第34卷 第17期 计 算 机 工 程 2008年9月
Vol.34 No.17 Computer Engineering September 2008
·工程应用技术与实现· 文章编号：1000—3428(2008)17—0216—03 文献标识码：A 中图分类号：TP393.1

ZigBee接入EPA网络的安全策略

魏 旻，王 平，胡国珍，王 泉
(重庆邮电大学重庆市网络控制技术与智能仪器仪表重点实验室，重庆 400065)

摘 要：针对ZigBee技术的特点，结合EPA控制网络的安全规范与工业现场实际应用的需要，提出ZigBee接入EPA网络的安全策略与基于安全组态的实现方法。测试表明，通过安全组态增加了设备鉴别、访问控制等安全措施的ZigBee接入点设备和现场设备，有效提高了EPA中ZigBee网络的安全性能，且运行稳定、工作可靠，满足了工作现场的多种需要。

关键词：无线；EPA总线；工业控制；ZigBee技术；安全

Security Strategy for ZigBee Access to Ethernet Process Automation Network

WEI Min, WANG Ping, HU Guo-zhen, WANG Quan
(Chongqing Key Lab of NC & IC, Chongqing University of Posts and Telecommunications, Chongqing 400065)

【Abstract】 Security is critical to a wide range of current and future wireless data applications and services. This paper introduces the security strategy and the security implementation for ZigBee access to EPA network. Test shows that the implementation of the security strategy improves the reliability of the EPA network. These security device, which can be configured, can run steadily and meet the need of the industry control system.

【Key words】 wireless; EPA bus; industry control; ZigBee; security

1 概述

在国家“863”计划的滚动支持下，重庆邮电大学作为核心单位参与制定了国家标准——《用于工业测量与控制系统的EPA(Ethernet for Plant Automation)系统结构和通信标准》，简称“EPA标准”。在此基础上形成的65C/357/NP以95.8%的得票率被国际电工委员会IEC发布为IEC/PAS 62409，并作为第十四类型列入实时以太网国际标准IEC 61748-2，作为第十四类型将列入现场总线国际标准IEC 61158 (修订版)。

在工业现场，一些工业环境禁止、限制使用电缆或很难使用电缆，还有一些工业环境要求完全把电缆屏蔽起来以高度防止来自大多数工业设施中的机器或其他无线电控制设备的干扰，更有一些高速旋转的设备根本无法通过电缆来传输数据信息，而无线通信技术却很容易解决这些问题[1]。

ZigBee是一种低速率(2 Kb/s~200 Kb/s) WPAN IEEE标准，传输速率只有100 Kb/s；同时，它又具有功耗低、架构简单、成本低的特点，满足多种无线需求，尤其在工控(监视器、传感器和自动控制设备)等领域更是显示出其独有的优势。鉴于此，把ZigBee作为EPA网络中的一种传输技术是最近研究的热点。

由于无线网络通过无线介质进行传输，它比有线网络更容易受到攻击[2]，因此EPA网络中ZigBee接入点和ZigBee现场设备的安全性问题也显得更为突出和重要。在《EPA安全规范》中规定通过EPA网桥将现场设备层网络划分成多个网段，由EPA网桥保证网段内部的安全，对现场设备采用基于角色的访问控制措施、安全功能块和IP层报文过滤3种安全保护措施进行安全保护，但对于无线网段的无线接入点设备和现场设备的通信安全性没有做出明确的规定。

2 ZigBee接入EPA网络的组网特点

在一个EPA控制网络系统中规定了2种网段[3]、即L1网段和L2网段，其中，L1网段由EPA有线网络由远程监控中心、应用计算机、组态服务器和数据库等构成；L2网段指现场设备层网段，由用于工业生产现场的各种设备(如变送器、执行机构、分析仪器等)组成。L1网段可采用工业以太网、ZigBee、蓝牙等通信网络技术。基于EPA的工业控制网络系统结构如图1所示。

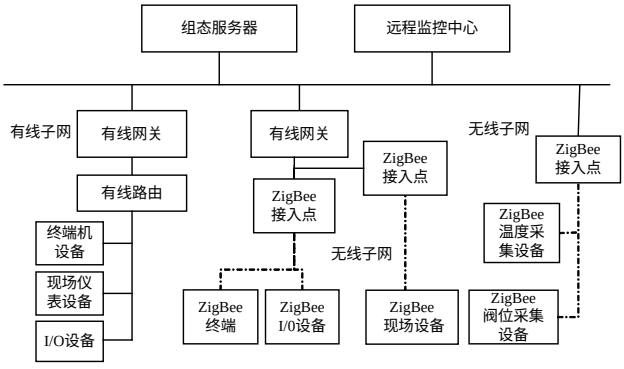

图1 基于EPA的工业控制网络系统结构

ZigBee网络由ZigBee现场设备和EPA的ZigBee接入点

基金项目：国家“863”计划基金资助项目(2006AA040302)；重庆市重点科技攻关计划基金资助项目(CSTC, 2007AB2027)
作者简介：魏 旻(1982－)，男，助教，主研方向：工业以太网及网络控制技术，无线工业通信技术；王 平，教授、博士、博士生导师；胡国珍，硕士研究生；王 泉，讲师
收稿日期：2007-10-20 **E-mail：**thinker9@163.com

构成。EPA 有线网络与 ZigBee 网络之间通过 EPA 的 ZigBee 接入点连接，ZigBee 接入点负责 ZigBee 网络和有线网络的连接和数据转发。

ZigBee 接入点是 EPA 控制网络中的重要设备之一，是负责终端设备的管理及协调无线与有线网络之间通信的关键部件。ZigBee 接入点具有将 ZigBee 设备接入 EPA 有线网络的功能，是连接 EPA 有线网络和 ZigBee 网络的桥接设备。ZigBee接入点作为无线网络接入有线网络之间的关键部件更易受到攻击，同时 ZigBee 终端设备的开放性和移动性，使其比有线网络更容易受到攻击，采集现场数据在传输过程中很可能被非法截获或更改。

3 ZigBee 接入 EPA 网络的安全方法及其实现

EPA的无线控制子网作为开放系统，容易受到各种各样的风险和安全威胁，包括窃听、欺骗和非授权访问、非授权的网络连接、未授权的信息破坏和篡改、拒绝DoS服务、洪泛攻击和耗能攻击等[4]。尽管ZigBee提供了三级安全模式，但其使用的安全体系在信息内容加密性、完整性和用户认证方面仍然存在缺陷。所以在接入EPA控制网络后，为了保证EPA网络不被非法入侵，报文不被非法篡改和破坏，需要采用必要的安全措施对网络保护。ZigBee接入EPA网络建立安全通信流程如图 2 所示。

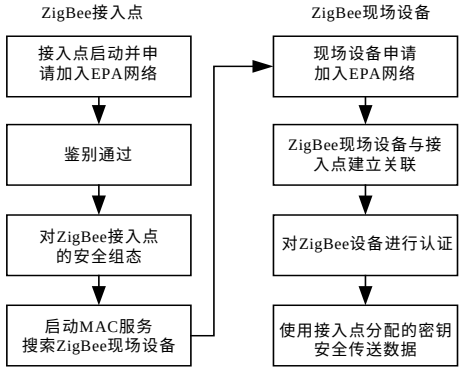

图 2　ZigBee 接入 EPA 网络建立安全通信流程

ZigBee 现场设备通过 ZigBee 接入点接入 EPA 工业以太网并建立安全连接的过程如下：

(1)启动并加入 EPA 网络：ZigBee 接入点复位启动后，发送设备声明和鉴别报文到 EPA 服务器中请求认证和组态。如图 3 所示。

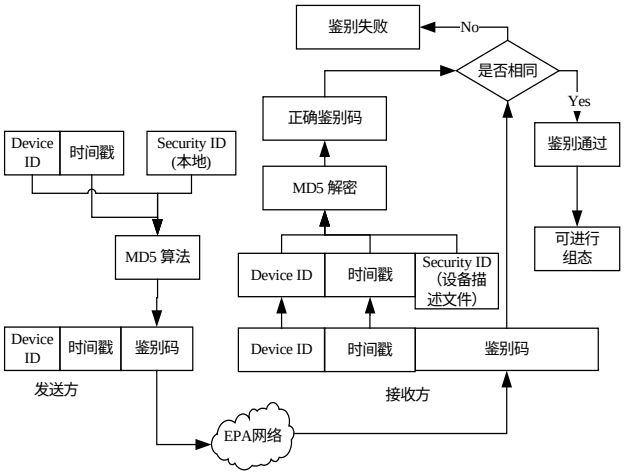

图 3　ZigBee 接入点和设备的认证鉴别流程

认证算法如下：利用 ZigBee 接入点设备的设备标识符(Device ID)、设备的时间戳和设备的安全 ID 生成鉴别报文，接入点上线后，通过调用鉴别服务，将鉴别报文发送到发送给组态服务器。组态服务器收到设备鉴别服务时，根据设备鉴别报文内的 Device ID 字段查找设备描述文件，从其中读取初始密钥。通过对接收到的用户报文中的设备标识和时间戳使用相同的 MD5 算法进行加密获得“ 正确鉴别码 ”，将“ 正确鉴别码 ” 与接收到的鉴别码进行比较，若相同则该设备通过鉴别，可进行后续操作；否则丢弃该数据包，并认为设备为不可信。组态软件对 ZigBee 接入点进行安全组态并进行安全消息管理。

ZigBee 接入点鉴别函数的相关实现如下：

```
void NS_Authen_Output(void)                    // 认证鉴别函数
{ …                                            // 变量定义，省略
  memcpy(outbuf, LocalDeviceDesp.DeviceID, 32); // 填充设备 ID
  GetDateTime((sTime *)(outbuf + 32));         // 获得时间戳函数
  GetSecID  (outbuf  + 40);                    // 获得安全 ID 函数
  MDString  (outbuf , kcode, 72);              // 计算HASH值[5]
  memcpy    (outbuf + 40, kcode, 16);          // 填充鉴别码
…
  // 填充其他负载，省略
  epa_send  (outbuf,  NSID_AUTHEN,  broadcast_ipaddr,
LEN_AUTHEN);  }    // 发送该认证鉴别服务
```

ZigBee 接入点和设备的认证鉴别流程如图 3 所示。

(2)对 ZigBee 接入点的安全组态：对 EPA 的 ZigBee 接入点的合法性检查之后，组态软件通过组态后 ZigBee 接入点正式加入 EPA 网络。组态软件通过变量读写服务读写 EPA 管理信息库的参数，对 ZigBee 接入点进行管理。组态软件通过变量读服务读取 EPA 管理信息库和 EPA 安全管理信息库中的可读参数。安全管理信息库包括管理信息首部对象、安全机制管理对象、访问控制对象、密码表管理对象和设备鉴别对象。

组态软件可以对密钥长度，密钥表偏移进行组态，为设备更新密钥，该操作包括随机生成 64 个字节串作为设备密码表并指定密钥的长度和在表内的偏移量。组态后的组态软件可显示的 ZigBee 接入点的密钥管理信息。完成所有参数的设置后，组态软件将配置新的管理信息库对象，并且将所有的对象写回设备管理信息库使其生效，对安全设备的本次组态也随之结束。

系统利用随机数生成算法产生密钥表，当 ZigBee 接入点和现场设备成功登入网络后，它们会根据用户设置的密钥长度和偏移量从密钥表中得到密钥。如要改变密钥表，则系统的所有设备必须同时变更密钥表，以保证整个系统的密钥表相同。

(3)搜索现场设备：ZigBee 接入点成功组态后，启动一个 MAC 服务搜索 ZigBee 现场设备，ZigBee 现场设备采用主动扫描或被动扫描的方式发现并选择提供 MAC 服务的合适的 ZigBee 接入点，并与所选 ZigBee 接入点进行同步。ZigBee 现场设备请求与所选的 ZigBee 接入点建立关联。

(4)ZigBee 现场设备的认证：在 ZigBee 现场设备搜索到可加入的 ZigBee 接入点并加入其中后，在建立连接之前需要一个认证过程。ZigBee 现场设备从接入点接入时，已通过鉴别的接入点中向 ZigBee 设备发放密钥。现场设备使用得到的密钥，将其设备 ID 加密以后，发送给组态服务器认证，认证通过后，才可以从该节点接收现场采集的数据。设备掉线或者是重起，都应该重新发起鉴别服务，进行重鉴别。

(5)安全的数据传送：ZigBee 接入点和 ZigBee 现场设备

的采用加密机制对数据进行加密传输。现场数据的传送必须满足 ZigBee 无线通信的要求，以一定的报文格式传送，因此在传送之前必须将数据封装成帧。图 4 描述了普通数据帧和安全数据帧的格式。0x44 代表数据格式，Node 为通信节点号，这里默认通信节点具有相同的网络号；Sec-type 是安全使能标识，Length 为 ZigBee 数据长度；Var-parameter 为阀门参数，包括读/写命令，地址等信息，占 3 个字节；Var-data 为阀门数据(阀位值或上下限)，为占 4 个字节的浮点数；CRC 为奇偶校验。安全帧增加了消息完整代码(MIC)，对加密后的数据进行完整性校验。对 ZigBee 接入 EPA 网络传输的报文加密，能够提高数据的保密性，保证 EPA 内部通信信息数据的安全。根据现场需要，发送方利用异或加密算法对用户数据进行加密运算。普通数据帧和安全数据帧如图 4 所示。

普通帧格式

字节：1	1	1	1	3	4	1
0x44	Node	Length	Sec-type	Var-parameter	Var-data	CRC

安全帧格式

字节：1	1	1	1	3	4	1	1
0x44	Node	Length	Sec-type	Var-parameter	Var-data	MIC	CRC

加密保护

图 4　普通数据帧和安全数据帧

对 ZigBee 现场设备传送数据进行安全处理的相关实现如下：

```
void bt_send(uint8 node, float var,uint8 key[16])
  //数据发送函数
{…
  //变量定义，省略
  security_checksum =security_check(bt_send_data,0x07,key[0]);
  //获得安全效验码
  bt_send_data[11]=security_checksum;
  //填充安全效验码
  encryption(key[16], bt_send_data) ;              //数据加密函数
for(i=0; i<11; i++){check_sum^=bt_send_data[i]; }
//ZIGBEE 报文效验码
bt_send_data [12] = check_sum;   }
```

(6)实现基于角色的访问控制机制：ZigBee 接入点采用基于角色的访问控制，防止非法设备对其的非法访问。访问控制机制基于访问控制列表实现，每台 ZigBee 接入点设备中都保存着组态时设置的访问控制列表。访问控制列表项包含了发起访问的远程设备 IP 地址、功能块 ID、对象 ID 以及本地设备功能块 ID、对象 ID、通信角色。通过以上 6 个参数，可以唯一地确定一对 EPA 通信关系。被访问 EPA 设备通过查询本地访问控制列表，判断是否存在对该设备的访问控制授权。

4　安全功能测试

程序的测试贯穿了软件实现的全过程。ZigBee 接入 EPA 网络安全功能测试目的在于证明该措施在设备与组态软件之间的实现是一致的，并且使用该措施可以防止非法设备接入 EPA 网络。在组态软件上为 ZigBee 安全设备配置正确的标识的设备描述文件，ZigBee 接入点设备上电发送设备鉴别报文，无论设备是否合法 EPA 组态软件都会给出 EPA 设备鉴别信息。认证鉴别措施安全功能测试结果如图 5 所示。测试结果显示，应用设备鉴别措施使组态软件可以对接入网络的合法与非法 ZigBee 设备进行区分，防止非法设备获取组态信息，从而阻止了非法设备接入 EPA 网络。

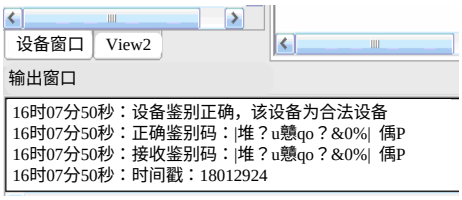

图 5　组态软件显示设备鉴别措施安全功能测试结果

使用网络监控计算机模拟未经授权的应用进程发送变量写报文测试访问控制。设置非法访问设备的目的应用标识、对象标识和子标识等属性，由于 EPA 设备组态未制定安全设备与该应用进程间的通信关系，因此该访问会被 EPA 安全设备拒绝，网络监控计算机接收到变量写负响应报文，判断该访问权限不存在。访问控制措施成功的防止了非法访问。

测试数据加密和数据校验措施的目的是确定数据加密和校验是否完成，加密和校验过程是否完全可逆的，并且不会对原数据造成影响。在报文接收端，经过报文解密、校验后，正确识别该报文。安全功能测试结果证明，报文校验与报文加密措施是完全可逆的，解密后报文信息不会受到损害。因此，报文校验和加密措施有利于 ZigBee 设备接入 EPA 系统安全性的提高。

5　结束语

将 ZigBee 接入 EPA 网络是计算机网络技术、通信技术和自动化技术相结合的新兴产物，具有广阔的应用前景。由于工业无线网络的安全性统一标准和 EPA 安全标准尚未确定，因此应根据 ZigBee 的不同使用环境和 ZigBee 的实际特点，有针对性地采取相应的策略加强其安全性。经测试，ZigBee 接入 EPA 网络的安全策略能够利用标准及开放的架构去满足现场级的安全要求，提供安全可靠的设备鉴别，实行有效的密钥管理机制，该策略考虑了 ZigBee 接入 EPA 网络中无线部分的安全需求，对于 EPA 网络本身，则还应采取相应的等同于有线网的安全措施来加强网络的安全性。

参考文献

[1] Manley M E, McEntee C A, Molet A M, et al. Wireless Security Policy Development for Sensitive Organizations[C]//Proc. of Systems, Man and Cybernetics(SMC) Information Assurance Workshop. New York, USA: IEEE Press, 2005.

[2] Park J C, Jun A H. A Lightweight IPSec Adaptation for Small Devices in IP-based Mobile Networks[C]//Proc. of ICACT'06. Phoenix Park, Korea: [s. n.], 2006.

[3] 曾　文, 王　宏, 徐皑冬. 基于 EPA 标准的无线通信技术的应用研究[J]. 微计算机信息, 2006, (2): 47-49.

[4] Wang Ping, Wang Heng, Wang Quan, et al. ISA-SP100 Proposal White Paper[Z]. Chongqing University of Posts and Telecommunications, 2006-10.

[5] Schneier B. 应用密码学[M]. 吴世忠, 译. 北京: 机械工业出版社, 2000-01.