低速无线个人区域网802.15.4的安全研究

朱建新 高蕾娜 张新访
(华中科技大学机械学院信息与系统技术研究所 武汉 430074)

摘 要 短距离无线通信技术近年来成为通信领域热点,其主要特征是低功耗、低成本和低数据率,可广泛应用于军事、工业控制、精准农业及医学等领域的无线传感器网络构建,将会在未来的后PC即普适计算时代发挥重要作用。同时,由于其开放传输信道和"三低"特性,安全性成为保证短距无线通信网络健壮稳定运行的关键"基石"。针对低速无线个人区域网(LR-WPAN)802.15.4,详细分析其安全架构,根据最高安全级别组件AES-CCM的底层加密算法AES和泛型CCM模式,结合安全帧格式,提出了一种AES-CCM实施的输入分组模型,并进行时间性能对比实验。针对LR-WPAN可能存在的攻击和802.15.4潜在的安全问题,提出相应的改进措施。

关键词 LR-WPAN,802.15.4,安全体系,安全组件,AES-CCM
中图法分类号 TP393.08 **文献标识码** A

Research on Security of LR-WPAN 802.15.4

ZHU Jian-xin GAO Lei-na ZHANG Xin-fang
(Information & System Technology Institute, School of Mechanical Science & Engineering, Huazhong University of Science and Technology, Wuhan 430074, China)

Abstract In recent years, short-range wireless communication becomes the hotspot in wireless industry, which has the prominent characters of low-power low-cost and relaxed throughput. It can be widely used in constructing wireless sensor network of the military, industrial control, precise agriculture and medical sensors and will play an important role with the coming ubiquitous computing age. On the other hand, due to the nature of radio communications and its inherent properties, security is a key point of providing robust and reliable network. Focusing on LR-WPAN 802.15.4, this paper introduced its security architecture and presented an input block model based on the underlying AES encryption algorithm and generic CCM mode when implementing AES-CCM security suite. An experiment compared with traditional DES on time performance was carried out. As possible attacks and problems in LR-WPAN 802.15.4, several measurements were proposed.

Keywords LR-WPAN, 802.15.4, Security architecture, Security suite, AES-CCM

1 引言

近年来,无线通信连接需求呈指数级增长趋势。与目前主要的高数据吞吐量无线工业相比,短距离无线通信技术将填补在吞吐量和时延要求宽松的简单无线连接应用领域的空白。在未来的普适计算时代,短距无线通信网将可能成为构建"智能微尘"空间的关键技术,而安全性将是网络稳健运行的重要因素,因而值得进行广泛关注和深入研究。

802.15.4是2003年5月由IEEE LAN/MAN标准委员会认可的低速无线个人区域网(LR-WPAN)协议[1],旨在为简单低成本的短程通信网络提供通用平台,适合于能量、体积及计算能力限制较大但吞吐量要求不高的无线连接场合,传输速率最高可达250kbps,传输距离为10m。该协议按照国际标准组织开放系统互连(ISO-OSI)七层模型思想,定义了物理层(PHY)及媒介访问控制子层(MAC)。与现在为人熟知的蓝牙技术相比,802.15.4具有更紧凑的协议栈、更少的功耗和更低的成本,可广泛应用于工业控制、环境监测、无线传感器网络、精准农业、医疗保健、军事、物流、玩具、家庭和楼宇无线自动化控制等领域。不同的应用场合具有不同级别的安全需求,为此802.15.4提供了不同的安全模式和安全服务。当高层(如应用层)提出在发送/接收帧之前需要执行安全操作时,MAC子层将启用安全机制。

2 安全体系

MAC子层提供数据与管理两种服务,分别通过数据服务接入点(MCPS-SAP)及与管理实体服务接入点(MLME-SAP)进行访问。数据服务保证实现符合协议数据帧的传输,管理实体MLME负责维护属于MAC子层管理对象的信息库MAC PIB,这其中也包括了用于实施安全操作的数据单元。

到稿日期:2008-02-02
朱建新(1966-),男,博士,副教授,研究方向为企业信息化、嵌入式系统;**高蕾娜**(1978-),女,博士生,研究方向为无线传感器网络、信息安全;**张新访**(1965-),男,教授,博士生导师,研究方向为智能IC卡操作系统、虚拟设计与制造技术及应用。

2.1 MAC 安全帧结构与 MAC PIB 安全属性

802.15.4 MAC 帧主要由帧头(MHR)、负载和帧尾(MFR)3 部分组成。帧头主要包括帧控制、序列号和地址信息 3 部分,负载特定于帧类型(分为信标、数据、命令和确认 4 类),帧尾实际上是一个 16 位的 ITU-T CRC。MHR 中帧控制字段的安全启动位表明是否对帧实施安全保护,如果该位被设为 1,将使用存储在 MAC PIB 的安全属性对帧进行相应的安全操作。

MAC PIB 包含了管理 MAC 子层所需的各类信息,与安全有关的属性如图 1 所示。MAC PIB 安全属性包含安全模式、一个默认 ACL 入口及若干个附加 ACL 入口,授权执行特定功能的访问控制清单 ACL 提供了设备选择与之通信的其他设备的能力。ACL 可包含 255 个入口,每一个 ACL 入口对应一个设备,包含设备地址、安全组件及安全资料。默认 ACL 入口包含相似内容,但不包含地址信息。

Security mode	Default ACL entry			Additional ACL entries		
	Default security	Security suite	Security material	Address	Security suite	Security material

Name	Security services			
	Access control	Data encryption	Frame integrity	Sequential freshness(optional)
None				
AES-CTR	√	√		√
AES-CBC-MAC	√		√	
AES-CCM	√	√	√	√

Bytes: 16	4	1	(4)	(1)
Symmetric key	Frame counter	Key sequence counter	Optional replay counter	
			external frame counter	external key sequence counter

图 1 MAC PIB 安全属性

2.2 安全服务

802.15.4 MAC 子层提供 4 种安全服务(见图 1 左下方):访问控制保证每个 802.15.4 设备维护一个 ACL 设备清单,并按清单过滤设备中的传输帧;数据加密用对称密码防止被不拥有密钥的对方读取,使用由一组设备共享的密码加/解密(通常以默认密钥存储)或使用由两个对等体共享的密钥(通常存储在一个附加 ACL 入口中),数据加密可能提供在信标、命令或数据负载中,但对确认帧不提供此服务;帧完整性提供使用消息完整码(MIC)的安全服务,防止数据被不拥有密钥的对方修改,它进一步为数据来自拥有密钥的对方提供保证,对于确认帧也不提供此项服务;序列更新是可选的使用有序输入序列的安全服务,防止重放攻击,当接收帧时,需对更新值进行校验,若通过,则证明接收数据是设备中的最新数据。

2.3 安全组件

802.15.4 MAC 子层提供 3 种安全模式:非安全模式、ACL 模式及安全模式。不同的工作模式对应不同的安全级别和安全服务,由 MAC PIB 安全属性中的相应标识符指定。工作在非安全模式下的设备,MAC 子层对帧的接收及发送不提供安全操作及服务。ACL 模式不对 MAC 帧做任何加密或修改操作,仅提供给设备一种按帧中源/目的地址进行过滤的机制,并将结果指示给高层。ACL 模式下提供的安全服务是访问控制。工作在安全模式下的设备使用 ACL 功能的同时为输入/输出帧提供密码保护,依据选取的安全组件,可能提供 4 种安全服务。

工作在安全模式下的设备启用相应的安全组件。安全组件是给 MAC 帧提供安全服务的一系列操作,802.15.4 标准中含有 8 种组件(见图 1 左下方),默认设置 None 表明不执行任何安全操作。安全组件中提供帧完整性安全服务的 AES-CBC-MAC 和 AES-CCM 根据计算完整码的位长分为 32,64,128 三种。标准中所有的安全组件,使用的底层算法是 NIST FIPS Pub 197[2] 高级加密标准(AES),这个 2001 年由 NIST 发布的标准最终选择 Rijndael[3] 算法,该加密算法通过使用 128/192/256 位对称密钥和 128 位输入分组来参数化,在智能卡等 8 位及个人 PC 等 32 位处理器上性能均表现优秀。相比于 DES 加密,AES 使用加倍的密钥和分组,因此在同一密钥下加密的分组数安全范围在 2^{64} 之内[4],这对于大多数应用是足够的。

计数器(CTR)加密算法的思想最早由 Diffie 和 Hellman 于 1979 年提出[5],2001 年成为 AES 标准的 5 种推荐工作模式之一。CTR 模式能并行处理加/解密操作,在软硬件效率方面具有优势。密码分组链接消息验证码(CBC-MAC)最早是基于 DES[6] 的,此对称验证算法产生一个 CBC 模式下的完整码,通过对包含验证数据的消息进行计算而得到。底层加密函数和初始向量的随机性为安全性提供保证。CCM 是联合 CTR 和 CBC-MAC 的对称加密验证模式[7,8],其输入分组在密钥生命期内是各不相同的。

2.4 安全模式下帧的处理流程

安全模式下,输出帧的处理流程可分为以下几步:管理实体 MLME 从高层收到准备进行安全帧的传输消息后,扫描 ACL 入口,以发现与创建帧的目的地址信息相匹配的入口。如果发现匹配,MLME 将从 MAC PIB 相关字段中选择安全组件和安全加密资料;如果不能定位相匹配的 ACL 入口,MLME 将检查默认 ACL 入口的安全性字段;如果默认 ACL 入口的安全字段为 TRUE,MLME 从 MAC PIB 中选择安全组件和安全资料,否则 MLME 将通知高层;在 MLME 从 ACL 中获得合适的安全组件及安全内容后,首先将帧控制字段的安全使能子域设为 1,然后对帧进行相应的安全操作。如果安全操作中有任何失败,MLME 将通知高层;如果安全性操作成功被执行,MAC 负载字段做相应修改,设备将计算修改帧上的 CRC。

安全模式对输入帧的解密处理与输出帧的加密操作类似,MLME 在收到帧时要先检查安全启动位的设置情况,如果为 0,则通知高层;如果为 1,就通过 ACL 或默认入口找到相应的安全组件和安全内容,然后执行相应的解密及完整码验算操作。如果至少有一个安全操作失败,设备 MLME 将丢弃帧并通知高层。如果安全操作成功执行,MAC 负载字段恢复未加密的原始状态,设备继续帧的后续处理。

3 安全组件 AES-CCM 的实施

3.1 MAC PIB 安全属性中的安全资料

MAC PIB字段中的安全资料将用于安全组件的操作。AES-CTR 和 AES-CCM 的安全资料格式如图 1 右下方所示。对于 AES-CBC-MAC，安全资料只包含对称密钥 K。对称密钥 K 是一种 AES key，在执行 CTR 加密、CBC-MAC 验证和 CCM 联合加密和验证时均要用到该参数。不同的安全组件使用不同的 AES key。帧计数器和密钥序列计数器包含在发送 MAC 帧的载荷字段中，安全帧每发送一次，计数器就加 1，以确保 Nonce 的唯一性。帧计数器达到最大值后将使用密钥序列计数器。可选的外部帧计数器及密钥序列计数器用来验证接收安全帧的序列更新，以防止重放攻击。两个可选字段分别代表与该 ACL 入口所对应安全帧中最后接收到的帧计数器和密钥序列计数器的值。

3.2 AES-CCM 安全组件的实施

AES-CCM 安全组件相当于 AES-CTR 和 AES-CBC-MAC 的联合，其操作包括执行 MAC 帧头(MHR) 链接 MAC 载荷上的验证操作，以及使用帧计数器及密钥序列计数器对 MAC 载荷和完整码上的加密操作。在 AES-CCM 安全组件实施安全操作后，受保护的 MAC 帧载荷字段包含帧计数器、密钥序列计数器、加密载荷及加密完整码。图 2(a)表明了 AES-CCM 安全帧的 MAC 载荷字段子域的顺序和长度。加密载荷字段的长度等于加密之前的长度。加密完整码字段长度相应于选择完整码的长度。本文详细研究 AES-CCM 安全组件的实施，对于 AES-CTR 和 AES-CBC-MAC 仅包含相应的部分操作即可。

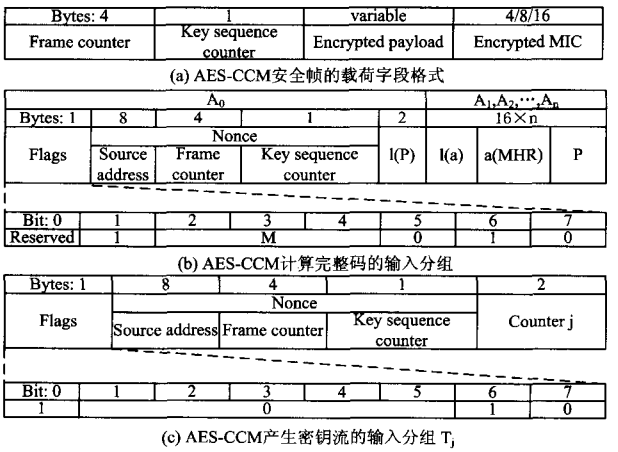

图 2 AES-CCM 安全组件的帧格式及输入分组模型

3.2.1 输入分组模型

在实施 AES-CCM 安全组件中的验证和加密操作之前，需要先确定各自的输入分组。Nonce 是两个输入分组都包括的部分，由源地址、帧计数器和密钥计数器构成。根据底层加密算法 AES 和泛型 CCM 模式，结合 802.15.4 的安全帧格式，提出了一种 AES-CCM 实施的输入分组模型：

(1)用于验证完整码计算的输入分组模型如图 2(b)所示，其中 Flags 字段中的 2～4 位 M 根据安全组件中指定完整码的字节长度减 2 后再除以 2 来进行编码，若完整码为 128 位 16 字节，则 M 段的编码应为 111((16－2)/2=7)。$l(P)$表示 MAC 帧中载荷字段的字节长度编码。A_0 是验证完整码计算中的第一个分组。用 MAC 帧中 MHR(帧头)作为额外的认证字段 a，其字段字节长度设为 $l(a)$，将 $l(a)+a$ 编码并后跟在 A_0，最后将 MAC 帧中的载荷字段作为消息 P 加在额外认证段 a 之后。$l(a)+a+P$ 组成的向量按每 16 字节进行分组，最后一个分组可能不足 16 字节，此时用 0 补齐。

(2)用于加密密钥流操作的输入分组模型如图 2(c)所示，可以看出，用于验证和加密的 Flag 字段是不同的，计数器 i 值从 0 开始，对应于需加密的 MAC 载荷字段 16 字节的分组逐次加 1。

3.2.2 AES-CCM 中的 CBC-MAC 验证码

在确定输入分组 $A_0, A_1, \cdots, A_n$ 后，对于输出帧的操作相当于利用底层 AES 算法进行验证完整码的计算，具体方法如下：

$$X_1 = E_K(A_0);$$

$$X_2 = E_K(X_1 \oplus A_1);$$

$$\cdots$$

$$X_{i+1} = E_K(X_i \oplus A_i)\ (i = 1, \cdots, n);$$

$$W = first\text{-}M\text{-}Bytes(X_{n+1})。$$

其中函数 $E_K()$表示 AES 加密算法，W 为计算得到的 M 字节完整码。

3.2.3 AES-CCM 中的 CTR 加密

计数器模式 CTR 计算加密的 MAC 载荷和加密的完整码。在确定用于加密的输入分组 $T_0, T_1, \cdots, T_n$ 后，计算密钥流分组，按以下方式产生：

$$O_j = E_K(T_j)\ (j = 0, 1, 2, \cdots, n);$$

密钥流 $O_0, O_1, \cdots, O_n$ 产生后，与 MAC 载荷字段分组进行异或操作以获得加密载荷，O_0 被用来产生加密的完整码，操作方法如下：

$$C_j = P_j \oplus O_j\ (j = 1, 2, \cdots, n-1);$$

$$C_n = P_n \oplus first\text{-}u\text{-}Bytes\ (O_n)。$$

由于载荷字段的字节数可能不是 16 的倍数，因此最后一个分组的字节数设为 u，$u \leqslant 16$。获得加密载荷后，再计算完整码的加密值，方法如下：

$$U = W \oplus first\text{-}M\text{-}Bytes(O_0)$$

在经过上述操作后，结合帧计数器、序列计数器及 C_1，$C_2, \cdots, C_n$ 和 U，获得新的如图 2(a)中所示的载荷字段。最后将帧计数器加 1 并插入 MAC PIB 相应字段。对于使用 AES-CCM 安全组件的输入帧，其安全操作包括对加密负载和加密完整码的解密，以及对完整码的验证，具体操作方法如下：

(1)如果可选的外部帧及密钥序列计数器值包含在相应的安全资料字段中，必须先验证输入帧计数器和密钥序列计数器是否大于设备 ACL 中的该值。此过程提供了序列更新的安全服务，以防止消息重放攻击。如果检查有一项失败，设备将丢弃帧，并通知高层。

(2)从输入帧或 ACL 获得源地址，从 MAC 载荷字段中提取帧计数器及密钥序列计数器来构建与输出帧相同的 Nonce。

(3)使用 AES-CTR 解密方法解密加密载荷数据和完整码，方法与输出帧中的加密方法类似，产生密钥流，进行异或操作，获得载荷 P 和完整码 W。

(4)使用输入帧中的 MHR 作为额外验证字段 a，载荷字段作为消息 P，计算完整码 W'。验证 W' 与 W 是否相等。如

果验证完整码失败，设备将丢弃帧，并通知高层。

(5)用来自于步骤(3)的解密数据替换 MAC 载荷字段。如果成功执行步骤 1 中的可选操作，将 MAC PIB 中相应密钥序列计数器及帧计数器设置为输入帧中的值。

4 应用中的安全需求及安全组件性能分析

LR-WPAN 802.15.4 工作在资源受限的环境中，因此安全操作可能成为其不能负担的额外开销。标准中的安全体系实际上体现了一种可裁剪和分级的思想，以方便应用设计实施方根据不同需求选择相应安全服务。适用场景之一的家庭照明及玩具中的无线控制可选用非安全模式或 ACL 模式，而对于工控、医疗及军事等高安全级应用则应采用安全模式的相应安全组件。对于同种设备而言，也可使用不同的安全应用，AES-CTR 和 AES-CCM 中的安全资料是完全相同的，可根据具体需要选取不同的安全组件。无线传感器网络是 802.15.4 标准适用的重要应用，网络中的设备分为全功能设备(FFD)和简化功能设备(RFD)。采用星型拓扑的协调器节点(FFD)由于具有较高的存储和计算能力，必要时可选用 AES-CCM。而对于 RFD 节点，由于资源非常有限，适宜采用低级别安全工作模式。

由上分析可知，安全组件的时间性能主要取决于底层加密算法 AES 和异或操作。理论分析表明，AES-CTR 和 AES-CBC-MAC 的耗时相当，近似等于 AES 加密时间加上进行异或操作的时间 $T(E_k)+T(XOR)$，AES-CCM 为 $2[T(E_k)+T(XOR)]$。在 VC 中实现了 128 位密钥的 3 种安全组件的加/解密并与传统 DES 算法进行对比，主要包括头文件 AES.h 和源文件 AES.cpp，AES-CTR.cpp，AES-CBC-MAC-128.cpp 和 AES-CCM-128.cpp，分别完成 Rijndael 算法及在 AES-128 位分组密码下 CTR 模式和 CBC-MAC 模式的加解密，CCM 模式是前二者的结合。选取 1k～300k 字节范围内的 10 个不同文件进行实验(见表 1)。实验 PC 机具有 P4 2.4GHz 的 CPU 和 512M 内存。依次提取文件中的 16 字节作为计算完整码的输入分组，设定一个 16 字节的字符数组作为产生密钥流的输入分组，实施方法如上所述。表 1 是 3 种安全组件在 5 次随机实验的加密耗时记录平均值(第一行表示加密文件的 kB 大小，第一列表示加密算法名称，表格的其余内容表示相应的加密耗时，单位为 ms)并绘制图 3，结果与理论分析一致。从图 3 可看出，AES-CCM 的执行效率高于 DES，且由于加倍的密钥和分组，因此具有更高的安全强度。

表 1 安全组件与 DES 加密耗时

	1	10	20	32	40	51	61	74	83	93	110	154	207	253	300
AES-CBC-MAC-128	0	28	47	94	103	129	157	194	222	244	272	391	513	625	731
AES-CTR	0	25	59	81	115	144	156	194	213	244	278	391	516	631	734
AES-CCM-128	0	56	100	162	210	244	312	382	403	453	553	750	1022	1228	1475
DES	0	62	134	194	241	306	378	459	516	584	684	947	1350	1519	1841

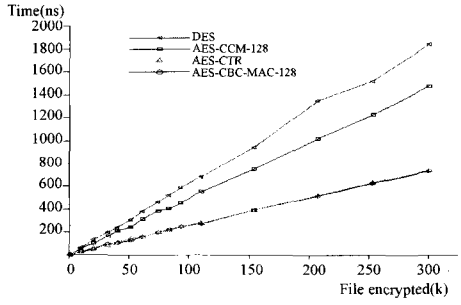

图 3 加密文件与耗时

5 LR-WPAN 802.15.4 安全性分析

5.1 LR-WPAN 可能存在的攻击及改进措施

LR-WPAN 在 PHY 和 MAC 层可能存在的攻击主要包括：无线干扰；捕获和篡改；资源耗尽；冲突及不公性。由于无线通信的天然特性，收发器启动设备将能接收和解码所有当前工作在相同信道及 POS(personal operating space)范围之内且遵循 802.15.4 标准设备所发出的消息，连同其他干扰源。LR-WPAN 在 PHY 层易受到干扰攻击的原因在于极低的传输能量。由于实施充分的物理保护会违背低成本的设计目标，捕获和篡改在 LR-WPAN 很难避免。虽然对于一些重要设备(如 PAN 协调器或持有敏感信息的设备)可能提供强大的物理保护，大多数设备会由于不提供保护而受到此种攻击。资源耗尽从服务可用性角度看是一种拒绝服务(DoS)攻击。一种强势攻击可由一个受损协调器发起，它可以显示高连接质量及低级别吸引大量节点与之连接，然后通过发送故意配置的信标强迫所有连接设备保持主动状态，从而导致能量的快速耗尽。冲突攻击通常是由偏离协议开始的，攻击方对于敏感的控制和管理帧能有选择地建立冲突。例如，确认帧冲突将使发送方的退避时间呈指数级增加；连接应答帧冲突将迫使设备从一开始就实行多步连接过程；信标启动协调器中的信标帧冲突将引起其孩子节点成为孤节点。不公性是 LR-WPAN 面临的另一个问题，虽然通常不会关闭整个网络，但能很大程度降低网络性能。媒介访问点是不公性攻击最易实施的环节。LR-WPAN 中，非时隙 CSMA-CA 用于非信标启动模式下的信道访问，时隙 CSMA-CA 用于信标启动模式下的竞争访问阶段(CAP)。在信标启动模式下，伪节点仅通过跳过退避和空闲信道评估(CCA)过程而在接收信标后直接捕获信道。在非信标启动模式下，伪节点能通过使用更小的退避周期或 CCA 持续时间取得访问信道的优先权。由于 802.15.4 没有使用如 802.11 中的严格机制以防止在一幅帧和相应确认帧之间存在其他传输，通过连续发送消息，伪节点能有很好机会保持对信道的控制，其他节点在伪节点完成所有传输之前，几乎不可能传输消息。Zheng 等人[9]利用 NS-2 模拟器对上述攻击进行建模并给出结果，从而验证了它们对 LR-WPAN 网络性能带来的危害。

以下提出一些改进措施以对抗或减轻潜在攻击给网络造成的影响：

(1) 干扰攻击紧密与 PHY 层有关，通常节点在遭遇此类攻击时并不能自动抵御。扩频技术可能是有效的抵抗措施之一。然而，由于简单性和低成本需求，如何匹配两设备之间的扩频伪随机码是值得深入研究的。对于像战场通信等需要高

可靠性和安全性的应用，有选择性地在一些重要设备（如PAN协调器、其他协调器及负责网络管理的设备）中装备扩频功能模块，以使它们能有效地抵抗干扰。虽然不对整个网络提供保护，小数量的保护设备将能执行关键的管理功能。还可在其中引入入侵检测技术，监视网络行为并在需要时请求人为干预。多频段信道的可用性也可提供针对干扰攻击的保护。

（2）与连接有关的资源耗尽攻击可通过验证敏感信息（如源地址和数级）来防止，可能需要使用公钥方案和证书服务。

（3）信道访问不公性问题主要来源于错误假设所有节点将会严格遵守协议[10]。一种抵抗措施是融合基于竞争和非竞争的方案。在LR-WPAN中，协调器可以在每一超帧开始时分配minislots，并以随机顺序分配给单独设备，分配信息包含在信标负载中。每一个需要访问信道的设备需要等待，直到它的minislot到来，它们应足够短而不引起大的时延。设备在minislot之内如有等待数据时，开始发送数据，而如果没有等待帧，它马上放弃minislot以使其他设备能访问信道。为阻止伪节点无间隔地连续发送数据，可按照某种机制将minislots插入竞争访问阶段（CAP）。

5.2 802.15.4安全问题及改进

一种802.15.4设备可使用255个ACL入口存储不同的密钥及相关Nonce，发送方基于目的地址选择合适的独立ACL入口。然而，如果两种不同的ACL入口使用相同密钥，发送方将很有可能因为重用Nonce而出现安全漏洞。例如，假设发送方使用AES-CTR安全组件，对于接收方 r_1，r_2 使用相同的密钥 K，初始化两个接收方的帧计数器和密钥计数器都设置为 N_0：0x0。如果发送方传输带有数据0xAA00的消息 m_1 给 r_1，加密后的数据为 $m_1 \oplus E_k(N_0)$，同时传输带有数据0x00BB的消息 m_2 给 r_2，密文为 $m_2 \oplus E_k(N_0)$，攻击方通过计算两个密文的异或值 $(m_1 \oplus E_k(N_0)) \oplus (m_2 \oplus E_k(N_0)) = m_1 \oplus m_2 =$ 0xAABB，从而获得纯文本的异或操作结果，这就完全破坏了机密性。对于群密钥或网络密钥加密模式将很有可能因为不同ACL入口使用相同密钥而造成Nonce重用问题[11]。同时，由于许多802.15.4设备是通过电池或太阳能供电，在出现低能量操作或能量失效时，如果出现清空的ACL表，将会再次出现Nonce值重用而破坏机密性。

当使用网络内的单一共享密钥（网络共享密钥模型）时，802.15.4的安全实施必须使用默认的ACL入口，此时将很有可能在重放攻击保护时出现问题。假设网络共享密钥装入默认ACL，节点 s_1 发送100条消息时使用重放计数器0～99，接收方获取这些帧并执行重放保护操作，每次接收帧后就更新默认ACL入口中的重放计数器，因此保存了最大重放计数器值99。如果发送方 s_2 发送一条消息，重放计数器值从0开始，接收方将会拒绝此消息，因为它只接受重放计数器大于99的帧。因此，如果接收方使用共享密钥模型下的重放保护，接收方必须调整重放计数器空间的使用。

标准中使用计数器加密模式的AES-CTR安全组件，并不使用认证码MIC。研究者已经发现在使用加密保护仅跟一个CRC而不跟加密MIC码的协议中将产生很多弱点。所有的攻击集中于这个事实：在修改密文的过程中，攻击方能对CRC作出合适的修改以使接收方接收帧。研究者已经在IPSec，802.11及SSH V1中发现了未认证的加密不仅损害完整性，同时损害机密性[12]。任何使用AES-CTR安全组件的应用都将受到相似攻击的威胁。另外，使用重放保护的AES-CTR安全组件还可能遭遇单帧拒绝服务攻击。假设一个发送方 S 和接收方通信使用密钥 K 的AES-CTR组件，接收方启动了重放保护。接收方保持一个由 K 和计数器组成的高标记位，拒绝接收小于此标记的帧。若攻击方发送一个带有源地址 S 的伪造帧，密钥计数器为0xFF，帧计数器为0xFFFFFFFF及任何的负载（可能是非有效的密钥 K 下的密文），接收方将用 K 解密帧并产生随机垃圾。由于没有消息认证，接收方将接收带有垃圾的帧。然而，在将错误负载传给应用之前，MAC层将更新高标记值为0xFFFFFFFF。下一次当真正的发送方 S 发送合法帧时，由于高标记位已经达到了最大值，接收方将拒绝任何帧。这表明如果使用带有重放保护的AES-CTR，攻击方能永久中断802.15.4连接。

802.15.4标准并没有对确认帧包含任何完整性或机密性保护。当发送一条帧时，发送方可在flag字段的确认请求位中设置是否需要从接收方反馈确认消息。如果确认请求位设置为真，接收方返回一条包含帧序列号的确认帧，发送方的MAC层在没有收到确认消息时会发送该帧有限次。然而，确认中缺少MAC允许攻击方对任何帧伪造确认帧。攻击方仅需从原始帧中获取合适的序列号创建伪造的确认帧，由于序列号是原样发送，这并不难做到。假设攻击方确定一条希望不被预定接收方接收的帧，并在帧发送时传输一小段干扰脉冲以引起CRC在接收方的失效而被丢弃，然后攻击方伪造一条看似有效的确认帧，欺骗发送方以为帧被接收。这种脆弱性导致当攻击方存在时确认帧的不可靠性。如果发送应用收到确认，它并不能确保数据是否真正到达目的地。

针对以上802.15.4安全体系中可能存在问题的分析，提出以下一些改进措施及建议：

（1）粗粒度的ACL控制将会导致单独ACL入口共享同一密钥，进而带来安全威胁。尝试解决方法之一是为密钥 k 创建单一的ACL入口。在发消息至节点 n_1 之前，将此ACL入口中的目标地址改为 n_1；如果以后需发送消息至 n_2 并使用同一密钥，必须将此ACL入口中的目标地址改为 n_2。也就是说，每次当发送帧时必须修改目标地址，这可能会增加帧传输过程的复杂度。如果接收方采取同样的地址转换策略，它须确保在发送帧到达之前具有一个相应于发送方的ACL入口，接收方因此须能预测哪一个节点会接着发送消息，以使ACL入口能被正确建立。

（2）在节点碰到能量失效后，如果不采取措施，节点在能量恢复后可能会出现清空的ACL表而破坏安全性。改进方法是：将计数器存在不可擦除的Flash内存中，在发送一个分组后就加1。也可一次保留若干个Nonce值并将最大值写入Flash，在能量恢复之后，无线芯片使用比Flash中保留的更大的一组Nonce值。由于写Flash操作，后者的效率可能更高。由于芯片知道何时进入及退出低耗模式，可利用软件保存及恢复Nonce状态。

（3）在网络共享密钥模型下使用默认ACL入口，很可能出现与重放保护不兼容的问题。问题来源部分是由于混淆了Nonce和重放计数器的角色。输出帧中的Nonce有两个目的：为保持机密性，发送方必须确保针对同种密钥不会使用相

同的 Nonce;为防止重放攻击,接收方需确保每个发送方使用单调增加的 Nonce 值。第一种需求表明 Nonce 应该强硬地与 Key 绑定:任何的密钥使用,即使是在不同的 ACL 入口,应该共享单一的 Nonce 寄存器。反过来,第二种需求表明重放 Nonce 计数器应该强硬地与发送方地址绑定:如果相同的密钥出现在多个 ACL 入口中,应该各自维护每个发送方的高位标记。确保机密性的发送和保护重放攻击的接收的相反需求对 ACL 结构提出了不同要求。将用于输出帧的 Nonce 与用于输入帧的重放计数器进行存储解耦能更好地支持组加密或群加密模型。解决方案之一是 802.15.4 芯片为实施自有的重放探测提供应用层 API 支持。当指示高层帧到达时,芯片应该提示重放计数器值,从而在应用级接管每一个发送方的计数器高标记值。这允许当一种密钥被一组节点共享时,接收方能实施重放保护。

(4) AES-CTR 由于未认证的加密而引入协议级的安全威胁。802.15.4 标准对 AES-CTR 的支持是可选的,AES-CCM-64 是推荐必须支持的安全组件。因此,在高安全级别需求的应用场合建议不使用 AES-CTR。

(5) 由于确认帧缺少加密和认证支持,攻击方可从原始帧中获取合适序列号创建伪造的确认帧,这种脆弱性导致当攻击方存在时确认帧的不可靠性。改进方法是增加认证的确认选项,这些确认仅可能通过与发送方共享密钥的节点产生。例如,取代从原始帧中包含 1 字节序列号的方式,接收方使用 4 或 8 字节的 MIC 缓冲,由接收帧地址构成。发送方在发送帧之前计算 MIC 值并保存,在收到确认帧后,比较该值与确认帧中的值。如果通过验证才被认为是有效确认帧,攻击方由于不能访问收发双方共享的私钥而得到正确的 MIC 值。

结束语 LR-WPAN 802.15.4 是近年新兴的短程无线通信网络,因其低成本、低功耗等特点而受到业界的关注。ZigBee 联盟 2005 年 7 月发布了基于 802.15.4 的网络及应用层协议,目前市场上出现越来越多的 ZigBee/IEEE 802.15.4 开发平台和产品,安全性是其重要组成部分。本文较为深入地研究了 LR-WPAN 802.15.4 的安全机制,在分析安全体系基础之上,对安全组件 AES-CCM 实施的输入分组建模并进行性能实验,验证了效率及安全强度。针对低速短距无线网和 802.15.4 中可能存在的安全问题,给出相应的改进措施。安全服务的有效性很大程度上取决于密钥管理方案的选择,这将是今后的研究重点。

参 考 文 献

[1] IEEE Computer Society. Standard for part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specification for Low-Rate Wireless Personal Area Networks (LR-WPANs)[S]. IEEE Std 802.15.4,2003

[2] National Institute of Standards and Technology (NIST). Federal Information Processing Standards Publication 197 (FIPS PUB 197): Specification for the Advanced Encryption Standard (AES)[S]. NIST,2001

[3] Daemen J, Rijmen V. The Block Cipher Rijndael[C]. Lecture Notes in Computer Science. Berlin Heidelberg: Springer-Verlag. 2000:277-284

[4] Walker J. 802.11 Security Series, Part III: AES-based Encapsulations of 802.11 Data[EB/OL]. Platform Networking Group Intel Corporation. http://cache-www.intel.com/cd/00/00/01/77/177-70_80211_part3.pdf

[5] Diffie W, Hellman M E. Privacy and authentication: An introduction to cryptography[C]. Proceedings of the IEEE, 1979, 67(3):397-427

[6] Bellare M, Kilian J, Rogaway P. The Security of the Cipher Block Chaining Message Authentication Code[J]. Computer and System Sciences, 2000, 61(3):362-399

[7] Whiting D, Housley R, Ferguson N. Submission to NIST: Counter with CBC-MAC (CCM), AES Mode of Operation[EB/OL]. http://csrc.nist.gov/encryption/modes/proposedmodes/ccm/ccm.pdf, 2002

[8] Jonsson J. On the Security of CTR+CBC-MAC[C]// Cryptography: 9th Annual International Workshop, SAC 2002. St. John's, Newfoundland, Canada. Berlin Heidelberg: Springer-Verlag, 2003

[9] Zheng Jianliang, Lee M J, Anshel M. Toward Secure Low Rate Wireless Personal Area Networks[J]. IEEE Transactions on Mobile Computing, 2006, 5(10):1361-1373

[10] Misic J, Shafi S, Misic V B. Performance limitations of the MAC layer in 802.15.4 low rate WPAN[J]. Computer Communications, 2006, 29:2534-2541

[11] Sastry N, Wagner D. Security Considerations for IEEE 802.15.4 Networks[C]// WiSe'04. Philadelphia, Pennsylvania, USA, October 2004

[12] Bellovin S M. Problem areas for the IP security protocols[C]// Proceedings of the Sixth Usenix UNIX Security Symposium. 1996