WIA-PA 网络密钥管理体系①

刘建明[1], 徐莉莉[2], 王金才[1], 张运杰[3]

[1](潍坊医学院 计算机中心, 潍坊 261053)
[2](潍坊职业学院 汽车工程系, 潍坊 261041)
[3](北京科技大学 计算机与通信工程学院, 北京 100083)

摘 要: WIA-PA 是基于 IEEE 802.15.4 标准的用于工业过程测量、监视与控制的无线网络系统. 作为一种新型的无线网络系统, 其安全问题尤为重要, 为保证 WIA-PA 网络的安全性, 设计了 WIA-PA 网络的密钥管理体系, 建立了集中式密钥管理模式, 保证了 WIA-PA 网络安全通信服务, 通过安全密钥管理测试, 验证了设计的密钥管理体系具备良好的安全性.

关键词: WIA-PA; 密钥; 密钥管理; 安全认证; 网络安全

Key Management System for WIA-PA Network

LIU Jian-Ming[1], XU Li-Li[2], WANG Jin-Cai[1], ZHANG Yun-Jie[3]

[1](Computer Department, Weifang Medical University, Weifang 261053, China)
[2](Automotive Engineering Department, Weifang Vocational College, Weifang 261041, China)
[3](Computer and Communication Engineering Department, University of Science and Technology Beijing, Beijing 100083, China)

Abstract: WIA-PA is a wireless network system for industrial measurement, monitoring and control based on IEEE 802.15.4. As a new kind of wireless network system, its security is extremely important. In order to ensure the security of WIA-PA network, we have designed WIA-PA network key management system, established a centralized key management mode, thus ensure WIA-PA network security communication services. Through the test of security key management, the safety of the key management system is verified.

Key words: WIA-PA; key; key management; security authorization; network security

WIA－PA 工业无线技术是一种新型的、我国拥有自主的知识产权的无线网络通讯技术, 它基于 IEEE 802.15.4 标准, 主要用于工业过程测量、监视与控制, 具有很强的抗干扰能力、超低能耗和实时通信等技术特征[1].

密钥管理是实现 WIA-PA 网络安全管理的关键, 为保证 WIA-PA 网络的安全性, 本文详细介绍了 WIA-PA 网络的密钥管理体系的设计, 建立了集中式密钥管理模式, 保证了 WIA-PA 网络安全通信服务, 并通过安全密钥管理测试, 验证了设计的密钥管理体系具备良好的安全性, 能够保证整个无线网络通信的可靠性.

1 WIA-PA网络拓扑结构

WIA-PA 网络采用两层网络拓扑结构, 第一层是 mesh 结构: 包括网关设备及路由设备; 第二层是星型结构: 包括路由设备及冗余路由设备或现场设备[1]. 如图 1 所示.

2 WIA-PA密钥管理体系设计与实现

我们采用了对称密钥来对WIA-PA的密钥进行管理.

2.1 密钥的管理架构

工业无线网络 WIA-PA 要得到全面的应用, 必须要解决安全风险问题, 建立一套安全的密钥管理机制是非常必要的. 我们采用对称密钥的方式, 在设备之

① 收稿时间:2012-10-15;收到修改稿时间:2012-11-22

间建立可共享的加密密钥，保障了系统的正常运行. 工业无线网络管理密钥的方式分为集中式和分布式两种[2]. 安全管理者将负责密钥的管理、网络安全策略的配置和设备的认证[3]. 本文采用了集中式密钥管理的方式，其安全管理架构如图 2 所示.

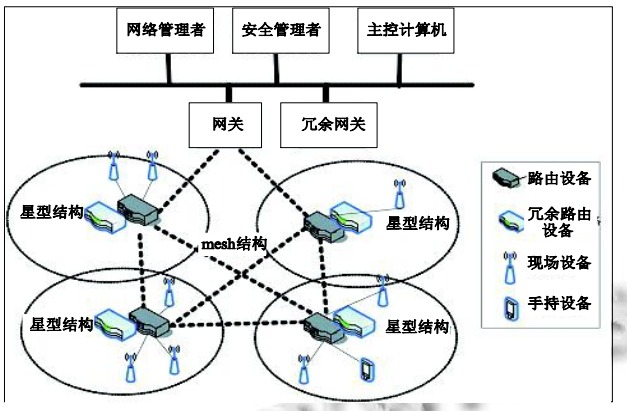

图 1　WIA－PA 网络拓扑结构

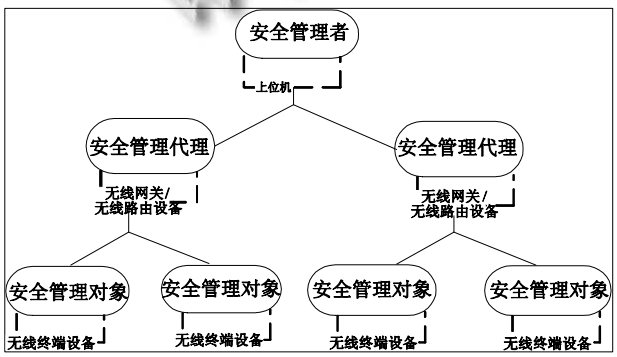

图 2　WIA-PA 网络集中式安全管理架构

安全管理者实现了密钥的产生、分配、更新、撤销等安全服务[4]. 我们采用的 WIA-PA 的对称密钥包括:

1) 密钥的配置(KP): 由网络安全管理者负责分配密钥，生成新的加入密钥.

2) 加入密钥(KJ): 加入密钥主要用来鉴别设备的身份，通常在设备加入网络时使用.

3) 密钥加密密钥(KEK): 在设备和安全管理者之间根据密钥协商协议产生的加密密钥，设备加入网络以后，负责加密保护传送密钥时的新密钥.

4) 数据加密密钥(KED): 数据加密密钥由网络安全管理者统一分配，它负责校验数据传输中各层数据帧的完整性和保密性.

5) 对称主密钥(SMK): 它是最高层次密钥，可以派生出设备的其它加密密钥. 在特殊情况下它也可以作为密钥加密密钥使用[5].

2.2 密钥的分发

由安全管理者统一分发 WIA-PA 网络中的所有密钥. 在安装 WIA-PA 网络无线设备之前，可以先把初始的密钥装载到现场设备，然后再进行配置也可以把配置完成的密钥直接装载到新设备中，然后通过一些移动设备进行分发. 安全管理者通过秘密密钥产生(SKG)[6]协议产生设备共享的对称主密钥，在此基础上建立通信密钥. SKG 协议实现流程如图 3 所示.

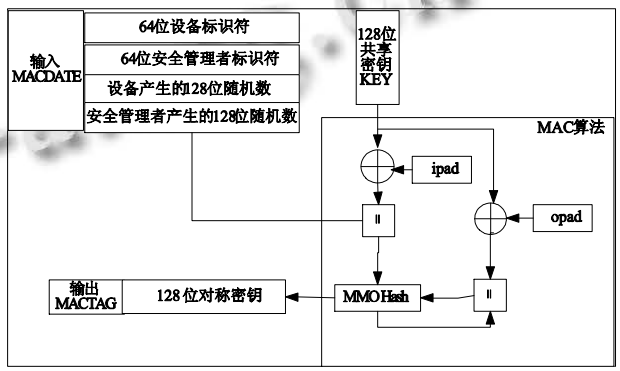

图 3　SKG 协议实现流程

第一步: 输入密钥产生的信息 MACDate, MACDate=安全管理者产生的 128 位随机数 ||设备产生的 128 位随机数 ‖64 位安全管理者标识符 ‖4 位设备标识，其中“||”为连接符.

第二步: 采用 HMAC 机制，利用 128 位共享的密钥和 MACData 可以计算出: MACTag=MACKey (MACData).

第三步: 把安全管理者和设备之间所需的共享秘密密钥设定为 MACTag.

2.3 密钥的更新

密钥更新前，先要根据安全强度的要求对安全密钥的策略进行升级，然后再由主密钥派生出新的密钥值，再利用设备的密钥加密密钥(KEK)进行加密，最后把它分发给网络中相应的设备. 设备成功接收到新的密钥后，利用自己的密钥加密密钥进行解密，完成密钥的更新[2]. 密钥的更新由安全管理者主动发起. 密钥更新的过程见图 4.

第一步: 安全管理者向网关设备发出密钥安全更新请求.

第二步: 网关设备调用网络属性配置请求原语，发送更新请求.

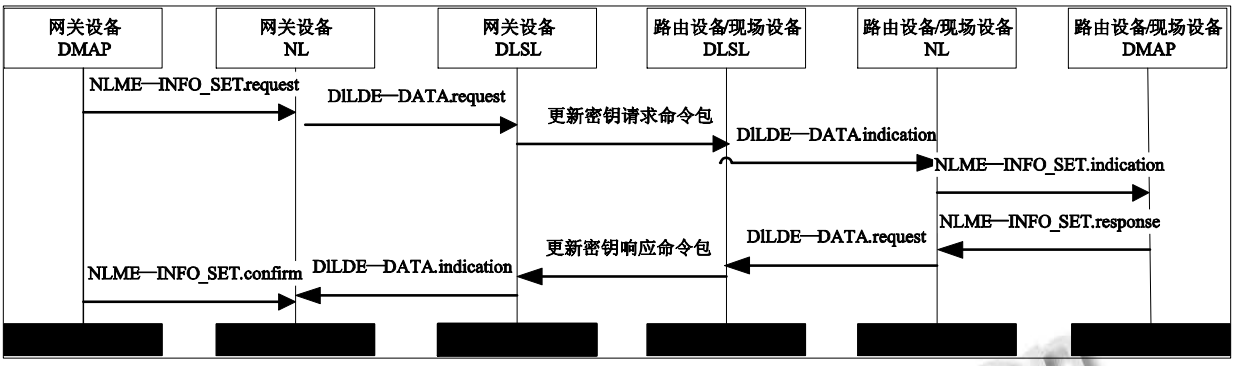

图 4 密钥更新时序图

第三步：收到更新请求的目的设备调用网络属性配置指示原语，把相应的信息在安全管理信息库中进行更新，再将响应命令包回复给网关.

第四步：网关将构造网络属性配置证实原语发送给安全管理者.

更新密钥信息请求命令包格式如表 1.

表 1 更新密钥信息请求命令包格式

13/14 字节	1 字节	1 字节	1 字节	2 字节	变长
网络层包头	命令标示符 默认值：0X1E	属性标示符 默认值：0X6C	属性成员标识符. 如果该值为 255，则表示读取全部的属性成员	属性标识符 索引	属性值

密钥更新部分源代码如下:

```
struct Attribute_identifier_type  // 属性标识符类型
{……
struct Key_identifier; //密钥标识符
struct KEY_TYPE; //密钥类型
struct KEY_LENGTH; //密钥长度
struct KEY_ACTIVETIME //密钥激活时间
struct KEY_REWOKETIME; //密钥撤销时间
struct KEY_DATA; //密钥值
struct KEY_tfm compress; //密钥攻击次数
……}
```

2.4 密钥的撤销

设备正常的更新密钥之后，所有过期的密钥将会被安全管理者撤销. 但是如果出现密钥已经被泄露或者密钥的安全受到威胁等情况，安全管理者就会及时将该密钥撤销. 当 WIA-PA 网络受威胁情况，安全管理者也可以强制撤销设备中的密钥，但在密钥撤销之前，安全管理者首先要完成对该设备密钥的更新.

2.5 密钥的生存周期

安全管理者需要对密钥进行定期地更新. 从建立到撤销每个密钥可能会处于不同的阶段，对密钥进行维护和更新时，安全管理者必须要根据设备的具体应用需求. 如果长期使用一把密钥，会存在很大的安全隐患，所以必须要摆脱对原密钥的依赖性. 对于共享密钥，一定要注意存储的安全性、真实性和秘密性. 密钥生存周期序列图如图 5 所示.

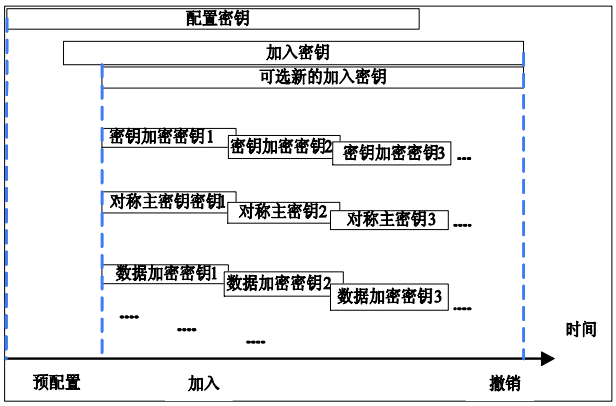

图 5 密钥生存周期序列图

首先要保证配置的密钥具有唯一性，然后再由安全管理者将密钥分配给所有的设备.

3　安全密钥管理测试

为了保持密钥的安全性、秘密性和真实性 ，我们建立了密钥管理体系，为了证明新建立的密钥管理体系的安全性，我们进行了一系列的测试，测试的过程包括了密钥的获取、分发、更新，如图 6、图 7 所示:

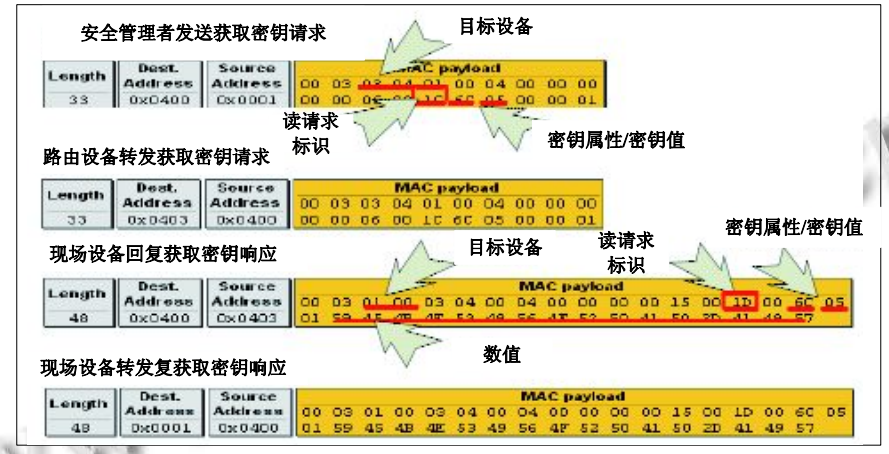

图 6　安全管理者获取密钥抓包截图

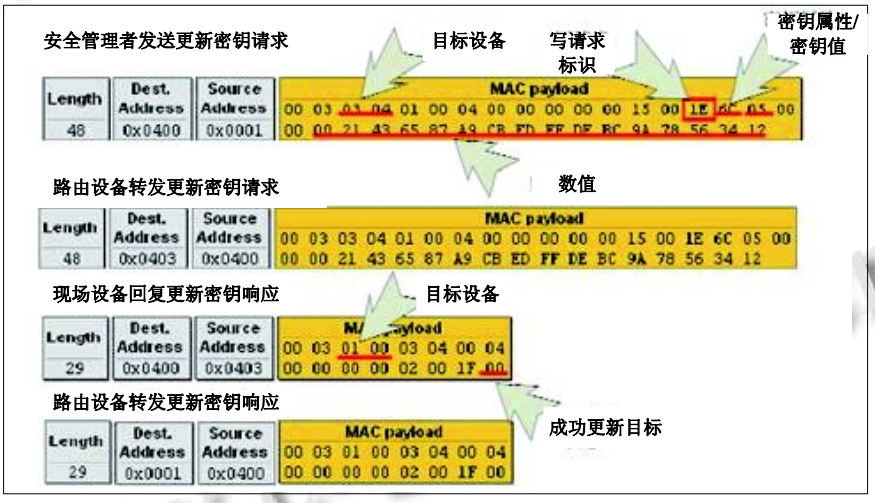

图 7　安全管理者更新密钥抓包截图

通过图 6、图 7 的测试结果显示，安全管理者向网关设备(address0x0400)发出密钥安全更新请求,网关设备调用网络属性配置请求原语，发送更新请求.

目的设备(address0x0403)收到更新请求，更新安全管理信息库中相应的信息，并将响应命令包回复给网关. 在密钥更新中“0”表示成功，“1”表示操作不成功，执行结果为“00”，表示成功更新状态，安全管理者可以根据现场环境来更新密钥，真正做到了密钥管理的安全性、真实性和秘密性.

由此可见，通过建立完善的 WIA-PA 网络密钥管理机制，可以为新设备入网认证服务提供了安全保障.

4　结语

为保证 WIA-PA 网络的安全性，本文设计了 WIA-PA 网络的密钥管理体系，保证了 WIA-PA 网络安全通信服务，安全管理者使用 MAC 认证协议[7]、SKG 协议[8]等对称密钥机制，实现了网络密钥的分发、更新、和撤销[9]等功能，设计了 WIA-PA 网络的密钥管理体系，建立了集中式密钥管理模式，通过安全管理者的集中式密钥管理，保证了 WIA-PA 网络安全通信

(下转第 175 页)

3.4 功能验证

利用本装置对部分发动机参数进行了检测验证，并通过液晶屏幕显示相关参数，如图 7 所示为气门位置波形，达到了预期效果.

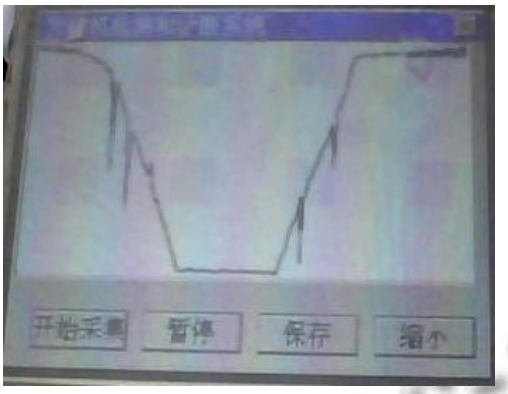

图 7 气门位置波形

4 总结

本发动机检测装置的设计采用 SEP4020 作为微处理器，移入了 μC/OS-II 嵌入式操作系统、μC/GUI 图形界面和 FAT32 文件系统. 以 TLC2543 为 AD 转换芯片，实现了多通道高效率的实时检测，通用性强，并且预留了三个同道可供用户拓展新功能. 以 SD 为存储设备，实现了方便快捷的存储数据的方式，达到了便携式移动存储的目的，提高了设备的灵活性. PC 机可直接对 SD 卡进行操作，又 SD 进行存储为后续对数据的分析处理备份做好了准备.

本文作者创新点：同以往其它的数据采集系统相比，本系统采用 TLC2543 多通道 ADC 芯片，可同时进行多路采集实现多功能. 在软件设计中植入了 μC/OS-II 嵌入式操作系统，使多任务运行更加稳定可靠；μC/GUI 图形界面支持系统为显示终端提供了绚丽多彩的图形界面，达到良好的人机交互效果；同时本系统采用 SD 卡作为移动存储器，以对现场的数据实时采集和高速保存，可轻松实现与计算机数据交换，达到现场采集数据，室内分析数据的目的.

参考文献

1 刘胜永,黄庆华. 嵌入式实时信号采集与处理系统实现方案. 微计算机信息,2008(11-2):61–63.
2 Labrosse JJ.邵贝贝译. μC/OS-II－源码公开的实时嵌入式操作系统.北京:中国电力出社,2001.
3 μC/GUI 用户手册.Micrium 公司,2003.90–114.
4 杨明极,陈方县,吴学君.嵌入式系统中 SD 卡的 FAT32 文件系统的设计.电声技术,2010(4-17):36–39.

(上接第 28 页)

服务，最后本文对安全密钥管理进行了测试，测试表明，我们所设计的密钥管理系统安全性能良好，可以为新设备入网认证服务提供了安全保障. 但是，随着计算机网络通讯技术的不断发展，会出现各种不同的网络安全风险，无线网络的安全密钥管理体系需不断完善.

参考文献

1 王华,刘枫,杨颂华.工业无线网络 WIA-PA 网络研究与设计. 自动化与仪表,2009,(7):21–23.
2 张萱.WIA-PA 网络安全通信协议栈研究与实现.重庆:重庆邮电大学,2010.
3 李力刚,王忠锋,王乐辉,黄剑龙.WIA 建筑能耗测量与优化运行系统.仪器仪表标准化与计量,2009,(3):78–81.
4 曾鹏,肖金超,张琼.WIA 网络与 MODBUS 网络互联设计与实现.仪器仪表标准化与计量,2009,(4):102–104.
5 刘扬,曾鹏,尚志军,张华良.基于工业无线网络 WIA 技术的储油罐监测系统.仪器仪表标准化与计量,2009(5):23–25.
6 Zhang XD, Hong J, Zhang L, et al. Li CP-TDMA: coloring and probability based TDMA scheduling forwireless ad hocnetworks. IEICE Transactions v91-B(1): Oxford University Press, Oxford, 2008: 322–326.
7 Wang W, Wang Y, Li XY, et al. Efficient Interference-aware TDMA link scheduling for static wireless networks. Proc. ACM MobiCom. 2006: 262–273.
8 Yue FY, Liu F. Research for cluster channel assignment in WIA-PA. Proc. of the 5th IEEE WiCOM (WiCOM'09). China, 2009: 1–4.
9 杨淼,梁炜,徐伟杰.基于 WIA-PA 的工业无线网络网关设备. 计算机工程,2010(23):12–14.