus M_i (i = 1, 2, \dots, t)$

步骤 4 密文 *Ciphertext* 取串 $C_1 \parallel C_2 \parallel \dots \parallel C_t$ 最左边的 $l(m)$ 个字节。

步骤 5 求 16 个字节的加密块 S_0 为:

$S_0 = E(\text{Key}, A_0)$

步骤 6 加密鉴权标志 U 是由密流 S_0 的最左边 M 个字节与鉴权标志 T 进行异或得到的, 具体值为:

$U = T \oplus \text{first } M - \text{bytes}(S_0)$

如果上述操作正确, 通过对密文 *Ciphertext* 和加密鉴权标志 U 进行右连接形成加密消息 c , 最后被输出。

6.4 解密变换

在获得了加密密钥 K 、鉴权域的长度 M 和加密消息 c 后, 就可以对密文进行解密, 其过程如下:

步骤 1 分解接收的消息 c 为 $C \parallel U$, 最右边的串 U 是一个 M 个字节串, 如果这个操作失败, 输出无效并停止。 U 是加密鉴权标志; 最左边串 C 的长度为 $l(c) - M$ 个字节。

步骤 2 形成一个增补消息 *CiphertextData*。它是通过右连接串 C 和非负数零, 最后形成的字节串 *CiphertextData* 能整除 16。

步骤 3 同样使用加密变换的过程, 输入需求的参数 *CiphertextData* 和鉴权标志 U , 而此时的分解消息为密文 *CiphertextData*, 将它分解为每块 C_i 为一个 16 个字节串。

步骤 4 输出串为 $m \parallel T$, 最右边串 T 是一个 M 个字节串, T 为鉴权标志, 最左边串 m 的长度为 $l(c) - M$ 个字节作为输出的明文消息。

总之, ZigBee 技术通过采用这种安全策略可以保证信息的安全传输, 阻止了攻击者窃听或截取重要的信息, 保证了无线传输的安全性。

6.5 应用实例

已知条件如下:

(1) 密钥长度是 128 位, 即为:

$\text{Key} = \text{C0 C1 C2 C3 C4 C5 C6 C7 C8 C9 CA CB CC CD CE CF}$

(2) 消息长度域 L 为 2 个字节, 临时值 N 为 $15 \sim L$, 则 N 等于 13 字节, 即为:

$N = \text{A0 A1 A2 A3 A4 A5 A6 A7} \parallel \text{03 02 01 00} \parallel \text{06}$

(3) 被加密的消息数据 m 为:

$m = \text{08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E}$

(4) 鉴权数据 a 为:

$a = \text{00 01 02 03 04 05 06 07}$

(5) 鉴权域长度 M 在本例中取值为 8。

6.5.1 输入变换

(1) 形成 a 的 $L(a)$ 即为:

$L(a) = \text{00 08}$

(2) $L(a)$ 与 a 进行右连接:

$L(a) \parallel a = \text{00 08} \parallel \text{00 01 02 03 04 05 06 07}$

(3) 形成数据 *AddauthData*:

$\text{AddauthData} = \text{00 08} \parallel \text{00 01 02 03 04 05 06 07} \parallel \text{00 00 00 00 00}$

(4) 形成数据 *PlaintextData*:

$\text{PlaintextData} = \text{08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17} \parallel \text{18 19 1A 1B 1C 1D 1E} \parallel \text{00 00 00 00 00 00 00 00 00 00}$

(5) 最后形成鉴权数据 *AuthData*:

$\text{AuthData} = \text{00 08 00 01 02 03 04 05 06 07 00 00 00 00 00 00 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 00 00 00 00 00 00 00 00 00}$

6.5.2 鉴权变换

(1) 形成标志域 *Flags*, 即为:

$\text{Flags} = 59$

(2) 形成 B_0 域:

$B_0 = 59 \parallel \text{A0 A1 A2 A3 A4 A5 A6 A7 03 02 01 00 00} \parallel \text{00 17}$

(3) 分解数据 *AuthData* 为 $B_1 \parallel B_2 \parallel \dots \parallel B_i$, 每一个消息块 B_i 为 16 个字节, 最后求得 *CBC-MAC* 的值 X_i , 如表 1 所示。

表 1 B_i 和 X_i 的值
Table 1 Values of B_i and X_i

i	B_i	X_i
0	59 A0 A1 A2 A3 A4 A5 A6 A7 03 02 01 00 06 00 17	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1	00 08 00 01 02 03 04 05 06 07 00 00 00 00 00 00	F7 74 D1 6E A7 2D C0 B3 E4 5E 36 CA 8F 24 3B 1A
2	08 09 0A 0B 0C 0D 0E 0F 11 12 13 14 15 16 17	90 2E 72 58 AE 5A 4B 5D 85 7A 25 19 F3 C7 3A B3
3	18 19 1A 1B 1C 1D 1E 00 00 00 00 00 00 00 00	5A B2 C8 6E 3E DA 23 D2 7C 49 7D DF 49 BB B4 09
4	00	B9 D7 89 67 04 BC FA 20 B2 10 36 74 45 F9 83 D6

(4) 求鉴权标志 T :

$T = \text{B9 D7 89 67 04 BC FA 20}$

6.5.3 加密变换

(1)形成标志域 $Flags$,即为:

$Flags = 59$

(2)定义 A_i 域的值,如表 2 所示。

表 2 A_i 域的值

Table 2 Values of A_i

i	A_i
0	01 A0 A1 A2 A3 A4 A5 A6 A7 03 02 01 00 06 00 00
1	01 A0 A1 A2 A3 A4 A5 A6 A7 03 02 01 00 06 00 01
2	01 A0 A1 A2 A3 A4 A5 A6 A7 03 02 01 00 06 00 02

(3)分解数据 $PlaintextData$ 为 $M_1 || M_2$, 每一个消息块 M_i 为 16 个字节。

(4)计算加密块 C_i, C_2 , 如表 3 所示。

表 3 加密块 C_i 的值

Table 3 Values of ciphertext block C_i

i	$AES(key, A_i)$	$C_i = AES(key, A_i) \oplus M_i$
1	12 5C A9 61 B7 61	1A 55 A3 6A BB 6C 61 0D 06 6B 33 75 64 9C EF 10 11 D4 66 4E CA DB 54 A8
	6F 02 16 7A 21 66	
	70 89 F9 07	
2	CC 7F 54 D1 C4 49	D4 66 4E CA DB 54 A8 35 46 21 46 03 AA C6 2A 17
	B6 35 46 21 46 03	
	AA C6 2A 17	

(5)形成密文 $Ciphertext$

$Ciphertext = 1A\ 55\ A3\ 6A\ BB\ 6C\ 61\ 0D\ 06\ 6B\ 33\ 75\ 64\ 9C\ EF\ 10\ 11\ D4\ 66\ 4E\ CA\ DB\ 54\ A8$

(6)定义加密块 S_0 :

$S_0 = E(key, A_0) = B3\ 5E\ D5\ A6\ DC\ 43\ 6E\ 49\ D6\ 17\ 2F\ 54\ 77\ EB\ B4\ 39$

(7)求得加密鉴权标志 U

$U = 0A\ 89\ 5C\ C1\ D8\ FF\ 94\ 69$

(8)输出加密密文 c :

$c = 1A\ 55\ A3\ 6A\ BB\ 6C\ 61\ 0D\ 06\ 6B\ 33\ 75\ 64\ 9C\ EF\ 10\ ||\ D4\ 66\ 4E\ CA\ D8\ 54\ A8\ ||\ 0A\ 89\ 5C\ C1\ D8\ FF\ 94\ 69$

6.5.4 解密变换

(1)分解加密消息 c 为 $C || U$:

$C = 1A\ 55\ A3\ 6A\ BB\ 6C\ 61\ 0D\ 06\ 6B\ 33\ 75\ 64\ 9C\ EF\ 10\ ||\ D4\ 66\ 4E\ CA\ D8\ 54\ A8$

$U = 0A\ 89\ 5C\ C1\ D8\ FF\ 94\ 69$

(2)形成一个增补消息 $CiphertextData$:

$CiphertextData = 1A\ 55\ A3\ 6A\ BB\ 6C\ 61\ 0D\ 06\ 6B\ 33\ 75\ 64\ 9C\ EF\ 10\ ||\ D4\ 66\ 4E\ CA\ D8\ 54\ A8\ ||\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00$

(3)形成标志域 $Flags$,即为:

$Flags = 01$

(4)同样使用加密变换(2)中定义的 A_i 。

(5)分解密文 $CiphertextData$ 为 $C_1 || C_2$ 。

(6)计算加密块 P_1, P_2 , 如表 4 所示。

表 4 加密块 P_i 的值

Table 4 Values of ciphertext block P_i

i	$AES(key, A_i)$	$P_i = AES(key, A_i) \oplus C_i$
1	12 5C A9 61 B7 61	08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17
	6F 02 16 7A 21 66	
	70 89 F9 07	
2	CC 7F 54 D1 C4 49	18 19 1A 1B 1C 1D 1E 00 00 00 00 00 00 00 00
	B6 35 46 21 46 03	
	AA C6 2A 17	

(7)提取明文消息 m :

$m = 08\ 09\ 0A\ 0B\ 0C\ 0D\ 0E\ 0F\ 10\ 11\ 12\ 13\ 14\ 15\ 16\ 17\ ||\ 18\ 19\ 1A\ 1B\ 1C\ 1D\ 1E$

7 结 论

ZigBee 技术是一项最新的短距离无线通信技术。目前主要用于自动控制和远程控制领域,它是按高度省电、满足小型廉价设备的无线联网和控制而制定的,现已被业界认同为传感器网络的基本通信技术。ZigBee 技术提供了数据完整性检查、身份认证、加密等功能。不同的应用可以依据各自的具体要求灵活确定其安全属性。总之,通过对 ZigBee 技术安全的深入研究,可以进一步开发或改进其在安全方面的性能,以便保证 ZigBee 技术的生存空间。

参考文献

- [1] AKYILDIZ I F, SU W, SANAKARASUBRAMANIAM Y, et al. Wireless sensor networks: A survey[J]. Computer Networks, 2002, 38(4): 393-422.
- [2] CULLAR D, ESTRIN D, STRVASTAVA M. Overview of sensor network[J]. Computer, 2004, 37(8): 41-49.
- [3] AKYILDIZ I F, SU W, SANKARASUBRAMANIAM Y, ET AL. A survey on sensor networks[J]. IEEE Communication Magazine, 2002, (8): 102-114.
- [4] KINNEY P. ZigBee technology: Wireless control that simply works [DB/OL]. <http://www.hometoys.com/htinews/oct03/articles/kinney/zigbee.htm>, 2004-08-30.
- [5] HANDZISKI V, KOPKE A, KARL H. A common wireless sensor network architecture [R]. Berlin: Technical Report TKN-03-012 of the Telecommunications Networks Group, 2003.
- [6] EDGAR H, CALLAWY J, CALLAWAY E H. Wireless sensor networks: Architectures and protocols [M]. New York: Auerbach Publications. 2003: 260-300.

- [7] POTTIE G J, KAISER W J. Wireless integrated network sensors[J]. Communications of the ACM(S0001-0782), 2000,43(5):551-558.
- [8] CALLAWAY E, GORDAY P, HESTER L, et al. Home networking with IEEE 802. 15. 4: A developments for low-rate wireless personal area networks[J]. IEEE Communication Magazine, 2002, 40(8): 70-77.
- [9] ZigBee Alliance. ZigBee Specifications v1.0 [EB/OL]. [http://www. zigbee. org/](http://www.zigbee.org/), 2005-07-25.
- [10] HOUSLEY R, WHITING D, FERGUSON N. Counter with CBC-MAC (CCM) [DB/OL]. [http://csrc. nist. gov/ encryption/modes/proposedmodes/](http://csrc.nist.gov/encryption/modes/proposedmodes/), 2002-06-03.

作者简介



任秀丽,女,1965年2月出生,1989年于中南大学获得学士学位,分别于1999和2004年在东北大学获得硕士和博士学位,2006年博士后出站于中科院沈阳自动化研究所,现为辽宁大学教授,主要研究方向为无线网络与通信。

E-mail:rxl@lnu.edu.cn

Ren Xiuli, female, was born in February 1965. She received bachelor degree from Central South University in 1989, received master degree in 1999 and doctor degree in 2004 both from Northeastern University. She finished postdoctoral research in Shenyang Institute of Automation, Chinese Academy of Sciences, Shenyang in 2006. Now she is a professor in Liaoning University. Her main research direction is wireless networks and communication.
E-mail:rxl@lnu.edu.cn




于海斌,男,1964年10月出生,1984年于东北大学获得学士学位,分别于1987年和1997年于东北大学获得硕士和博士学位,现为中科院沈阳自动化研究所研究员,主要研究方向为工业通信和人工智能。

E-mail:yhb@sia.cn

Yu Haibin, male, was born in October 1964. He received bachelor degree in 1984, master degree in 1987 and doctor degree in 1997 all from Northeastern University. Now he is a research fellow in Shenyang Institute of Automation, Chinese Academy of Sciences. His research direction is industry communication and artificial intelligence.

E-mail:yhb@sia.cn

ZigBee技术的无线传感器网络的安全性研究

作者: [任秀丽](#), [于海斌](#), [Ren Xiuli](#), [Yu Haibin](#)
作者单位: [任秀丽, Ren Xiuli \(辽宁大学信息科学与技术学院沈阳, 110036\)](#), [于海斌, Yu Haibin \(中国科学院沈阳自动化研究所沈阳, 110016\)](#)
刊名: [仪器仪表学报](#)   
英文刊名: [CHINESE JOURNAL OF SCIENTIFIC INSTRUMENT](#)
年, 卷(期): 2007, 28(12)
被引用次数: 10次

参考文献(10条)

1. [AKYILDIZ I F, SU W, SANAKARASUBRAMANIAM Y](#) [Wireless sensor networks: A survey](#) 2002(04)
2. [CULLAR D, ESTRIN D, STRVASTAVA M](#) [Overview of sensor network](#) 2004(08)
3. [AKYILDIZ I F, SU W, SANKARASUBRAMANIAM Y](#) [A survey on sensor networks](#) 2002(08)
4. [KINNEY P](#) [ZigBee technology: Wireless control that simply works](#) 2004
5. [HANDZISKI V, KOPKE A, KARL H](#) [A common wireless sensor network architecture](#)[Berlin: Technical Report TKN-03-012] 2003
6. [EDGAR H, CALLAWAY J, CALLAWAY E H](#) [Wireless sensor networks: Architectures and protocols](#) 2003
7. [POTTIE G J, KAISER W J](#) [Wireless integrated network sensors](#) 2000(05)
8. [CALLAWAY E, GORDAY P, HESTER L](#) [Home networking with IEEE 802.15.4: A developments for low-rate wireless personal area networks](#) 2002(08)
9. [ZigBee Alliance](#) [ZigBee Specifications vl.0](#) 2005
10. [HOUSLEY R, WHITING D, FERGUSON N](#) [Counter with CBC-MAC \(CCM\)](#) 2002

相似文献(10条)

1. 期刊论文 [马斌, 赵辽英, MA Bin, ZHAO Liao-Ying](#) [ZigBee无线传感器网络在点餐系统中的应用 - 计算机系统应用](#) 2010, 19(1)

介绍了ZigBee技术的特点, 同时阐述了信息化餐饮管理的三种模式, 提出了一种基于ZigBee无线传感器网络的点餐系统设计方案. 该方案给出了点餐系统的具体管理模式, 对系统各部分的软、硬件进行了设计, 并着重阐述了无线传感器组网的过程. 研究表明, 该无线传感器网络实现了网络组建和数据通信的功能. 基于ZigBee技术的点餐系统具有低功耗、低成本、无线化、通信距离远等特点.

2. 学位论文 [马海](#) [基于ZigBee无线传感器网络的远程数据监测的设计与实现](#) 2010

无线传感器网络(Wireless Sensor Network, WSN)是一种集成了计算机技术、通信技术、传感器技术的新型智能监控网络, 已成为当前无线通信领域研究的热点. 无线传感器网络具有以数据为中心、自组织、可快速部署等特点, 非常适合一些特殊场合的应用.

ZigBee技术是一种新兴的基于IEEE802.15.4无线标准研制开发的有关组网、安全和应用软件方面的无线通信技术, 其典型特点是近距离、低复杂度、低功耗、低速率、低成本等. ZigBee技术的出现, 为无线传感器网络的发展提供了契机.

本文重点研究了如何采用ZigBee技术来搭建无线传感器网络, 并且利用ZigBee无线传感器网络实现远程数据监测. 论文首先介绍了无线传感器网络体系结构. 接着, 论文阐述了ZigBee技术的优点, 本文采用ZigBee技术作为无线传感器网络的传输载体. 以这个思路为基础, 论文详细分析了ZigBee无线传感器网络的架构, 包括网络节点类型和网络拓扑结构等, 并对ZigBee技术的组网原理作了详细的研究.

论文采用从JENNICE公司的JN5121无线通信模块及相关的软硬件开发包, 设计了整个网络的流程, 并编写相应的程序, 实现了ZigBee无线网络的组建与测试. 最后, 为了说明ZigBee无线传感器网络的应用前景, 本文给出了具体的应用实例, 论文利用所组建的无线传感器网络, 设计了一个远程数据监测系统, 实现了远程数据的采集和传输. 传感器节点通过集成在节点上的传感器模块, 采集温湿度和电压数据, 并把这些数据通过ZigBee网络传输到协调器节点, 协调器节点负责收集网络上传输过来的数据, 通过串口将数据直接发送给上位机, 或者通过GPRS网、Internet等实现远程数据传输. 文中还利用VC语言和ACCESS数据库等技术, 开发了一个简单的数据管理中心软件, 数据中心在接收到传感器网络发送的数据后, 完成对数据的解析和存储. 论文很好地融合了ZigBee技术、无线传感器网络技术和数据监测技术, 实现了远程数据监测系统的设计.

3. 期刊论文 [张睿, 刘志刚, 赵艳华, ZHANG Rui, LIU Zhi-gang, ZHAO Yan-hua](#) [基于TETRA与ZigBee的无线传感器网络研究 - 合肥工业大学学报 \(自然科学版\)](#) 2010, 33(3)

文章使用TETRA集群数据通信系统开放的PEI数据端口, 与ZigBee无线传感器网络中的主节点相衔接, 可以构成一种基于TETRA和ZigBee的二级无线传感器网络. 通过相应的研究及实验证实, 该网络能够完成远距离、大规模及低成本的传感器数据传输, 较好地满足了某些特殊应用场合的需求.

4. 学位论文 [沈澍](#) [基于ZigBee协议的无线传感器网络开发系统的研制](#) 2008

无线传感器网络是由大量微型无线传感器节点组成的自组织分布式网络智能系统, 集成了传感器、微机电系统、现代网络及无线通信、分布式信息处理技术等, 在军事、空间探索、医疗等领域中有着广泛的应用前景. ZigBee技术是一种短距离、低复杂度、低功耗、低数据速率、低成本的无线通信技术, 其特点表明了它很适合用于无线传感器网络. 本文在研究了ZigBee技术的基础上设计了一套基于ZigBee协议的无线传感器网络的开发系统. 论文

状。

其次研究了适用于无线传感器网络的IEEE 802.15.4/ZigBee的协议架构, 主要包括IEEE 802.15.4PHY层和MAC层结构、功能及主要特点; 以及ZigBee网络层、应用层的基本结构、网络实体及其功能。在研究IEEE 802.15.4 MAC协议的通信原语以及基于通信原语的组网算法的基础上, 分析了IEEE802.15.4 MAC协议和ZigBee网络层协议, 可以完成建立新网络、加入网络、离开网络等网络维护功能以及数据的发送接收、路由选择和广播通信等功能。

接着介绍了一种基于ZigBee协议的无线传感器网络开发系统的硬件设计。给出了无线传感器网络节点的设计方案, 主要包括射频SoC芯片CC2430的介绍、PCB板的设计及单板天线的设计等内容。还给出了用于无线传感器网络实验开发所要用的评估板、开发板以及仿真器的硬件设计, 主要包括USB控制器模块、电源管理模块、UART模块、控制输入模块、显示输出模块、语音扩展模块、传感器模块、外部存储器模块和扩展IO接口模块等的设计。

随后介绍了基于ZigBee协议的无线传感器网络开发系统的软件设计及实现技术。介绍了ZigBee软件编程集成开发平台, 在ZigBee协议栈Z-Stack的基础上进行了相关的软件设计, 包括操作系统的完善、硬件驱动的设计、网络配置、实例程序解析和无线温度传感器网络创建等软件设计与实现。

最后介绍了一些开发工具和系统测试。

5. 期刊论文 [赵仕俊, 张朝晖, 丁为, ZHAO Shi-jun, ZHANG Zhao-hui, DING Wei 基于ZigBee技术的石油钻井现场无线传感器网络研究 - 石油矿场机械](#)2009, 38(7)

在LEACH算法的基础上, 研究了一种基于ZigBee技术的石油钻井现场层次型无线传感器网络系统。根据石油钻井现场工况和无线网络节能的需要, 设计了层次型无线传感器网络的拓扑控制机制和路由机制以及周期性模式和中断模式2种工作模式, 并对设计方案进行了试验测试。测试结果表明, 根据所设计的拓扑控制机制和路由机制, 在周期性模式下, 网络数据传输良好, 能够稳定、可靠地对数据进行周期性地采集; 在中断模式下, 网络能够及时地对超限数据进行传输, 具有良好的预警功能。该无线传感器网络的应用能够有效弥补石油钻井现场现有的有线监控系统的不足, 对保证钻井安全生产具有重要意义。

6. 学位论文 [沈大伟 基于ZigBee技术无线传感器网络的研究](#) 2008

随着科学技术的飞速发展, 人类目前已经置身于信息时代, 信息的获取是实现信息化的前提, 获取信息的一种重要工具就是传感器。综合了传感器技术、嵌入式计算机技术、现代网络及无线通信技术、分布式信息处理技术等无线传感器网络是多学科高度交叉的新兴前沿研究热点领域。在作人员通信、环境和气象监测、灾害预警、智能家居、辐射监测等众多领域都发挥着重要作用。低成本、低功耗、应用简单的IEEE802.15.4和ZigBee协议的诞生为无线传感器网络提供了互联互通的规范。

ZigBee协议是由IEEE802.154标准的PHY和MAC层再加上ZigBee的网络层和应用层组成的, 由于网络节点具有成本低、体积小、能量和通信能力有限等特点, 所以此种网络的突出特点是网络系统支持低成本、易实现、低功耗等。

本文介绍了无线传感器网络在国内外的研究现状, 给出了无线传感器网络节点设计的方案和步骤, 分析和研究了无线传感器网络采用的802.15.4协议和ZigBee规范, 对CSMA/CA算法进行了数学分析和仿真, 并对仿真结果做了理论分析。

7. 期刊论文 [李小珉, 赵志宏, 郭志, 谭浩, Li Xiaomin, Zhao Zhihong, Guo Zhi, Tan Hao Zigbee无线传感器网络的研究与实验 - 电子测量技术](#)2007, 30(6)

ZigBee低功耗无线网络作为现存的最适合于搭建无线传感器网络的新兴技术, 目前已经越来越多的受到人们的关注。本文详细介绍了ZigBee无线协议的框架结构, 消息传输及寻址方式, 并给出了基于ZigBee无线传感器网络的组网及路由过程。最后通过使用Microchip公司提供的TS2-008 ZigBee开发套件, 进行了基于ZigBee协议的消息发送、接收及RFID设备功能实验。实验表明, 基于ZigBee技术的无线传感器网络完全可以实现消息的正常传输及组件间的相互控制, 可以最大限度地满足一般应用对无线传感器网络的要求。

8. 期刊论文 [朱祥贤, 葛素娟, 卢素锋, ZHU Xiang-xian, GE Su-juan, LU Su-feng 基于ZigBee技术的无线传感器网络应用方案 - 科技信息](#)2009(35)

介绍了无线传感器网络的重要性, 提出了基于zigBee技术的无线传感器网络技术方案, 介绍了zigBee技术的协议栈结构、ZigBee网络的节点类型、路由方法、网络拓扑结构、组网过程、TI的单芯片ZigBee解决方案cc2430, 最后介绍了基于ZigBee无线网络通信技术的某国家粮食储备库远程监控系统的的设计实例, 该系统能耗低、成本低, 寿命长, 大大节省人力, 提高安全性。

9. 学位论文 [刘辉 ZigBee无线传感器网络的设计与应用](#) 2007

无线传感器网络是当前国际上备受关注的、由多学科高度交叉的新兴前沿研究热点。无线传感器网络综合了传感器技术、无线通讯技术和计算机技术等, 具有信息采集、传输和处理的能力。低成本、低功耗、应用简单的ZigBee协议的诞生为无线传感器网络及大量基于微控制的应用提供了互联互通的国际标准, 也为这些应用及相关产业的发展提供了有力的契机。

目前, 国内主要以ZigBee技术的应用研究为主, 尚没有对外公布的协议栈。多数应用都是以Freeseale或Microchip公司所提供的开发套件为基础平台, 也有少数有自己的硬件平台, 但软件上仍然是在Freeseale或Microchip公司所提供的底层协议API接口基础之上开发实现的。

本文首先介绍了无线传感器网络和ZigBee技术的相关基础知识, 然后在现有的ZigBee硬件方案中选择了Freescall公司提供的解决方案: MC9S08GB60和MC13192, 并以此方案为背景设计开发了MT-ZigBee硬件平台。接着在深入分析ZigBee协议规范的基础上, 对ZigBee协议物理层、MAC层和网络层功能的设计与实现作了详细介绍。作为对MT-ZigBee硬件平台和协议栈可行性的测试与验证, 论文的最后以农业大棚为实际的应用对象, 组织了一个较为简单的应用实例, 验证了MT-ZigBee硬件平台和协议栈的可用性。

本文所设计实现的MT-ZigBee硬件平台与简化的ZigBee协议栈, 对于ZigBee技术和无线传感器网络的应用研究具有一定的参考价值和实际意义, 为ZigBee无线技术在工业、农业、家庭建筑和环境监测等方面的进一步应用提供了相关的软硬件基础平台, 同时也为对ZigBee协议本身的研究与改进提供了相应的工作基础。

10. 期刊论文 [丁飞, 宋光明, 李建清, 宋爱国, Ding Fei, Song Guangming, Li Jianqing, Song Aiguo 基于ZigBee无线传感器网络的家庭控制系统 - 东南大学学报\(英文版\)](#) 2008, 24(4)

提出了一种基于ZigBee无线传感器网络的家庭控制系统, 给出系统的软、硬件设计。所设计的网关节点具备网关的基本功能, 并结合了Bluetooth和GPRS通信功能, 可以支持近程和远程的综合接入。用户可以采用Pocket PC或者笔记本电脑实现实时数据的采集或者控制指令的执行, 也可以通过发送短消息的方式实行远距离的控制操作。Pocket PC的软件开发平台(包括笔记本电脑监控平台)采用的是Labview图形开发软件。除了网关以外的其他节点都采用了休眠管理来降低能耗, 并最终有效改善了整个系统的生命时间。

引证文献(10条)

1. 董方武, [华铨平, 应玉龙 基于ZigBee的棉织物丝光碱浓度监控系统设计](#)[期刊论文]-[化工自动化及仪表](#) 2010(4)
2. [李长青, 张晓芬 基于ZigBee的瓦斯传感器节点的研究](#)[期刊论文]-[通信技术](#) 2010(2)
3. [董方武 基于ZigBee的汽车空调控制系统](#)[期刊论文]-[电子技术应用](#) 2009(11)

精品女装

T恤 连衣裙 针织衫 雪纺衫棉衣 毛衣 风衣 衬衫 皮衣牛仔裤 半身裙 吊带 裤子短外套 马甲 牛仔裤 职业装

<http://www.ryanruby.info/search.php?q=%C0%CB%C2%FE%D2%BB%C9%ED&catid=16>

女士内衣

文胸 保暖内衣 塑身内衣 女袜 睡衣 隐形胸罩 内裤 情侣内衣 内衣套装 情趣内衣男士内裤 男士背心 吊袜带

美容护肤

护肤品 彩妆 香水 化妆工具睫毛膏 眼影 美甲产品 粉饼唇彩/唇蜜 眼线笔 彩妆套装假发 美发护发 睫毛增长液

数码、手机、笔记本

MP3/MP4 移动存储 电池摄像头 配件 电脑周边 蓝牙耳机 读卡器 外壳 诺基亚摩托罗拉 三星

联想 苹果 <http://www.ryanruby.info/list.php?catid=50010443>

鞋包配饰

女靴 雪地靴 女鞋 休闲鞋凉鞋 帆布鞋 手袋 钱包 手包 后背包 腰包 家纺床品时尚饰品 流行男鞋 服饰配件

超高好评+销量！O.SA2011春装 新款大码修身加厚 打底裤 SK90901

皇家遗韵 O.SA2011新品 韩版双排扣毛呢大衣 外套 女 爆款 SD81002

(亏本秒杀)&HM81501&2011新款春装 星星中长韩版针织连衣裙+围脖

包邮 新款磨白铅笔裤韩版显瘦弹力大码牛仔裤小脚裤子女休闲长裤

秒杀—促销 韩版2010秋冬新款 f758#系带修身毛领短外套 实拍

雅尼拉新品牌女装2010冬装清仓新款韩版热卖真毛领外套棉衣9202

2011春季韩版秋冬新款弹力显瘦保暖花纹多款入打底裙裤

2011春季新款雪花欧美时尚弹力多彩花纹多款入打底裤

2010秋冬2011新款春装韩版女装显瘦长款毛衣毛衣裙5折 满就减包邮

之月 细节 秋冬韩版加绒加厚保暖9分打底铅笔裤特价

7W-482-1875 包邮细节冬装女装韩版短款加厚棉袄棉衣外套棉服棉衣

2011女装 冬装清仓 大码修身保暖拉绒加厚踩脚 打底裤

2011春冬新款细节 韩版长款女装厚毛呢大衣-泡泡袖毛呢外套

2011新款春装 韩版女装 假透肉竹炭银丝超

双皇冠特价 新品阿迪达斯 adidas 男士香水100ML 冰点 激情等7款

包邮 蓝色妖姬女士香水30ml 正品 专柜 淡雅 持久清香特价限时秒杀

双皇冠正品最热卖阿迪达斯男士香水 adidas100ML 天赋香水 包快递

泡妞必备德国艾科 AXE 男士香水止汗喷雾 诱惑催情 买2瓶包快递

正品 ALOBON 雅邦香水 古龙雅邦丛林男士香水 AB6雅邦 香水 古龙香水

特价包快递 Adidas 香水阿迪达斯男士香水 天赋 卖疯了

新款 Adidas 阿迪达斯男士香水100ml 冰点 征服 纵情 能量 等7款选

皇冠包邮 天使之爱女士香水30ml 正品 专柜 持久淡香特价生日礼物

店主推荐【美国版原装正品】CK/<http://www.ryanruby.info/list.php?catid=1625>

女士服装、内衣

外套 小背心/小吊带 雪纺衫 衬衫 针织衫 连衣裙 T恤 风衣 毛衣 打底裤 文胸 文胸
套装 女袜/男袜 肚兜 情侣内衣 家居服 保暖内衣 抹胸/裹胸

帽子围巾、鞋包

围巾/丝巾 头巾 耳套 袖扣 手帕 鞋包/皮带配件 制衣面料 腰带/腰链/腰饰 手套 领带
女鞋 凉鞋 凉拖 编织鞋 运动鞋 帆布鞋 增高鞋 靴子 皮鞋

美容彩妆、护肤

美容工具 眼线笔 彩妆套装 唇膏/口红 指甲油 眼影 洁面 面膜 面部精华 身体
护理 隔离霜 去角质 唇部护理 眼部护理 面部防晒 面霜

数码产品、手机

笔记本电脑 单反镜头 三脚架 摄像服务 数码摄像机 数码相机 闪存卡/U盘/移动存储
摄像头 蓝牙耳机 游戏软件 游戏配件 MP3/MP4

3C 数码配件市场

电池 MP3/MP4配件 保护套/硅胶套 读卡器 专用线控耳机 LCD 屏幕贴膜/保护膜 笔记本
散热底座/降温卡 数据线 数码相框 数码清洁用品 手写输入/绘图板

手机卡类、游戏币

移动卡号 联通卡号 IP 电话卡 网络电话卡 GPRS/CDMA 上网卡 Skype 充值专区 影音娱
乐充值 平台专项卡 IP 卡/网络电话/手机号码 网站 ID 注册/会员卡

男士服装、饰品

T恤 Polo衫 卫衣 衬衫 牛仔裤 休闲裤 西裤 风衣 棉衣 皮衣 羽绒服 西服 夹克 西
服套装 男士内裤 男士背心 流行男鞋 男士背心

流行手表、珠宝

吊坠 项链 纯银 耳环 日韩流行 戒指 发饰 男士 手链 脚链 珍珠 情侣 水晶 琥珀 韩
饰 太阳眼镜 ZIPPO 打火机 瑞士军刀 烟具/酒具 流行眼镜 礼品刀具

影音制品、书籍

乐器 CD/DVD 电影 电视剧 教育音像 动画碟 戏曲综艺 生活百科 外语/语言文字 文
化 计算机/网络 自然科学 政治军事 娱乐时尚 育儿书籍 二手书

居家日用、收纳

完美日用 厨房用品 驱蚊/驱虫 清凉油/防暑贴/防暑用品 酒具/酒杯/酒壶 卫浴用品用具
保鲜盒 茶具 安利日用 浴室用品套件 烧烤/烘焙用具 保暖用品>

零食食品、茶叶

铁观音 奶酪/乳制小吃 糖果/果冻 水果/水产/罐头即食品 调味品/果酱/沙拉 山核桃/坚果/
炒货 火腿/腌腊制品 饼干/糕点 藕粉/麦片/冲饮品 巧克力/DIY 巧克力

办公设备、电脑 <http://www.ryanruby.info/list.php?catid=14>

打印机 传真机 墨盒/墨水 财会用品 扫描仪 内存 硬盘 有线鼠标 移动硬盘 台机电源
网卡 光驱/刻录机/DVD 电视卡/电视盒 路由器

床上用品、家饰

蚊帐| 被套| 凉席套件| 枕套/枕巾| 保健枕| 床品套件| 床单/床裙| 毛巾/浴巾| 挂帘/门帘| 布艺制品| 儿童床品| 刺绣| 音乐盒| 储蓄罐| 品牌家饰| 钟/闹钟/钟表

女装品牌、品牌女鞋

歌莉娅| 江南布衣| 欧时力| 淑女屋| 哥弟| ONLY| 艾格| VERO MODA| 阿依莲| 太平鸟| 浪漫一身| Eland| 罗马鞋| 天美意| 达芙妮| 她她| 百丽

妈妈用品、婴儿

防辐射服| 孕妇装| 亲子装| 连身衣/爬服/哈衣| 婴幼儿营养品| 妈妈护理| 宝宝洗浴护肤品| 哺乳期用品| 胎教/早教学习类| 儿童玩具/益智玩具(1岁以上)

<http://www.ryanruby.info/list.php?catid=50008090>