ZigBee 传感网的一种新型安全方案①

施　鹏，赵华伟

(山东财政学院 计算机信息工程学院，济南 250014)

摘　要：研究了目前传感网存在的安全隐患，针对主要攻击手段提出一种简单可行的安全方案。该方案包括两部分：1.以帧的序列号为初始向量，采用 AES 算法对相应的 PANID(个人区域网络标识符)进行加解密；2.根据接受帧的序列号对接收帧的有效性进行判断。由此，该方案在保证 PANID 的机密性、防止伪装攻击方面有着比较显著的效果。

关键词：ZigBee；传感网；伪装攻击；安全方案；AES

New Security Solution of ZigBee Sensor Network

SHI Peng, ZHAO Hua-Wei

(School of Electronic Science and Technology, Shandong Institute of Finance, Jinan 250014, China)

Abstract: For the ZigBee sensor network is still not safe enough, this article proposes a simple feasible security solution. It contains two parts. First, with the frame series number as the initial vector, using the AES algorithm encrypts /decrypts the cor responding PANID. Second, judge the validity of the frame received according to the series number. Actually,this solution has a significant effect on ensuring PANID security and preventing disguised attack.

Key words: ZigBee; sensing network; disguised attack; security solution; AES

1　引言

近十年来，随着半导体技术和无线通信技术的不断发展，无线传感网的研究和应用正在世界各地蓬蓬勃勃地展开，具有成本低、体积小、功耗低的 ZigBee 技术无疑成为目前无线传感网络中，作为无线通信应用的首选技术之一。因此，无论是自动控制领域、计算机领域、无线通信领域对 ZigBee 技术的发展、研究和应用都寄予了极大地关注和重视。

ZigBee 是一组基于 IEEE802.15.4 无线标准而研制开发的有关组网、安全和应用软件方面的通信技术；其实现了在数千个微小的传感器之间相互协调通讯。这些传感器只需要很少的能量，就能以接力的方式通过无线电波将数据从一个节点传到另一个节点，从而实现在全球 2.4GHz 免费频带范围内的高效、低速率的通讯功能。同时，该技术具有数据传输速率低、功耗低、成本低等特点。所以，该技术现已成功的运用于农业生产，工业控制，生物医疗，智能家居，环境监测，智能建筑和医疗等领域。

本文首先对 ZigBee 技术的协议体系结构以及通信原理进行简单的阐述，主要包括物理层协议、MAC 层协议、网络层协议等；在此基础上，概括当前 ZigBee 技术中主要的安全方案和分析在实际应用过程中所存在的隐患和缺陷；最后，在结合 ZigBee 体系构架的前提下，提出一种全新的可行安全方案，并对该方案的有效性进行了科学性的论证。

2　ZigBee传感网的工作原理

2.1 体系构架

在 ZigBee 技术中，其体系机构通常由层来量化它的各个简化标准。每一层负责完成所规定的任务，并且向上层提供服务。各层之间的接口通过所定义的逻辑链路来实现[6]。ZigBee 技术的体系结构主要由物理层(PHY)、媒体接入控制层(MAC)、网络/安全层（NWK)以及应用框架层(APS)组成。其中，PHY 层的特征是

① 收稿时间:2010-11-24;收到修改稿时间:2011-01-16

启动和关闭无线收发器，对能量、链路质量进行检测，选择信道，清楚信道评估（CCA)，以及通过物理媒体对数据包进行发送和接收。MAC 层的特征是信标管理，信道接入，时隙管理，发送确认帧，发送连接及断开连接请求。除此之外，MAC 层为应用合适的安全机制提供一些方法。网络/安全层（NWK)的特征是用于 ZigBee 的 LR-WPAN 网的组网连接、数据管理以及网络安全等。应用框架层（APS)的特征是用于为 ZigBee 技术的实际应用提供一些应用框架模型等，以便对 ZigBee 技术的开发应用。

基于 ZigBee 技术的无线传感器网络通常存在两种不同类型的设备：一种是具有完整功能的设备（FFD)，一种是简化功能的设备(RFD) [8,9]。在网络中，FFD 通常有 3 种工作状态:⑴作为个人区域网络(PAN）的主协调器；⑵作为一个协调器；⑶作为一个终端设备。一个 FFD 可以同时和多个 RFD 或多个其他的 FFD 通信，而对于一个 RFD 来说，它只能和一个 FFD 进行通信。其工作过程如图 1 所示[1]。

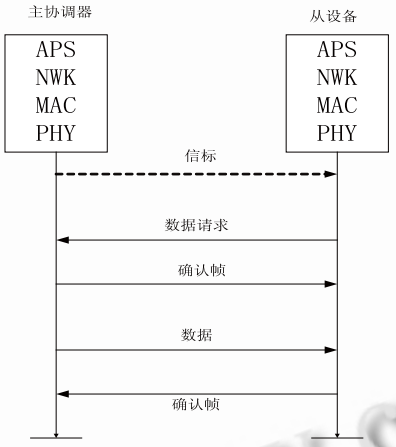

图 1

2.2 通信原理

在 ZIGBEE 体系中，存在网间通信和网内通信两种方式。由于，网内通信与网间通信相类似。因此，本文以网内通信为例阐述其通信原理。其通信过程如图 2 所示[1,2]。

2.2.1 网络形成

FFD 设备首先根据来自网络层的初始化命令；并结合应用层所设定的信道标号（Channel ID)、个人区域网络标识符（PAN ID）以及本主协调器的网络地址（Net Address)，进行相关信息的初始化和信道扫描。若指定的 Channel ID 和 PAN ID 不与现存网络冲突，则开始形成网络；若指定的 Channel ID 和 PAN ID 与现存网络冲突，则从备选的信道中选择另外一个信道，避免在该信道中 PAN ID 不冲突；形成网络并开始监听指定信道的网络数据[9]。

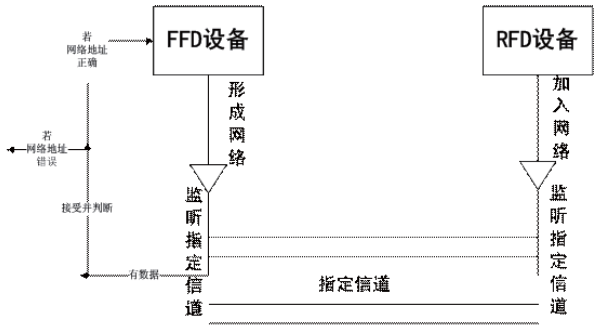

图 2

2.2.2 网络连接

当 RFD 开始工作时，其首先根据应用层所设定的信道标号（Channel ID)、目的区域网络标识符（PAN ID）以及本设备的网络地址（Net Address）进行相关信息的初始化和主动的信道扫描；以确定其是否网络存在。当确定网络存在以后，网络层发送连接请求原语到媒体接入控制层（MAC 层)；MAC 层就会根据其指令，生成连接请求的数据帧，该数据帧中除了包含自身的网络地址（Net Address）外还包括所要加入的区域网络的标识符（PAN ID）[7]。进而指示物理层检测当前发送机状态；若当前发送机已经打开，并且处于空闲状态，则就在指定的信道中发送连接请求数据[2]。

至此，整个 ZIGBEE 网络体系形成；可以开始进行相关的通信。

3 现存安全方案的隐患和缺陷

在现存的安全方案中，无论是计数模式加密还是密码块链消息认证码；其更多的是注重保证应用数据的安全；但是这并不代表能够保证整个 ZigBee 网络的安全。由于安全方案大多数针对 MAC 层载荷（应用数据）;而没有对 MAC 帧头信息进行必要的保护；使得无线传感网与互联网类似，也存在很多的攻击。其中，最典型的攻击是伪装攻击[5]。

根据攻击的方式不同，伪装攻击可以分为主动伪装攻击和被动伪装攻击。

3.1 主动伪装攻击

在 ZigBee 协议中，无论是连接请求或连接回应都是以 MAC 帧为载体。并且在传输过程中，无论是否采取安全方案，其 MAC 帧头信息都是以明文形式传输的。这就会使攻击者通过 Sniffer 等专业工具获取目的 PAN 标识符(PANID)和源 PAN 标识符(PANID)；进而可以根据所获得 PAN 标识符伪装成合法协调器或协调器，与网络中的其他设备进行连接。

3.2 被动伪装攻击

在网络连接或数据传输过程中，即使数据包使用了密文形式，也不能完全阻止攻击者进行攻击。这是因为，攻击者仍然可以通过专业工具获得密文形态的数据包。进而，就可以在以后的某个时间，重新发送该密文形式的数据包，使得网络中的其他设备误以为是正常连接，导致整个网络陷入瘫痪[7]。

4 新的安全方案

通过对于伪装攻击的介绍可知：主动伪装攻击实施成功的原因在于 MAC 层帧头信息没有必要的保护；使得攻击者能够获得目的 PANID 等相关机密信息；而被动伪装攻击实施成功的原因是由于接受机制没有对接受数据进行一个有效性的判断。在本文中，提出一种可行性安全方案。即在 MAC 层中添加一个模块；该模块包含两个功能：1.以帧的序列号为初始向量，采用 AES 算法对相应的 PANID 进行加解密；这样就可以对 PANID 进行合理保护，使得攻击者无法获得 PANID。2.根据接受帧的序列号来对接受数据的有效性进行判断，从而使攻击者的重发数据无效[1]。

具体流程如图 3 所示：

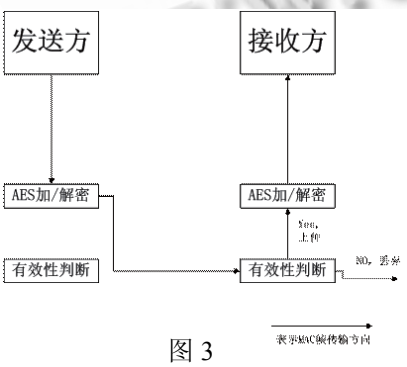

图 3

发送方发送数据时，在生成 MAC 帧以后，选用帧头信息中的帧序列号作为初始向量，对 PAN 标识符进行 AES 算法加密。完成相关的加密动作后，交由物理层进行数据的发送。接收方接受数据时，首先，除了进行网络地址的判断外，在交由 MAC 层进行处理前；还要由帧的有效性判断机制来判断接受帧的有效性；若无效，则丢弃；反之，则提取当前帧的序列号，并进行 AES 算法的解密。最终，将所解密后的 MAC 帧交由 MAC 层进行进一步的处理[3-6]。

4.1 AES 加/解密

加/解密对象是 MAC 帧头信息中的 PANID 区域；加/解密的初始向量是当前帧的序列号；由于加密的时机是在 MAC 层生成 MAC 帧以后。其优点在于由于采用了序列号作为初始向量；使得每次加密后的 PANID 值不相同；并且由于加密时机是选择在 MAC 层中来完成，不用去修改 ZigBee 原有的体系结构。

4.2 帧的有效性判断机制

该机制由两部分构成；一部分是相应的序列号表格，用来记录已处理过的帧的序列号和当前正在处理的序列号；另一部分是帧的有效性判断模块，其作用是根据已设置的有效性判断规则，对当前帧进行有效性判断。

(1) 保证了 PANID 的机密性

由于在每次发送 MAC 帧时，都要事先以序列号作为初始向量，对 PANID 号进行 AES 算法加密；进而保证每次发送的 MAC 帧的 PANID 不同，使得无法借助数理统计的方法获得真实的 PANID。

(2) 保证了接受帧的有效性

由于在每次接受 MAC 帧时，通过对其序列号的有效性进行判断，能够保证该帧的有效性。若判断为无效，则对该帧进行丢弃处理；进而能够有效地防止被动伪装攻击攻击。

本方案之所以能有效的防止伪装攻击；是由于对 PANID 进行了加密；大大增加了攻击者获得真实 PANID 的难度。在本文中，将通过构造线性回归方程模型以及最小二乘估计的技术手段来论述攻击者是如何进行 PANID 破获，并指出其攻击难度。假定 R 表示参与运算的帧序列号，X 表示真实的 PANID 值，Y 表示加密后的 PANID 值。

构造线性回归方程模型：

首先，根据相关的统计方法，选择规模为 N 的样本数据：(Yi, Xi, Ri), i=1,2,…,n ①;

其次，假定 Y 与 X 和 R 成线性相关；即：

Y=β0+β1X+β2R+α ②;

其中，β0、β1、β2 为未知参数；α 为随机误差，且其服从标准正态分布；

由①和②可得：

Yi=β0+β1X i+β2Ri+α i; i=1,2,⋯,n ③;

其中，α1,α2,⋯αn 相互独立，且均服从标准正态分布，③就是所构造的线性回归方程模型；

最小二乘估计

线性回归方程构造完以后，需要去对未知参数进行估计，从而才能获得确定函数关系。

在这里，采用最小二乘估计法估计未知参数。

由最小二乘原理得正规方程组 X'Xβ=X'Y; ④

其解为β0、β1、β2 的最小二乘估计。

那么，Y 的回归值 y=β0+β1X+β2 R;

根据δ2 无差估计理论可知：当α i (i=1,2,⋯,n) 满足服从标准正态分布时；y 就可以取代 Y。换言之，就可以根据 y=β0+β1X+β2 R 来推算得到 X。

在整个运算过程中，攻击者从拿到数据到推算得出 X；中间有几个必要环节需要解决：

样本的数据选取问题；样本的好坏决定了所构造的正规方程组的好坏，以及α i (i=1,2,⋯,n)的无差估计是否成立。由于安全方案采取的以序列号为初始向量的 AES 加密，这就使得加密后的数据杂乱无章，进而使得在选择样本数据时毫无规律可言。样本数据选择不好，就无法进行有效的最小二乘估计。

影响因变量 Y 的因素确定问题。建立回归方程的前提，就是首先要确定自变量的个数以及种类。在本方案中，我们除了把 PANID 作为自变量以外，还选择帧的序列号作为自变量。这样对于攻击者而言，其无法清晰地获得自变量的个数和种类，从而无法构造比较合适的回归模型，进而无法进行深入的数学推算。

5 总结

在现存的 ZigBee 协议中，伪装攻击是比较有效的一种攻击方式。针对于此，本文在同时考虑到物联网各设备计算能力有限的情况下，提出了一种有效的安全方案。理论证明，该方案在保证 PANID 机密性、防止伪装攻击等方面，有非常显著的效果。

参考文献

1 刘旭东.无线传感器网络上的攻击.中国科技信息,2005,12(8):46-54.

2 杨伟丰,汤德佑,孙星明.传感器网络安全研究术.计算机应用研究,2005,32(1):33-35.

3 VRaghunatha C, Srivastava SM. EnergyAware wireless mierosensor networks, 2002,34(16):11-17.

4 Cagalj M, Capkun S, Hubaux J.P. Wormhole-Based Anti-Jamming Techniques in Sensor Networks. IEEE Trans. on Mobile Computing, 2007,8(1):58-62.

5 沈苏彬,范曲立,宗平,毛燕琴,黄维.物联网的体系结构与相关技术研究.南京邮电大学学报(自然科学版),2009,12(6):78-89.

6 王建刚,王福豹,段渭军.加权最小二乘估计在无线传感器网络定位中的应用.计算机应用研究,2006,(9).

7 王保云.物联网技术研究综述.电子测量与仪器学报,2009,5(12):45-50 .

8 孔晓波.物联网概念和演进路径.电信工程技术与标准化,2009,9(12):18-29.

9 宋合营,赵会群.物联网分布式识读器数据采集方案设计与实现.北方工业大学学报,2008,2(1):66-98.