基于 Hash 变换的智能配电系统通信安全性研究*

黄世泽[1]，王梦莹[2]，徐秋勇[3]，郭其一[3]，屠旭慰[4]
(1. 同济大学 道路与交通工程教育部重点实验室，上海　201804；
2. 同济大学 铁道与城市轨道交通研究院，上海　201804；
3. 同济大学 电子与信息工程学院，上海　201804；
4. 浙江中凯科技股份有限公司，浙江 温州　325604)

黄世泽(1983—)，男，副研究员，研究方向为信息安全、电磁兼容仿真与测试。

摘　要： 深入研究了智能配电系统的安全需求，对智能配电系统与传统信息系统的区别进行了详细的总结，并全面分析了智能配电系统设备层通信的脆弱性以及存在的安全隐患。在此基础上，从 Modbus 协议安全的角度出发，基于 Hash 函数提出了 Modbus 报文安全性解决方案，设计了 Modbus 安全认证协议。通过修改 KB0 系列控制与保护开关的源代码，在实物通信中证明了该方案的可行性与可靠性。基于安全性关键技术，初步建立了智能配电系统安全防护体系，对研究智能配电系统安全具有指导意义。

关键词： 智能配电系统；Modbus-RTU；Hash 函数；Modbus 安全认证协议；控制与保护开关

中图分类号： TM 76　**文献标志码：** A　**文章编号：** 2095-8188(2018)21-0030-06

DOI： 10.16628/j.cnki.2095-8188.2018.21.007

Research of the Key Security Technologies of Intelligent Power Distribution System Based on Hash Fuction

HUANG Shize[1]，*WANG Mengying*[2]，*XU Qiuyong*[3]，*GUO Qiyi*[3]，*TU Xuwei*[4]
(1. Key Laboratory for Road and Transportation of the Ministry of Education, Tongji University, Shanghai 201804, China; 2. Institute of Rail Transit, Tongji University, Shanghai 201804, China;
3. College of Electronics & Information Engineering, Tongji University, Shanghai 201804, China;
4. Zhejiang Zhongkai Science Company Limited, Wenzhou 325604, China)

Abstract: This article studied the safety needs of the intelligent power distribution system, summarized the difference between the intelligent power distribution system and the traditional information system in detail, and thoroughly analyzed the vulnerability as well as the existing security risk of the mechanical floor of the intelligent power distribution system. Then starting from the Modbus protocol security, Modbus message security solutions based on Hash function were proposed and Modbus security authentication protocol was designed. Meanwhile, the foresaid plan was verified on account of the intelligent power distribution system which is constituted of control and protective switching devices. By modifying the source code of control and protective switching devices (KB0), the feasibility and reliability of the schemes were proved in the physical communication. Based on the security-critical technology, the safeguard system of the intelligent power distribution system has been preliminary established, which is of guiding significance to the study on the safety of the system.

Key words: intelligent power distribution system; Modbus-RTU; Hash function; Modbus protocol security authentication protocol; control and protective switching devices (CPS)

王梦莹(1996—)，女，研究方向为智能配电系统。
徐秋勇(1992—)，男，硕士研究生，研究方向为智能配电系统。

* 基金项目：国家自然科学基金(61703308)；中央高校基本科研业务

0 引 言

智能配电系统是按用户需求,遵循配电系统标准规范而二次开发的一套自动化和智能化程度高、可靠性高、性能优越的电能管理系统。在“以信息化带动工业化、以工业化促进信息化,将信息技术广泛应用于工业生产的各个环节,走新型工业化道路”的两化融合背景下,智能配电系统日益广泛地与企业管理信息系统甚至互联网产生数据交换,以往由物理环境的封闭性和专用性所带来的安全性已不复存在,智能配电系统的网络安全问题正面临巨大的挑战。过去10年间发生的许多配电故障或事故都被认为是网络安全所致的[1],因此如何保证智能配电系统的机密性、完整性和可用性已经成为当下热议话题。但目前国内外对智能配电系统安全性的研究还没有展开,更多的是对工业控制系统安全性的研究,且只在起步阶段,没有引起足够多的重视。

智能配电系统虽属于工业控制系统的范畴,但其实现的功能更具体,作用更明确,应用的范围更小,与工业控制系统之间存在着一定的区别,无法完全移植工控系统安全防护方法,因此有必要深入研究满足智能配电系统安全需求的关键技术,从根本上保障智能配电系统的安全运行。

从协议安全的角度出发,工业控制系统用到设备类别多种多样,通信协议包括Modbus、Profibus、以太网等,而智能配电系统所采用设备类型相对固定,通常为可通信控制与保护开关(CPS)以及可通信电表。目前学术界已开始研究的IEC 61850协议功能强大,但实现极为复杂[2];当前电厂智能终端设备普遍应用的仍是Modbus通信协议,但该协议尚存在缺乏认证、缺乏授权、缺乏加密等安全隐患[3]。

为增强协议安全,一般采取两种方式:第一种方法是直接修改协议,增加认证环节或者对协议进行加密,如应用Hash链的概念对Modbus主站进行认证,这样入侵者就无法伪装成主站对从站设备发号施令,从而使从站设备认证了收到指令的合法性[4];第二种方法是增加信息安全层,既可以以硬件的形式实现,也可以以软件的形式实现,如设计与通信系统独立的信息安全层,无需改变底层数据传输模式即可保障信息安全[5]。

本文在现有研究基础上,提出了基于Hash函数的Modbus报文安全性解决方案,以完善Modbus安全认证协议,并通过修改KB0系列CPS的源代码,在实物通信中证明了该方案的可行性与可靠性,为智能配电系统安全性的研究提供有效的解决方案。

1 智能配电系统及Modbus协议介绍

1.1 智能配电系统

智能配电系统是将先进的电子技术应用于电气开关、断路器、接触器等传统配电设备而产生的,因而具备状态检测、参数设定、故障记录与报警、远程控制与保护等功能[6]。

智能配电系统一般采用分层分布式结构,分为现场设备层、网络通信层和系统管理层[7]。系统典型的整体架构示意图如图1所示。

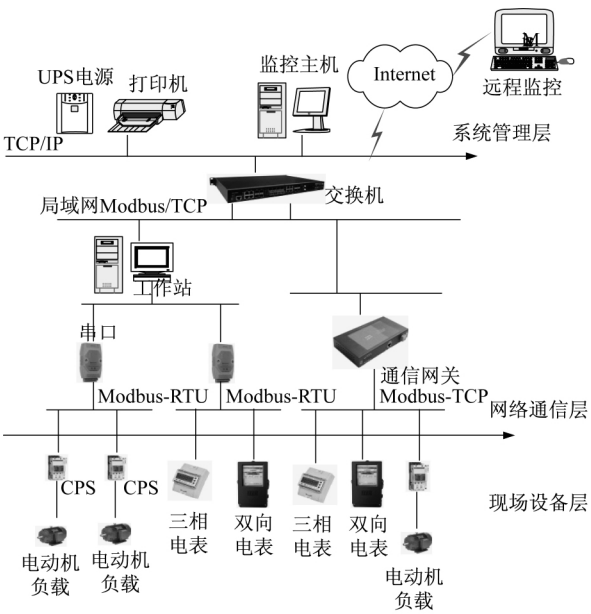

图1 系统典型的整体架构示意图

1.2 智能配电系统与传统信息系统差异性分析

互联网信息安全技术经过多年的发展已经相对成熟,但其更多应用于商业领域,应用环境与智能配电系统有着明显的不同之处,因此互联网信息安全技术不能直接应用于智能配电系统的信息安全防护。为了更好地借鉴互联网信息安全技术,首先应明白两者的不同之处,分析出智能配电系统的特有属性,并结合自身的特点,在互联网信息安全技术的基础之上加以改进,真正地研究出

适合智能配电系统的安全防护措施,以保障系统安全。智能配电系统与传统信息系统的差异化比较如表1所示。

表1　智能配电系统与传统信息系统的差异化比较

要求	传统信息系统	智能配电系统
可用性	允许在短时间内或周期性的间断以及进行维护	必须要求保证24 h/7 d/365 d模式下的可用性
实时性	允许一定的时延	要求实时响应
系统生命周期	生命周期较短,一般在3~5年之间	生命周期较长,一般情况下不会轻易更换,可使用长达20年
信息安全意识及准备	信息安全技术已经相对成熟,前期积累的安全知识已足以应对一些信息安全事故	没有基础,正处于探索期
保密性	要求较高,往往第一时间考虑保密性	设计初期要求较低,基本不考虑保密性
设备类型	较少,系统中用到的设备往往就那几种,主机、网关、防火墙等	较多,各种类型的可通信开关、智能电表、传感器等
风险管理要求	数据的保密性以及完整性最重要,允许短时间的软件更新升级	正常持续运行最重要,不容许有系统死机、停机的情况存在
资源限制	系统资源足,能支持第三方应用	受限于主机的硬件配置,没有足够的计算资源来支撑其他应用
通信协议	具有标准的通信协议,主要用有线网络以及一些本地无线功能	通常采用Modbus协议

由表1可见,传统信息系统是在保密性的基础之上保障信息完整性以及可用性,而智能配电系统设计初期是在可用性的基础之上完善信息完整性以及保密性,两者出发点不同,存在着明显的差别,由此更体现出智能配电系统通信安全性研究的紧迫性和必要性。

1.3　Modbus协议

Modbus协议是在工业控制系统中广泛采用的一种现场总线,国标中规定的Modbus协议模型如图2所示。

由图2可见,Modbus协议作用于应用层。Modbus通信采用主从方式,某一时刻,只能有1个主站和最多247个从站同时连接在总线上。在每次通信过程中,都由主站发起通信,从站只有在收到请求时,才会发送数据,各从站之间不会相互通信。主设备向从设备发送数据请求,从设备收到请求后作出相应的动作。如果该过程中出现问题使得请求无法到达设备或者设备动作无法完成时,则会在主、从站超时到一定程度后放弃该过程,继续下一个动作。

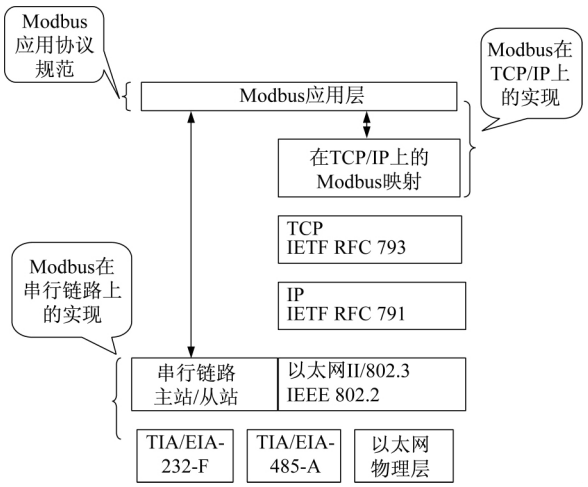

图2　国标中规定的Modbus协议模型

Modbus协议在设计之初,只考虑了功能的实现,并未对协议安全做过多的设计,随着工控系统不断地向智能化、自动化方向发展,协议的安全性漏洞正被无限放大,入侵者不断地利用协议漏洞对系统进行攻击,获取有用信息,严重影响了整个工控系统的安全运行,因此有必要对Modbus协议加以改进,通过提高通信协议的安全性,从根本上增加通信过程的安全性。

1.4　Modbus协议串行传输方式

Modbus有ASCII和RTU两种串行传输方式。当设备使用RTU模式进行通信时,报文中每个8 Byte的数据字节需要组织成11 Byte字符,根据设备本身实际情况,设置校验模式为:奇校验、偶校验或无校验,默认的校验模式是偶校验,如果采用无校验则有两个停止位。RTU报文帧的结构如表2所示。

表2　RTU报文帧的结构　　Byte

从站地址	功能码	数据	CRC
1	1	0~252	2

由发送设备将Modbus报文构造为带有已知起始和结束标记的帧,使报文接收设备可以在报文的开始就接收新帧,且知道报文何时结束。

单个或多个报文帧的传送如图3所示,在RTU模式中,报文帧由至少3.5个字符时间长度的空闲间隔区分,这个时间间隔称为$t_{3.5}$。

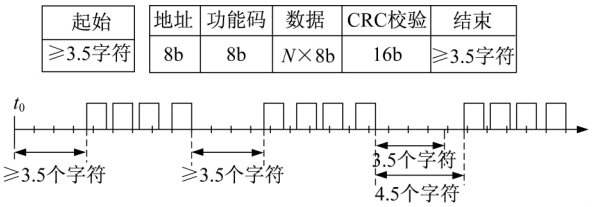

图3　单个或多个报文帧的传送

整个报文帧要以连续的字符流形式发送，Modbus 帧内间隔如图4所示，报文帧中只要出现两个字符之间的间隔大于1.5个字符时间，就被认为不完整，被接收节点丢弃。

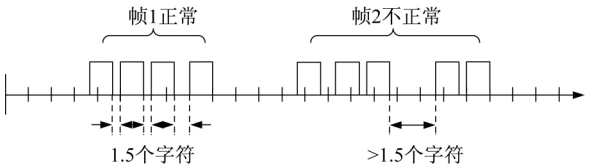

图4　Modbus 帧内间隔

一般情况下设备都默认设置为 RTU 模式，所以本文提出的 Modbus 协议安全方案也主要针对 Modbus-RTU。

2　Modbus 协议安全方案

2.1　Hash 函数与 MD5 算法

Hash 函数俗称散列函数，即把任意长度字符的输入通过一定方式的变换，形成长度确定的输出。该固定长度值被称为散列值，同时 Hash 必须具备以下性质[8]：

(1) Hash 函数对任何长度大小的数据块都有用；

(2) 经 Hash 函数变换后产生的输出长度固定；

(3) Hash 函数具有单向性，即找到满足 $H(x)=h$ 的 x，对任意给定的 h，在计算上都是无法实现的；

(4) Hash 函数具有抗弱碰撞性，即找到满足 $y=x$，且 $H(x)=H(y)$ 的 y，对任何一个 x，在计算上都是无法实现的；

(5) Hash 函数具有抗强碰撞性，即找到任意满足 $H(x)=H(y)$ 的偶对 $x=y$，在计算上都是无法实现的。

目前标准 Hash 函数有两大类：MDx 系列的 MD4、MD5、HAVAL、RIPEMD 等和 SHA 系列的 SHA-1、SHA-256、SHA-512 等。其中 MD5 采用直接构造的办法，以任意长度的字符作为输入，经过变换后，产生一个固定长度为 128 Byte 的散列值作为输出[9-10]，应用十分广泛。

2.2　基于 Hash 函数的 Modbus 报文完整性认证方案

考虑到工控设备的内存以及计算速度有限，本文将应用 MD5 算法对 Modbus 的报文进行完整性认证，通过验证上位机与下位机中 MD5 的值是否一致，来判断报文是否被非法人员修改，从而判断通信会话的合法性，Modbus 报文完整性认证具体方案如图5所示。

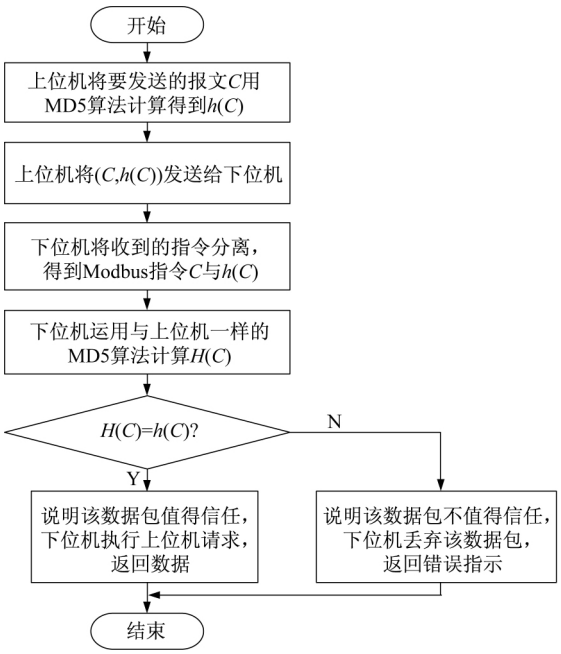

图5　Modbus 报文完整性认证具体方案

(1) 第一步：上位机将要发送的报文 C，经 MD5 计算后变为 $h(C)$，并向下位机发送报文(C，$h(C)$)。

(2) 第二步：下位机接收到上位机发送的报文，通过分析收到报文的首字节判断该报文是否发送给自己，如果不是，则丢弃。

(3) 第三步：下位机分离出 Modbus 报文信息 $C1$ 与 $h(C_1)$，然后再通过与上位机相同的 MD5 算法计算值 $H(C_1)$。

(4) 第四步：比较 $H(C_1)$ 与 $h(C_1)$ 是否相等：若相等，则证明上位机发送的报文指令 C 未被修改，可以信任，此时下位机响应上位机的请求，反

馈数据给上位机;若不相等,说明上位机发送的报文指令 C 已被修改,不能信任该报文,应丢弃。

运用 MD5 算法对 Modbus 报文在上位机和下位机之间传送的完整性进行认证,能从一定程度上防止入侵者修改报文信息。但如果入侵者用 MD5 算法对自己构造的报文进行计算并发送,这时从站将无法判断这种报文的真实性,即无法判断用户身份的真实性。

2.3　基于 Hash 链的 Modbus 安全认证协议

上述方法原理简单,只用了一次 Hash 计算,计算过程简单,占用的内存较小,不影响通信的实时性,同时验证了上位机的身份信息,较好地保证了通信过程的安全性。但该方法每次发送指令时用的都是同一个哈希值,如果非法分子获知 R 以及 $h(R)$ 的值,就能假冒上位机,与下位机进行非法通信,并非法控制下位机。

因此本文提出应用 Hash 链的方法,即采用不同的哈希值,即便入侵者获知其中某一个哈希值,也无法对整个通信过程造成危害。

在 Modbus 应用协议中,主站可能会同时向 m 个不同的从站发送 n 条指令。这里先就主站与一个从站设备通信的情况作具体说明,具体认证过程如下:

(1) 第一步:上位机选择随机数 R,生成哈希链:$h^0(R)$、$h^1(R)$、$h^2(R)\cdots..h^{n-1}(R)$、$h^n(R)$,其中,$h()$ 为满足安全要求的哈希函数,$h^0(R)=R$,$h^i(R)=h(h^{i-1}(R))$,$1\leqslant i\leqslant n$。哈希链中的每一项 $h^i(R)$,$0\leqslant i\leqslant n$,都在上位机中秘密保存。

(2) 第二步:将 $h^n(R)$ 存储于下位机中,此时只有上位机以及下位机知道 $h^n(R)$ 的值。

(3) 第三步:当上位机需要向下位机发送指令 C 时,如果是第一次发送指令,上位机用 $h^n(R)$ 作为对称加密算法的密钥加密$(C,h^{n-1}(R))$,得到$M=E_{h^n(R)}(C,h^{n-1}(R))$,上位机将$(addr,M)$ 发送给下位机,其中 $addr$ 为下位机的地址。

(4) 第四步:下位机通过 $addr$ 判断指令是否发送给自己,并在接收到$(addr,M)$ 后,用事先存储好的 $h^n(R)$ 作为密钥对 M 进行解密,计算$D_{h^n(R)}(M)=D_{h^n(R)}(E_{h^n(R)}(C,h^{n-1}(R)))$,解密出$(C,h^{n-1}(R))$,然后比较下位机中存储的 $h^n(R)$ 与通过下位机计算所得的 $h(h^{n-1}(R))$ 值是否相等:若相等,则确认下位机接收到的消息确实来源于上位机,上位机身份得到确认,此时下位机处理请求指令 C,并将处理结果返回给上位机,随后用 $h^{n-1}(R)$ 更新下位机中存储的 $h^n(R)$;若不相等,则下位机拒绝处理指令请求 C,并向上位机返回“消息非法”信息。

这种方法通过计算 m 条不同的 Hash 链用以分别表示不同的从站设备。这样即便不法分子获知了其中一条 Hash 链,也只能获取相应的一台从站设备的信息,只能对相应的一台从站设备进行控制,无法对其他设备进行控制,大大增加了从站设备的安全性。但这种方法需要分别计算 m 条不同的 Hash 链,对主站的计算速度以及内存有很大的要求,需要高性能的主站作为支撑,不适用于一般的主站设备。

3　Modbus 协议安全试验验证

3.1　试验系统搭建

本文利用现有 CPS 设备搭建了一套测试系统,用以测试上文提出的 Modbus 协议安全解决方案的可行性,并将上文提出的基于 Hash 函数的 Modbus 协议安全解决方案在 Modbus/RTU 串口传输模式下进行实验验证,因此这里使用了一个 RS-485 转 USB 的通信模块。

测试系统架构图如图 6 所示。具体的实物测试环境如图 7 所示。

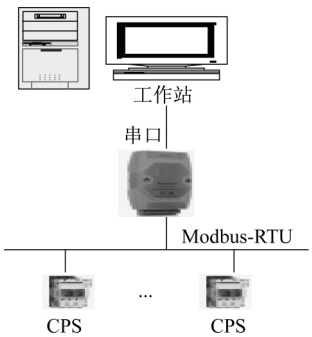

图 6　测试系统架构图

本文利用 KB0T 型 CPS 对所提方案进行试验验证,通过修改 KB0T 底层代码,达到要求的试验目的。

3.2　试验结果与分析

为了更清晰地查看试验结果,可用 AccessPort 软件监视上位机与下位机的通信过程,获取通信报文,并对报文进行分析。

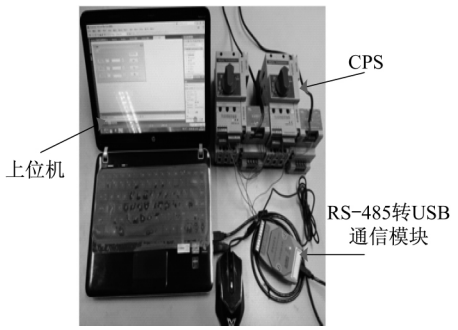

图7　测试系统实物图

正常通信情况下的通信报文如图8所示。

15:20:26.831	0.00238298	WindowsFormsAp	IRP_MJ_WRITE	COM12	SUCCESS	Length: 8, Data: 08 03 00 A1 00 01 D5 71
15:20:26.858	0.01339666	WindowsFormsAp	IOCTL_SERIAL_WAIT_O...	COM12	SUCCESS	
15:20:26.874	0.00002932	WindowsFormsAp	IRP_MJ_READ	COM12	SUCCESS	Length: 7, Data: 08 03 02 00 08 65 83

图8　主从站正常通信报文

如图8所示,上位机发送08 03 00 A1 00 01 D5 71报文给下位机,用以请求读取下位机通信地址,下位机返回报文08 03 02 00 08 65 83,说明下位机通信地址为08,整个请求-应答过程共用时43 ms。

Hash函数用以认证Modbus报文完整性情况下的通信报文如图9所示。

15:22:32.028	0.00237809	WindowsFormsAp	IRP_MJ_WRITE	COM12	SUCCESS	Length: 24, Data: 08 03 00 A1 00 01 D5 71 24 6C 7B 2F 72 AF A2 58 88 85 03 C4 FE EE C1 96
15:22:32.074	0.07375105	WindowsFormsAp	IOCTL_SERIAL_WAIT_O...	COM12	SUCCESS	
15:22:32.089	0.00024289	WindowsFormsAp	IRP_MJ_READ	COM12	SUCCESS	Length: 7, Data: 08 03 02 00 08 65 83

图9　Hash函数用以认证Modbus报文完整性情况下的通信报文

如图9所示,上位机发送08 03 00 A1 00 01 D5 71 24 6C 7B 2F 72 AF A2 58 88 85 03 C4 FE EE C1 96给下位机,其中08 03 00 A1 00 01 D5 71为上位机正常请求的报文,24 6C 7B 2F 72 AF A2 58 88 85 03 C4 FE EE C1 96为08 03 00 A1 00 01 D5 71经Hash运算后的报文;下位机返回报文08 03 02 00 08 65 83,返回报文正确。整个请求-认证-应答过程共用了61 ms,比正常通信过程多了18 ms。由于单个指令的执行占用时间也要以100 ms为数量级计算,所以该试验结果在可接受范围内,说明该方案正确可行。

上面对基于Hash函数的Modbus报文完整性认证方案进行了试验验证,试验证明了方案的正确性以及可行性。由于KB0T系列CPS单片机内存以及计算速度的限制,对本文提出的基于Hash链的Modbus安全认证协议并未作试验验证,所以这也是今后需要进一步研究的地方。

4　结　语

(1)本文对智能配电系统的安全性进行了深入调研,在查阅了大量国内外技术文献后,探究了智能配电系统与传统信息系统安全性的差异,突出强调了智能配电系统特有的安全需求特点,从Modbus协议安全的角度出发,提出了基于Hash函数的Modbus协议安全解决方案,设计了Modbus安全认证协议,并试验验证了所提方案的可行性与可靠性。

(2)由于KB0系列CPS内存及计算速度的问题,而本文提出的基于Hash链的Modbus安全认证协议并未得到试验验证,因此有必要升级硬件,对所提方案进行进一步验证。

【参 考 文 献】

[1] 徐丽娟. 基于攻击图的工业控制网络安全隐患分析[D]. 北京:北京邮电大学,2015.

[2] 王智东. IEC 61850报文安全性关键技术研究[D]. 广州:华东理工大学,2016.

[3] DZUNG D, NAEDELE M, VON HOFF T P, et al. Security for industrial communication systems[J]. Proceedings of the IEEE, 2005, 93(6): 1152-1177.

[4] LIAO G Y, CHEN Y J, LU W C, et al. Toward authenticating the master in the modbusprotocol[J]. IEEE Transactions on Power Delivery, 2008, 23(4): 2628-2629.

[5] 屈婉莹,魏为民,朱苏榕. 工业控制系统通信协议安全研究[C]//2015年全国智能电网用户端能源管理学术年会论文集,2015.

[6] 徐秋勇,郭其一,黄世泽,等. 基于控制与保护开关的智能配电系统研究[J]. 智能建筑电气技术,2015(5): 23-26,32.

[7] 潘藩,郭其一,黄世泽,等. 酒店电能管理系统的设计与实现[J]. 智能建筑电气技术,2016(2): 74-77.

[8] 柯品惠,郑秋鸿. Hash函数研究综述[J]. 福建电脑,2008(12): 1-4,35.

[9] 魏晓玲. MD5加密算法的研究及应用[J]. 信息技术,2010(7): 145-147,151.

[10] 毛明,陈少晖,袁征,等. 关于Hash函数MD5的解析[J]. 计算机科学,2009(11): 106-108,164.

收稿日期: 2018-10-10