配电网 IEC60870-5-104 协议的抗中间人攻击算法

王 勇[1], 王 相[2,1], 刘丽丽[3], 刘金永[1], 武津园[1], 李双飞[4,1]

1. 上海电力大学计算机科学与技术学院, 上海 中国 200090
2. 国网上海市电力公司, 上海 中国 200122
3. 华电电力科学研究院有限公司国家能源分布式能源技术研发(实验)中心, 杭州 中国 310030
4. 上海云剑信息技术有限公司, 上海 中国 200433

摘要 馈线终端单元(Feeder Terminal Unit,FTU)采用 IEC60870-5-104 协议进行远动信息传输。但是由于该 104 协议报文采用明文传输, 缺乏基于数字签名的认证机制, 导致其存在中间人攻击的安全隐患。为了验证 104 协议通信存在的问题, 本文构建了馈线终端 FTU 与主站的通信系统, 验证了中间人攻击截获的 104 协议数据, 为了增强协议安全, 提出了一种基于身份认证的(BM-RAP, Bellovin-Merri based RSA & AES Protocol)改进方法, 在虚拟机实验环境下, 完成一次主从站身份认证时间在 20-80 毫秒之间, 实验结果表明, 该方法增强了抵御中间人攻击的能力。

关键词 馈线终端; 104 协议; 中间人攻击; ARP 欺骗; 身份认证
中图法分类号 TP393 **DOI 号** 10.19363/J.cnki.cn10-1380/tn.2019.11.05

An Algorithm for IEC60870-5-104 Protocol of Distribution against Man-in-the-Middle Attack

WANG Yong[1], WANG Xiang[2,1], LIU Lili[3], LIU Jinyong[1], WU Jinyuan[1], LI Shuangfei[4,1]

1. College of Computer Science and Technology, Shanghai University of Electric, Shanghai 200090, China
2. State Grid Shanghai Municipal Electric Power Company, Shanghai 200122, China
3. National Energy Distributed Energy Technology Research and Development (experimental) Center, Huadian Electric Power Research Institute Co., LTD., Hangzhou 310030, China
4. Shanghai Yunjian Information Technology Co., Ltd., Shanghai 200433, China

Abstract Feeder Terminal Unit (FTU) uses IEC60870-5-104 protocol for telecontrol information transmission. However, since the 104 protocol message is transmitted in plain text, the authentication mechanism based on the digital signature is lacking, which causes a security risk of a man-in-the-middle attack. In order to verify the problem of 104 protocol communication, this paper constructs the communication system between the feeder terminal FTU and the primary station, and verifies the 104 protocol data intercepted by the man-in-the-middle attack. In order to enhance the protocol security, an identity-based authentication (BM-RAP, Bellovin-Merri based RSA & AES Protocol) improved the method of verifying the authentication time of a master-slave station in the virtual machine experiment environment between 20-80 milliseconds. The experimental results show that the method enhances the ability to resist man-in-the-middle attacks.

Key words feeder terminal unit; IEC60870-5-104 protocol; man-in-the-middle attack; ARP spoofing; authentication

1 引言

IEC60870-5-104 协议(以下统称为 104 协议)是 IEC60870-5-101 协议的增强版, 主要应用于网络通信数据传输。104 协议在 101 协议的基础上充分发展, 已经在电力系统中得到了广泛应用。104 协议对传统电网通信系统的串口数据传输方式进行了改变, 具有传输速度更快、便于升级、实时性更好、可靠性更高等优点。电网通信协议最注重的是消息的身份认证、报文的完整性和信息的实时性。所以, 研究

通讯作者: 俞能海, 博士, 教授, Email: ynh@ustc.edu.cn。
本课题得到国家自然科学基金项目(No.61772327); 奇安信大数据协同安全国家工程实验室开放课题(No.QAX-201803); 浙江大学工业控制技术国家重点实验室开放式基金(No.ICT1800380); 智能电网产学研开发中心项目(No.A-0009-17-002-05)资助。
收稿日期: 2018-12-28; 修改日期: 2019-03-31; 定稿日期: 2019-11-04

104 协议的安全性, 设计并实现具有报文加密与身份认证功能的更加安全的通信协议, 增强通信协议的安全性, 具有很重要的意义。

随着近几年网络安全事件的频发, 104 协议面临报文内容遭受窃听篡改的问题, 104 协议没有身份认证和加密功能, 因此很容易被黑客利用中间人攻击和网络钓鱼等方式, 对 104 协议通信过程造成严重的威胁。针对提高 104 协议安全性, 主要面临如下难点: 1)现有的安全性措施难以施加在正在使用中的设备上, 无论是正在运行工业或者是电网, 都无法暂停工作, 加入现有的安全性措施; 2)当前主流的安全性措施是采取通信报文加密的方式, 但是加密势必会导致通信时间延长, 通信报文的实时性降低。

针对上述问题, 当前针对 104 协议安全性的研究主要分为: 通信协议的建模转换[1-5]、协议测试等方法[6-7] 、通信过程加密保护[8-9]。

在 104 协议的建模通信转换领域, 孙俊男等通过深入分析 IEC60870-5-104 的结构模型, 提出并实现了 IEC60870-5-104 的通信模块设计方案, 其硬件平台能够成功实现对 PLC 架构的支持, 其软件平台通过嵌入式实施多任务操作系统实现调度任务[1]。王飒等通过对 IEC60870-5-104 和 IEC61850 的信息模型进行深入研究, 并与 XML 技术相结合, 设计了两种协议的转换网关, 最终通过以太网通信、IEC61850 信息建模、信息映射以及配合文档描述等方式对两种协议进行转换[2]。吕鹏等研究了 DL/T 645 协议和 IEC60870 -5 -104 协议, 构建了两种协议相互转换的模型及其软件实现流程图。在经过以太网通信和 485 串口通信、DL/T 645 协议和 IEC 60870-5-104 协议的解析与重组、协议映射关系的建立等一系列调试运行后, 最终实现了两个协议之间的相互转换[3]。针对远动主站和子站之间能否及时并正确通信和系统不能及时发现网络故障等问题, 赵会彬等设计并开发了一个应用于电力远动设备的 IEC60870-5-104 通信协议监听与测试系统, 该系统能够实现对远动主站和子站之间通信的监听与测试, 可以在通信故障发生时立即报警, 为电力远动系统的正常运行提供了保障[4]。徐迅等以 IEC 61850 标准为基础, 建立了配电终端信息模型, 并在该模型中增添了具备远程维护和实时监测功能的逻辑设备。通过将目前常用通信协议的优缺点进行对比后, 提出了采用扩展的 IEC 60870-5-104 协议来实现配电主站与配电终端的信息传递的方案[5]。

针对协议的测试方面, 周鸿艳研究并开发了一款全新的测试软件, 能够真实地模拟主站与配电终端通过 104 协议进行通信, 同时还能够测试配电终端设备对 104 协议的实现符合行业要求, 目前该软件已经成功应用于长沙配电网的测试[6]。李宣义等以河北南网调度自动化实验室为基础, 通过与河北南网 D5000 系统实际运行情况相结合, 针对不同厂家设备 104 协议存在的互操作性问题, 依托 D5000 模拟平台搭建变电站综合自动化调试试验系统, 对 104 协议一致性测试进行研究, 制定了符合河北南网实际运行情况的 104 协议一致性测试流程和方案, 大大地缩短了设备的联调周期, 有效地降低了设备之间互联的风险, 提高了设备入网的检测效率, 在技术上为河北南网今后开展综合自动化设备投运前评估和在运设备定期巡视提供了有力支撑[7]。

针对 104 协议可能出现报文内容遭受窃听篡改的问题, 刘园园设计并实现了带报文加密与访问认证的安全通信协议, 并开发了以安全机制为基础的远动终端应用软件, 增加了报文传输的安全性[8]。马钧等以采用 IEC60870-5-104 协议的配电自动化通信系统 EPON 为对象, 针对其网络安全的现状, 分析了配电系统通信的安全需求, 以消息重要性为依据, 在原协议基础上新加了身份认证的不同方法, 提出了一种安全协议, 用来确保配电自动化系统运行的可靠性, 防止了假冒主站对终端进行虚假操作, 实现了主站对真实的配电终端数据进行分析。该安全协议与现有电力系统安全协议解决方案相比, 具有更高的安全性和效率。下一步将继续设计与开发配电网安全协议仿真系统, 对在配电网通信中使用新协议对抗网络攻击的能力进行进一步评测, 并对安全协议的性能优化进行研究[9]。

上述方法在一定程度上解决了 104 协议通信建模、测试和安全传输的困难, 并且实现了协议的加密。但是, 如刘园园的远动终端安全通信协议 RTUSec 使用了数据加密及消息认证双重安全保障机制, 使得经过安全处理后的通信报文长度过长, 在一定程度上限制了报文传输的速度与效率。

本文针对当前存在的问题, 针对馈线终端 FTU 与主站的通信系统, ARP 欺骗的中间人攻击可以截获 104 协议数据, 提出了一种基于身份认证的 104 协议的(BM-RAP, Bellovin-Merri based RSA & AES Protocol)改进方法, 抵御中间人攻击的能力, 在虚拟机实验环境下, 完成一次认证时间在 20~80 毫秒, 增强了抵御中间人攻击的能力。

本文后续章节安排如下: 第二部分对 104 协议进行详细的问题分析, 第三部分搭建真实环境, 并对 104 协议进行安全测试及分析, 第四部分针对存

在的安全性问题提出 BM-RAP 算法对 104 协议进行双向身份认证, 在文章的最后, 我们对本文的研究进行总结并提出对未来的展望。

2 问题分析

2.1 配电网 104 协议原型系统

配电网自动化的系统结构可以分为配电主站、配电子站、配电终端三部分。主站一般运作的是工作站、服务器等设备; 终端可以是在架空馈线使用的配电终端 FTU。104 协议采用平衡传输方式, 当区域主站对子站没有传输数据时, 若子站出现数据变化, 则可由子站主动传输变化的数据到主站。

FTU 在实际使用过程中的通信环境如图 1 所示。FTU 和开关刀闸相连, 实时监测刀闸闭合断开状态。并且, FTU 把监测的数据通过路由器传送到配电子站。本实验平台所使用的硬件为某厂商生产的 FTU 设备, 按照设备真实地通信环境, 将 FTU 通过网线连接到路由器, 路由器再通过网线与终端电脑进行连接。

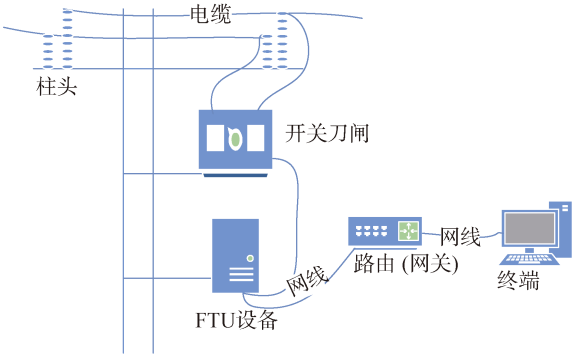


图 1 104 协议的真实通信环境

Figure 1 The true communication environment of the 104 protocol

2.2 协议通信过程

104 协议作为一种网络通信规约, 其通信过程是由客户端和服务端组合而成, 服务端口默认为 2404。104 协议的基本通信流程如下:

(1) 由客户端向服务器发出建立连接的请求, 同时, 发送链路启动帧;

(2) 服务端在接收到客户端发来的链路启动帧后, 向客户端发送启动确认帧;

(3) 客户端在收到服务端发来的启动确认帧后, 向服务端发送总召数据请求帧;

(4) 服务端在收到客户端发来的总召数据请求帧后, 发送总召数据响应帧, 然后继续发送总召数据, 总召数据帧发送完成后, 继续发送总召数据结束帧;

(5) 客户端在接收到总召数据结束帧后, 发送对时请求帧;

(6) 服务端在收到对时请求帧后, 向客户端发送对时响应帧;

(7) 由服务端主动向客户端发送变化数据帧。同时, 服务端会收到客户端发送来的控制类命令, 并回复相应的操作结果;

(8) 客户端等待下一个数据总召周期, 之后再重复第(4)步之后的全部流程。

104 协议的通信交互过程如图 2 所示。

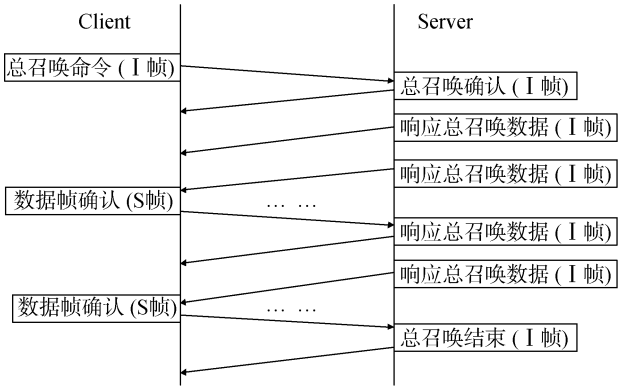


图 2 104 协议通信交互过程

Figure 2 The communication interaction process of 104 protocol

2.3 104 数据结构分析

104 协议将 101 协议与 TCP/IP 提供的网络传输功能进行了结合使用, 处于 OSI 参考模型第七层的应用层, 使用端口号为 2404 的 TCP 协议。

104 协议应用协议数据单元(Application Protocol Data Unit,APDU)的组成包括由应用协议控制信息(Application Protocol Control Information, APCI)和应用服务数据单元(Application Service Data Unit,ASDU)两部分, 如图 3 所示。

104 协议对启动字符和 ASDU 的长度规范和控制域进行了定义。其中, 控制域定义包括抗报文丢失和重复传送的控制信息、报文传输的启动和停止以及传输连接的监视。控制域的主要作用如下:

(1) 带有编号的信息传输格式(I 格式), 主要用于传输信息报文, 该格式上带有发送和接收的, 方便接收方对报文进行及时有效的确认。

(2) 带有编号的监视功能格式(S 格式), 该格式主要用于本站在一段时间内不需要发送信息帧时, 向另一方发送已经收到的信息帧的序列号, 方便接收方对发送方进行确认。

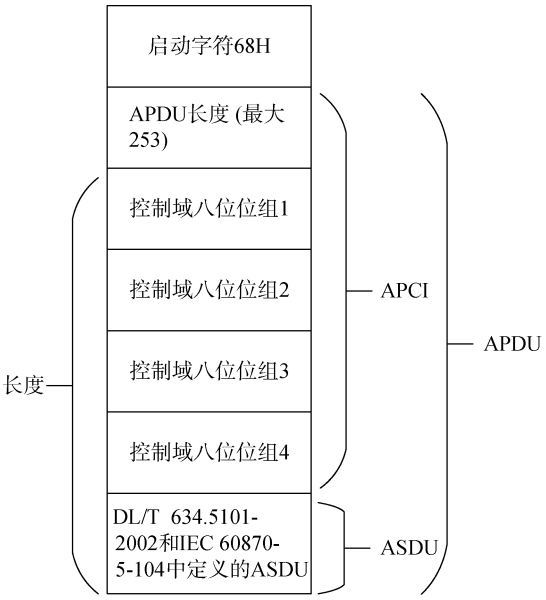


图 3 APDU 结构

Figure 3 The architecture of APDU

(3) 不编号的控制功能格式(U 格式), 该格式的作用就是发起链路测试命令和确认, 启动数据传送命令和确认, 停止数据传送命令和确认。

ASDU 的构成主要包括数据单元标识符和信息对象, 而且所有 ASDU 的数据单元标识符和信息对象的结构都是相同的。

2.4 安全问题

104 协议本身存在着不少的安全漏洞与隐患, 一旦这些漏洞和隐患被攻击者发现并加以利用, 就能够轻松对使用 104 协议的通信系统进行各种攻击, 轻者通信数据会被攻击者截获, 导致通信内容的泄露, 严重的话会导致整个系统的崩溃, 威胁电力系统的安全。

104 协议所存在的安全问题包括如下几个方面:

(1) 104 协议传输报文采用的是明文传输方式, 没有对应用数据单元进行任何加密, 所有功能的传输内容都是明文的。所以 104 协议面临着关于信息保密性和数据完整性的问题, 协议传输的报文很容易被攻击者窃取, 如果 FTU 与控制中心的通信数据被中间人获取, 攻击者可以随意对报文进行修改和伪造, 达到攻击的目的, 可能导致整个系统通信紊乱, 更为严重的, 可能引起系统的崩溃。

(2) 主站对召唤数据没有相应的认证, 同时子站对主站发出的控制命令也没有认证, 因此攻击者能够进行非法访问, 并对报文进行伪造和窃取。一旦攻击者冒充主站向子站发送虚假的调度控制命令, 可能会导致整个系统的瘫痪。

(3) 104 协议规定了防止报文丢失和重发机制来确保应用层 ASDU 的通信可靠性。104 协议通信过程主要以报文附加的接收序号为依据, 进而确认成功传输到接收端的报文数量, 通过对比报文计数器的数字来确认报文是否丢失。一旦序号不正确, 则判定报文丢失, 将会断开进行重新连接。一旦攻击者能够监听报文并预测到确认序号, 那么就能伪造报文, 进而对系统造成威胁。

(4) 104 协议通信时如果发送 12 个 APDU 未收到确认报文时, 应中止传输; 因此如果攻击者截断报文, 将会造成系统在等待 12 个 APDU 发送后得不到确认, 进而会使网络断开, 无法通信。

(5) 104 协议的 U 帧格式可以控制 104 协议交互过程的开始与停止。而 104 协议在启动 U 帧格式之后, 其序列号通常都是以 0 或 1 开始的, 这样黑客能够非常轻易地进行重放攻击。同时, 由于序列号的内容并没有经过完整性措施进行保护与加密, 因此也很容易被黑客利用并进行篡改, 最终达到重放攻击的目的。

104 协议在通信过程中可能遭受中间人攻击的环节如图 4 所示。

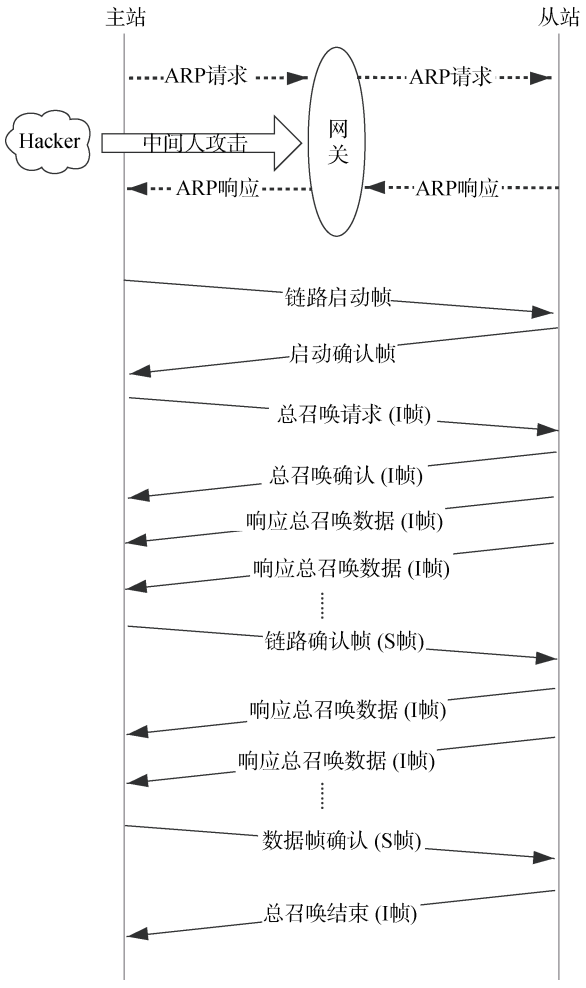


图 4 104 协议通信过程中存在的攻击漏洞

Figure 4 Attack vulnerability during the 104 protocol communication

在图 4 中, 在主站与从站通过网关建立 104 协议通信之前, 首先需要确定通信双方的 IP 地址所对应的 MAC 地址, 并通过目的 IP 地址与 MAC 地址发送 104 协议的数据包。在这一过程中, 攻击者可以通过伪造的 ARP 协议数据包将自己伪装成目标主机和网关, 从而发起中间人攻击, 进而截获 104 协议通信过程中后续的所有数据包, 最终能够进行篡改 104 协议数据等恶意行为。

3 实验测试与分析

3.1 实验环境

本实验系统通过某厂商的 FTU 设备、路由器和终端电脑组成, 硬件设备物理连接情况如图 5 所示。在完成物理连接之后, 在终端电脑上安装并运行 PMA 通信协议分析及仿真软件。

图 5 实验硬件设备连接图

Figure 5 Hardware device connection diagram

本文首先通过使用 PMA 通信协议分析及仿真软件来验证 104 协议是通过明文传输, 该软件是专业的电力调度 PMA 测试工具, 可以模拟主从站之间的通信过程。

首先我们在软件中对主从站的通信地址进行配置, 配置完成后就可以对主从站进行通信连接, 如图 6 所示, 主从站链路连接成功并能进行实时通信。

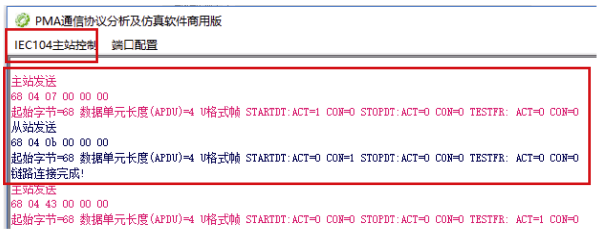


图 6 主从站链路连接及通信报文界面

Figure 6 Master-slave link connection and communication message interface

通过与图 7 所示的从站报文传输界面进行对比可以发现, 104 协议确实是通过明文进行数据传输, 没有进行任何加密, 通信安全性受到很大影响。

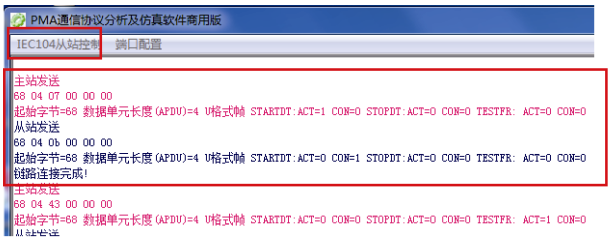


图 7 从站报文传输界面

Figure 7 Slave message transmission interface

3.2 中间人攻击

中间人攻击是指攻击者在不被通信双方发现的情况下, 与通讯双方分别建立单独联系, 控制整个通信过程, 嗅探并篡改数据。

本实验网络环境配置如下:

攻击者 IP 地址 192.168.0.129

物理地址(MAC): 00-0c-29-d3-56-45

目标主机 IP 地址: 192.168.0.183

路由(网关)IP: 192.168.0.1

物理地址(MAC): 0c-4b-54-17-0c-8c

网络拓扑结构如图 8 所示。

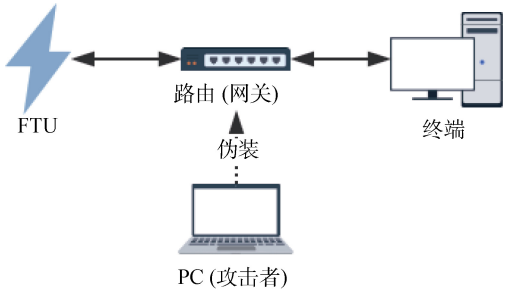


图 8 网络拓扑结构

Figure 8 Network topology

终端电脑与 FTU 成功连接之后, FTU 指示灯呈现绿色, 表示通信功能正常, 如图 9 所示。

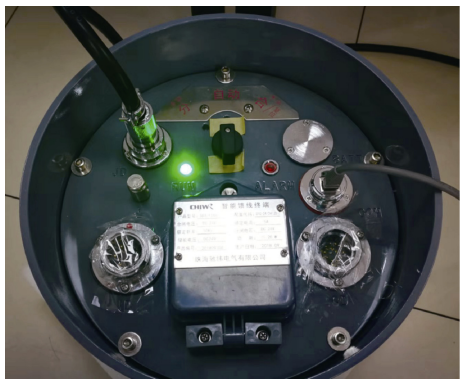
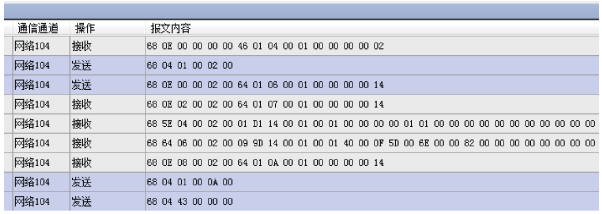


图 9 FTU 通信设备

Figure 9 FTU communication function is normal

可以通过终端维护软件对通信数据进行读取, 通信报文内容如图 10 所示。



通信通道	操作	报文内容
网络104	接收	68 0E 00 00 00 00 46 01 04 00 01 00 00 00 00 02
网络104	发送	68 04 01 00 02 00
网络104	发送	68 0E 00 00 02 00 64 01 06 00 01 00 00 00 00 14
网络104	接收	68 0E 02 00 02 00 64 01 07 00 01 00 00 00 00 14
网络104	接收	68 52 04 00 02 00 01 D1 14 00 01 00 01 00 00 00 00 01 01 00 00 00 00 00 00 00 00 00 00 00
网络104	接收	68 64 06 00 02 00 09 9D 14 00 01 00 01 40 00 0F 5D 00 6E 00 00 82 00 00 00 00 00 00 00 00
网络104	接收	68 0E 08 00 02 00 64 01 0A 00 01 00 00 00 00 14
网络104	发送	68 04 01 00 0A 00
网络104	发送	68 04 43 00 00 00

图 10　通信报文读取

Figure 10　Communication message reading

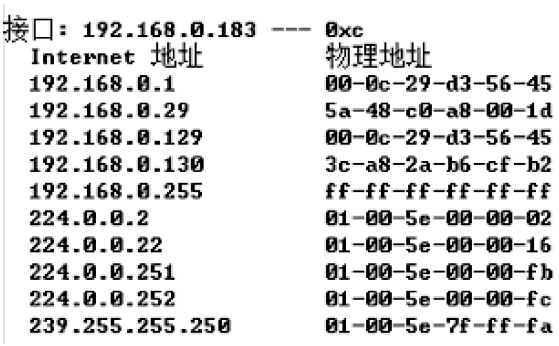
运行使用 Python 语言编写的 ARP 欺骗程序代码并欺骗成功。ARP 欺骗成功前后, 目标主机的 ARP 缓存列表变化如表 1 所示。

表 1　攻击前后 ARP 表变化

Table 1　The ARP table changes before and after the attack

配置项	攻击前	攻击后
网关 IP	192.168.0.1	192.168.0.1
网关 MAC	0c-4b-54-17-0c-8c	00-0c-29-d3-56-45
攻击者 IP	192.168.0.129	192.168.0.129
攻击者 MAC	00-0c-29-d3-56-45	00-0c-29-d3-56-45

在 CMD 窗口使用 arp -a 命令查看 APR 缓存表, 显示结果如图 11 所示。



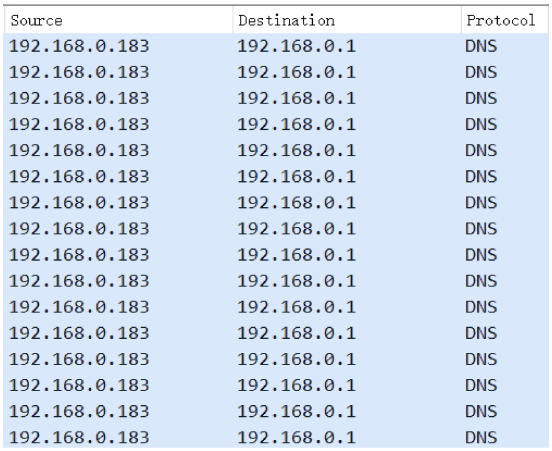
```
接口: 192.168.0.183 --- 0xc
  Internet 地址         物理地址
  192.168.0.1           00-0c-29-d3-56-45
  192.168.0.29          5a-48-c0-a8-00-1d
  192.168.0.129         00-0c-29-d3-56-45
  192.168.0.130         3c-a8-2a-b6-cf-b2
  192.168.0.255         ff-ff-ff-ff-ff-ff
  224.0.0.2             01-00-5e-00-00-02
  224.0.0.22            01-00-5e-00-00-16
  224.0.0.251           01-00-5e-00-00-fb
  224.0.0.252           01-00-5e-00-00-fc
  239.255.255.250       01-00-5e-7f-ff-fa
```

图 11　ARP 缓存表显示结果

Figure 11　The displayed result of ARP cache table

从目标主机 ARP 缓存列表欺骗前后的变化可以发现, 目标主机 ARP 缓存列表的网关 192.168.0.1 的 MAC 地址由攻击之前本身真实的物理地址 0c-4b-54-17-0c-8c 变成了攻击者主机的 MAC 地址 00-0c-29-d3-56-45。也就是说, 攻击者成功地欺骗了目标主机和 FTU 设备, 在两者的通信过程中充当了中间人。

在实现 ARP 欺骗后, 104 协议通信被攻击者劫持, 监控终端与 FTU 设备无法再通过网关建立连接, 如图 12 所示。



Source	Destination	Protocol
192.168.0.183	192.168.0.1	DNS
192.168.0.183	192.168.0.1	DNS
192.168.0.183	192.168.0.1	DNS
192.168.0.183	192.168.0.1	DNS
192.168.0.183	192.168.0.1	DNS
192.168.0.183	192.168.0.1	DNS
192.168.0.183	192.168.0.1	DNS
192.168.0.183	192.168.0.1	DNS
192.168.0.183	192.168.0.1	DNS
192.168.0.183	192.168.0.1	DNS
192.168.0.183	192.168.0.1	DNS
192.168.0.183	192.168.0.1	DNS
192.168.0.183	192.168.0.1	DNS
192.168.0.183	192.168.0.1	DNS
192.168.0.183	192.168.0.1	DNS
192.168.0.183	192.168.0.1	DNS
192.168.0.183	192.168.0.1	DNS

图 12　抓包结果

Figure 12　The result of packet capture

同时, 由于攻击端没有运行 FTU 通信程序, 因此对 FTU 发送的数据无响应, 最终导致 104 协议通信环境的瘫痪。

4　抗中间人攻击算法

4.1　安全模型

在使用 104 协议一类的工业通信环境下, 将基于 BM-RAP 算法进行双向身份认证的 Server 端和 Client 端程序分别部署到相应终端, 只要在工业通信进行前对网络内终端身份加以认证, 那么攻击者就无法以中间人攻击的方式伪装网关, 这样就能够有效保障接下来的正常通信的安全性。

在工业协议通信环境中, 连接在同一网关下的 Server 端与 Client 端通过使用身份认证程序来进行双向身份认证。当验证能够成功通过时, 则 Server 端、网关、Client 端三者就可以构成安全的局域网络, 在该网络下进行工业通信的所有设备的身份均是可信的, 通过配置路由规则等方式可以将包括攻击者在内的其他无关设备拦截在外。这样的安全网络拓扑结构如图 13 所示。

类似前文所述的针对 104 协议通信环境的身份认证实验, 在一般性情况下, 给出适用于更多工业协议的基于身份认证的抗中间人攻击安全通信通用模型, 在后期研究中将加以验证和扩展, 如图 14 所示。

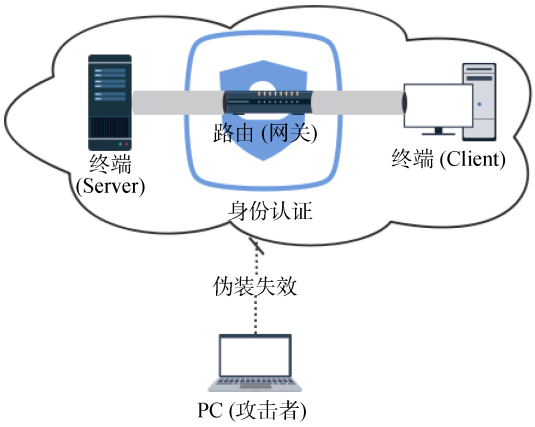


图 13　安全网络拓扑结构

Figure 13　Secure network topology

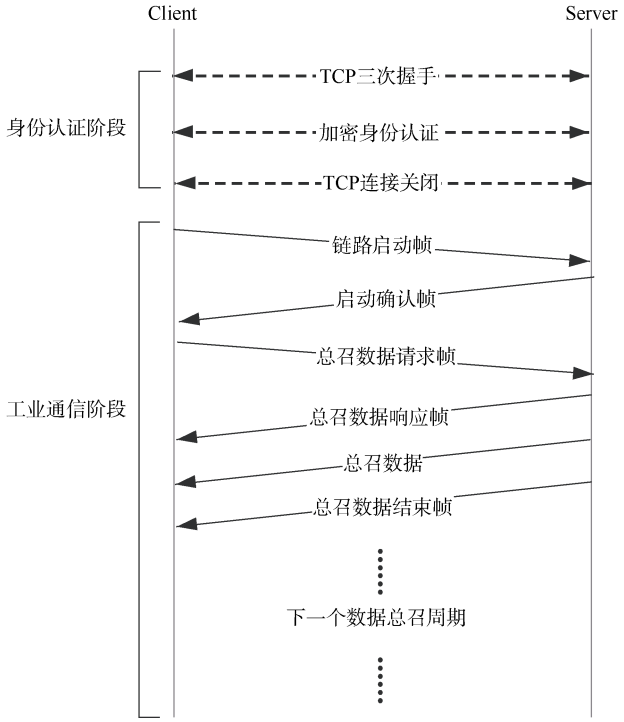


图 14　安全通信通用模型

Figure 14　General model of secure communication

将身份认证算法的应用背景推广到更一般的情况下, 我们提出了如下的基于身份认证的一般性安全通信算法:

算法 1: 基于身份认证的一般性安全通信算法

输入: 无

输出: 无

步骤:

1. 在需要通信的 Server 端与 Client 端之间建立 socket 连接;
2. 分别使用身份认证算法对两端身份加以认证;
3. IF (Server 认证通过&&Client 认证通过)

关闭 socket 连接;

建立 104 等协议通信;

ELSE

关闭 socket 连接;

终止通信。

4.2　基于 BM-RAP 抗中间人攻击算法

从 104 协议安全性测试的目的出发, 为了增强 104 协议下的通信数据机密性、完整性、可用性与可控性, 针对典型的中间人攻击, 本文基于 Bellovin-Merrit 协议, 提出 BM-RAP(Bellovin-Merri based RSA & AES Protocol)算法, 实现了身份认证与抗中间人攻击, 为 104 协议通信提供更安全可信的环境。

BM-RAP 算法用到两个 AES 对称加密方案和一个 RSA 公钥加密方案作为基本元素, 两个对称加密方案的加密算法分别记做 E0 和 E1, 公钥加密算法记做 E, pw 是 A、B 共享的口令字, 用于身份认证与加密传输。详细步骤如下:

(1) A 随机生成公私钥对 pkA-skA, 用口令字 pw 对 pkA 进行加密并发送给 B;

(2) B 收到后, 随机生成会话密钥 Ks, 通过对称加密算法 E0 解密得到 pkA, 用 pkA 加密 Ks, 再次使用 E0 算法以 pw 为密钥进行双重加密, 将结果发送给 A;

(3) A 解密得到 Ks, 随机生成 NA, 然后使用对称加密算法 E1 对 NA 加密并发送给 B;

(4) B 解密得到 NA, 随机生成 NB, 然后将 NA、NB 合并, 使用对称加密算法 E1 对 NA||NB 加密后, 发送给 A;

(5) A 解密后验证第一个分量是 NA, 并得到 NB, 使用对称加密算法 E1 对其加密, 然后发送给 B;

(6) B 接收后解密, 验证明文为 NB。此时身份认证成功, A、B 双方建立可信通信环境;

(7) 当步骤(1)、(2)、(5)和(6)中 A、B 有一方或双发验证失败, 则身份认证失败, 无法进行后续通信。

身份认证流程图如图 15 所示。

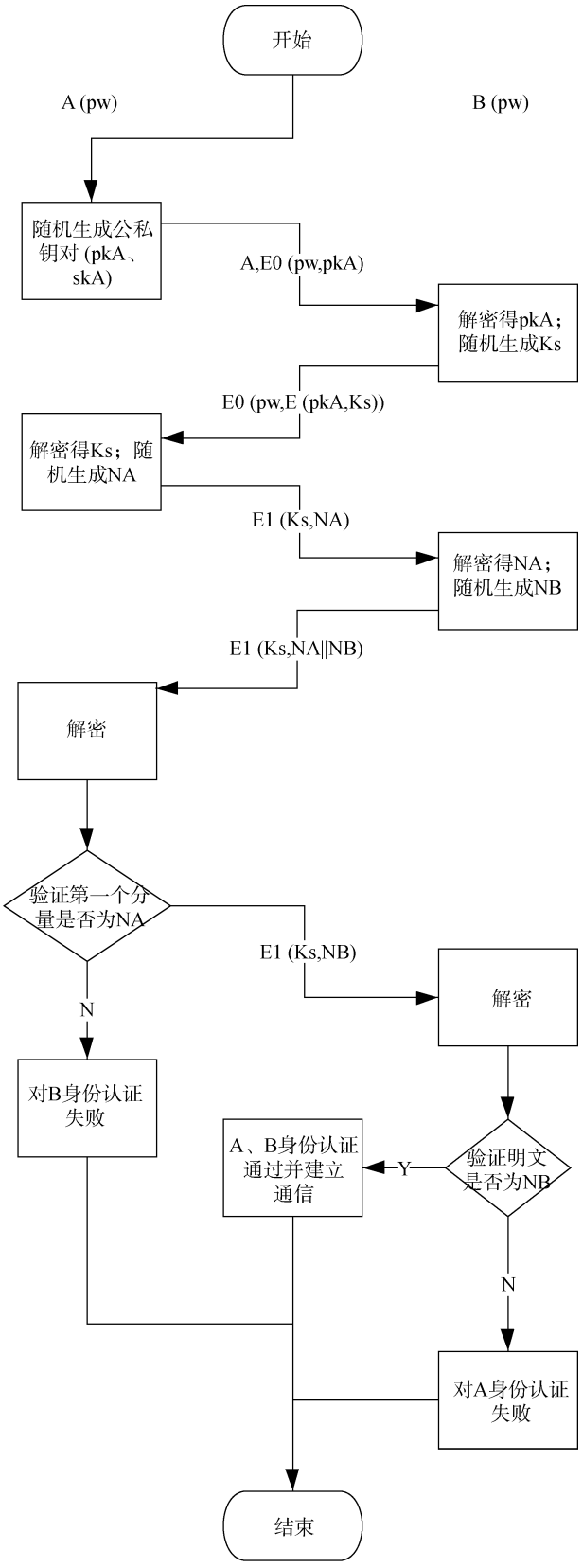


图 15　BM-RAP 算法流程图

Figure 15　The flow chart of BM-RAP algorithm

程序算法描述如下:

算法 2: Client 端 BM-RAP 算法

输入: 无

输出: 身份认证结果

步骤:

1. 初始化, 定义共享口令字 *pw*、用于对称加密方案 E0、E1 的 AES 加解密函数并用公钥加密方案 E 随机生成一对公钥 *pkA* 和私钥 *skA*;
2. 使用给定 IP 和端口号创建与 Server 端的 socket 连接;
3. Client(C)→Server(S):*A*|| E0(*pw*,*pkA*);
4. 解密 E0(*pw*,E(*pkA*,*Ks*))→*Ks*;
5. 随机生成 *NA*;
6. C→S:E1(*Ks*,*NA*);
7. 解密 E1(*Ks*,*NA*||*NB*)→*NA'*;
8. IF

NA=*NA'*

THEN

对 Server 身份认证成功

ELSE

对 Server 身份认证失败;

9. C→S:E1(*Ks*,*NB*);
10. 关闭 socket 连接。

算法 3: Server 端 BM-RAP 算法

输入: 无

输出: 身份认证结果

步骤:

1. 初始化, 定义共享口令字 *pw*、用于对称加密方案 E0、E1 的 AES 加解密函数并用公钥加密方案 E 随机生成一对公钥 *pkA* 和私钥 *skA*;
2. 使用给定 IP 和端口号创建与 Client 端的 socket 连接;
3. 解密 E0(*pw*,*pkA*)→*pkA*;
4. 随机生成 Ks;
5. Server(S)→Client(C): E0(*pw*,E(*pkA*,*Ks*));
6. 解密 E1(*Ks*,*NA*)→*NA*;
7. 随机生成 *NB*;
8. S→C:E1(*Ks*,*NA*||*NB*);
9. 解密 E1(*Ks*,*NB*)→*NB'*;
10. IF

NB=*NB'*

THEN

对 Client 身份认证成功

ELSE

对 Client 身份认证失败;

11. 关闭 socket 连接。

BM-RAP 算法采用了如下策略来抵抗中间人攻击:

第一, 让通信双方共享口令字。只有鉴别双方知道口令字 pw, 任何不知 pw 值的中间人都不能成功冒充 A 或 B。因为双方建立通信的第一步就需要对加密传输的 pw 值进行验证, 与本地预先存储的 pw 值比对, 一致后才进行下一步验证, 不然身份认证将会失败, 通信终止。假定攻击者设法获得了 pw, 但是因为缺少公钥加密算法 E 的公钥 pkA, 同样不能进行身份冒充。

第二, 采用多重加密认证技术, 使得攻击者不能生成针对临时会话密钥 Ks 的有效签名, 从而很难冒充成功。假设攻击者在之前步骤中通过攻击成功得到共享口令字以及公钥, 且成功在第一步的通信中充当了中间人角色, 但为了解密另一方所发送的数据, 攻击者还需要知道对称加密算法 E0 和公钥加密算法 E 的详细设计, 才能通过两层解密得到会话密钥 Ks, 此外, 最后一个阶段的验证还需要对称加密算法 E1。只要加密算法密钥长度足够长, 变换、替换过程足够复杂, 攻击者就面临着几乎无法解决的困难, 因此被动攻击同样无济于事。

104 协议增加 BM-RAP 算法身份认证前后安全性对比如表 2 所示。

表 2 安全性对比

Table 2 Security comparison

	实时性 (4mm)	抗中间人攻击	抗被动攻击
无认证的 104 协议	√	×	×
使用 BM-RAP 算法身份认证后的 104 协议	√	√	√

4.3 实验分析

本实验以 BM-RAP 算法为基础设计了能够进行双向身份认证的 Server 端和 Client 端的 Python 语言程序, 网络环境配置如下:

Client IP: 192.168.15.130
Client MAC: 00-0c-29-12-08-cf
Server IP: 192.168.15.131
Server MAC: 00-0c-29-1d-21-f2
攻击者 IP: 192.168.15.132
攻击者 MAC: 3c-a8-2a-b6-cf-b2
路由(网关)IP: 192.168.15.2
路由(网关)MAC: 00:50:56:fb:fc:8b

网络拓扑结构如图 16 所示。

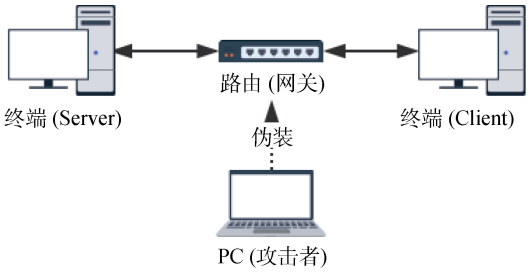


图 16 网络拓扑结构

Figure 16 Network topology

当且仅当 Server 端与 Client 端身份认证通过, 证明两者身份可信, 可安全进行 104 协议通信。如果攻击者通过 ARP 欺骗等方式充当中间人, 那么就无法通过身份认证, 通信连接将被终止, 从而无法窃听或影响 104 协议正常通信。

当攻击者试图冒充 Clienrt 端与 Server 端建立通信时, 身份认证程序显示如图 17、图 18 所示。

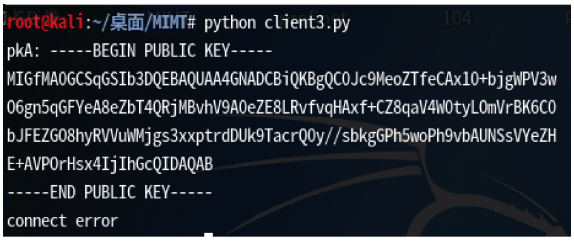


图 17 攻击者 Client 对 Server 的身份认证

Figure 17 Identity authentication of Client of the attacker to Server

图 18 Server 对攻击者 Client 的身份认证

Figure 18 Identity authentication of Server to Client of the attacker

攻击者由于无法通过窃听获得 A、B 双方约定的口令字, 生成新公私钥对, 进而不能伪造新的会话密钥 Ks, 也就无法通过 A、B 身份认证, 使得攻击无效。

进一步, 通过静态路由绑定网关 ARP 表后, 那么攻击者针对网关的 ARP 欺骗就无法实现, 实验验证结果如表 3 所示。

在 CMD 窗口再次使用 arp -a 命令查看 APR 缓存表, 显示结果如图 19 所示, 证明攻击无效。

表 3 防护前后 ARP 表变化

Table 3 The ARP table changes before and after the protection

配置项	防护前	防护后
网关 IP	192.168.0.1	192.168.0.1
网关 MAC	0c-4b-54-17-0c-8c	0c-4b-54-17-0c-8c
攻击者 IP	192.168.0.129	192.168.0.129
攻击者 MAC	00-0c-29-d3-56-45	00-0c-29-d3-56-45

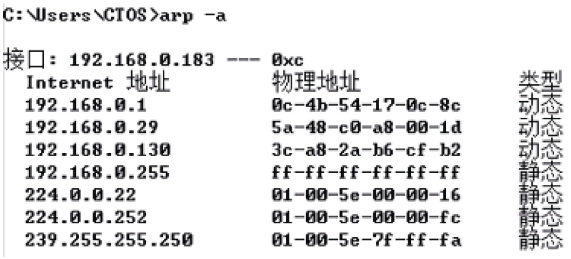


图 19 ARP 缓存表显示结果

Figure 19 The displayed result of ARP cache table

需要指出的是, 由于身份认证程序使用 RSA、AES 等加密算法, 且为 Python 语言开发, 实际测试验证发现认证效率有限, 在实验环境选择使用 VMware Workstation 14 Pro 平台运行 Kali Linux 4.17.0 amd64 虚拟机, 主要硬件为 Intel Core i7-5500U 2.4GHz CPU、2G RAM 且未开启 CPU 虚拟化引擎的条件下, 程序完成一次身份认证所需时间在 20 毫秒至 80 毫秒之间。测试结果记录如图 20 所示。

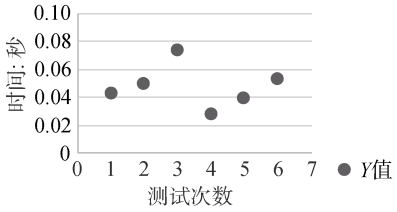


图 20 通信双方完成一次身份认证的时间

Figure 20 The duration of completing an identity authentication

为了满足 FTU 主从站通信 4ms 实时性要求, 认证的过程在建立 104 协议通信前完成, 也就是说, 身份认证过程需要在正常通信之前独立进行。

4.4 进一步工作

现有的抗中间人攻击算法的局限性主要体现在以下几个方面。

(1) 计算耗时较长。因为算法不能满足 104 协议通信实时性要求, 身份认证过程的加入需要独立于通信过程。

(2) 对运行环境有依赖。程序依赖于 Python 环境, 并且需要调用 Crypto 密码类库, 存在一定的部署难度。

(3) 难以抵御时间上串行的重放攻击。如果攻击者在身份认证过程开始之初就利用网络监听或者其他方式拦截并重发所有数据, 那么身份认证就失去了有效性。

基于上述算法局限性的分析, 我们下一步的工作主要是重点研究具有高效性的身份认证机制, 在算法执行效率的基础上通过引入时间戳或流水号的形式提高算法安全性, 针对更多工业协议通信软硬件环境进行优化测试, 提高其普适性。

5 结论

本文在 104 协议通信环境下, 对目标主机成功地进行了 ARP 欺骗, 冒充通信主站与从站之间的网关, 破坏整个通信系统安全。在中间人攻击成功后, 凡是经过目标主机网关的数据都被会发往攻击者的主机, 攻击者可以截获在主从站之间传输的全部数据包, 轻松地获取它们之间的通信报文和采集到的数据信息等。如果馈线终端 FTU 系统遭到大面积的攻击的话, 系统之间传输的数据将大量泄漏, 攻击者将会获取通信过程的所有数据, 并实施重放、篡改、终止通信等攻击手段, 进而对系统的安全稳定运行造成难以估量的威胁。针对典型的中间人攻击, 本文设计实现了抵御中间人攻击的身份认证算法, 将根据该算法编写的相应程序分别部署于主站与从站, 通过实验验证了抗中间人攻击有效性, 为 104 协议通信提供更安全可信的环境, 并且给出了基于身份认证的抗中间人攻击安全通信通用模型, 可向更多工业协议推广。

参考文献

[1] J.N.Sun, M.Z.Liu and K.D.Xu, Design and implementation of PLC communication module based on IEC60870-5-104 telecontrol protocol, *Chinese High Technology Letters*, vol.26,no.4, pp.389-395, 2016.
(孙俊男, 刘明哲, 徐皑冬, “基于 IEC60870-5-104 远动规约的 PLC 通信模块的设计与实现”, *高技术通讯*, 2016, 26(4): 389-395.)

[2] S.Wang, R.W.Huang and J.Wu, Research on IEC 60870-5-104 Protocol and IEC 61850 Interconversion Communication Gateway, *Shanxi Electric Power*, vol.41, no.10, pp.76-79, 2013.
(王飒, 黄若伟, 伍俊, “IEC 60870-5-104 协议与 IEC 61850 互相转换通信网关的研究”, *陕西电力*, 2013, 41(10): 76-79.)

[3] P.Lv, J.R.Wang and K.Xu, Design and implementation of IEC104

protocol and DL/T 645 protocol conversion, *Microcomputer and application*, vol.33, no.18, pp. 4-6, 2014.
(吕鹏, 王俊仁, 许昆, “IEC104 协议与 DL/T 645 协议转换的设计与实现”, *微型机与应用*, 2014, 33(18): 4-6)

[4] H.B. Zhao and X. OuYang, Monitoring of IEC 60870-5-104 communication protocol for power telecontrol equipment, *Value Engineering*, vol.36, no.2, pp. 85-87, 2017.
(赵会彬, 欧阳鑫, “电力远动设备的 IEC60870-5-104 通信协议的监听”, *价值工程*, 2017, 36(2): 85-87.)

[5] X.Xu, J.Mei and C.Qian, Research on Implementation Method of Self-Description Function of Distribution Terminal Based on IEC 60870-5-104 Protocol Extension, Power System Protection and Control, vol.44, no.7, pp.128-133, 2016.
(徐迅, 梅军, 钱超, “基于 IEC 60870-5-104 协议扩展的配电终端自描述功能实现方法研究”, *电力系统保护与控制*, 2016, 44(7): 128-133.)

[6] H.Y.Zhou, “Test scheme and software design of intelligent distribution network terminal equipment based on IEC60870-5-104 protocol[M.S.dissertation]”, *Changsha University of Science and Technology*, Changsha, 2012.
(周鸿艳, 基于 IEC60870-5-104 协议的智能配电网终端设备测试方案及软件设计[硕士学位论文], 长沙: 长沙理工大学, 2012.)

[7] X.Y.Li, B.Liang and J.Q.Li, Research on 104 Protocol Conformance Test Based on D5000 System, *Northeast Electric Power Technology*, vol.10, pp. 13-15, 2017.
(李宣义, 梁宾, 李均强, “基于 D5000 系统的 104 协议一致性测试研究”, *东北电力技术*, 2017, 10: 13-15)

[8] Y.Y. Liu, “Research and implementation of IEC 60870-5-104 protocol based on networksecurity[M.S.dissertation]”, Xi’an Polytechnic University, Xi’an, 2015.
(刘园园, 基于网络安全的 IEC60870-5-104 协议研究与实现[硕士学位论文], 西安: 西安工程大学, 2015.)

[9] J.Ma and Y.B.Zhang, Distribution automation communication security protocol based on IEC60870-5-104, *Computer Science*, vol.40, no.11, pp.81-84, 2013.
(马钧, 张一斌, “基于 IEC60870-5-104 的配电自动化通信安全协议”, *计算机科学*, 2013, 40(11): 81-84.)

王勇 于 2007 年在华东师范大学系统分析与集成专业获得博士学位。现任上海电力大学信息安全系教授。研究领域为电力控制系统信息安全。研究兴趣包括: 电力系统病毒分析与防御。Email: wy616@126.com

王相 于 2019 年在上海电力大学电力信息技术专业获得硕士学位。现任国网上海市电力公司单位见习生。研究领域为电力系统智能巡检、电力系统安全。研究兴趣包括: 无人机智能巡检。Email: ShawnWang611@163.com

刘丽丽 于 2008 年在东北电力大学控制理论与控制工程专业获得硕士学位。现任华电电力科学研究院有限公司分布式能源技术部高级工程师。研究领域为分布式能源系统控制策略研究。研究兴趣包括: 多能互补的分布式能源系统控制策略研究。Email: lili-liu@chder.com

刘金永 于 2017 年在河南理工大学自动化专业获得学士学位。现在上海电力大学电力信息技术专业攻读硕士学位。研究方向为可编程控制器的通信安全性研究。研究兴趣包括: 工业控制系统漏洞挖掘技术, 电力通信安全防护技术。Email: ljy9685@163.com

武津园 于 2017 年在华北电力大学科技学院电气工程及其自动化专业获得学士学位。现在上海电力大学电力信息技术专业攻读硕士学位。研究领域为电力系统状态估计、电力系统虚假数据注入攻击检测, 研究兴趣包括: CPS 系统安全。Email: qqddoo@126.com

李双飞 于 2019 年在上海电力大学信息安全专业获得理学学士学位。 现任上海云剑信息技术有限公司技术部主管。 研究领域为工业网络漏洞挖掘技术、可编程逻辑控制器安全。 研究兴趣包括: 电磁攻击防御技术、工业控制系统动态防护技术。 Email: Frank6122c@outlook.com