

馈线终端单元 FTU 的 101 规约安全性测试

王勇¹, 王相¹, 贺文婷², 周宇昊³, 蔡雨帆¹

(1. 上海电力学院信息安全系, 上海 200090;

2. 华能上海石洞口发电有限责任公司华能上海石洞口第二电厂, 上海 200942;

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, 浙江 杭州 310030)

摘要: IEC60870-5-101 规约主要用于电力 SCADA 数据监控采集系统主站和子站之间传输报文, 由于该报文主要采用“帧校验和”的方式, 其安全性较低, 存在中间人攻击的安全隐患。为了验证该 101 规约的通信存在问题, 构建了馈线终端 FTU 与主站的通信系统, 在云服务器上采集 FTU 移动物联卡的遥测信息, 利用中间人攻击方式, 采用 ARP 欺骗截获通信数据分组, 解析数据分组中的遥测信息, 尝试数据篡改并成功使监控端数据得不到及时更新, 最后提出了一种基于 Hash 签名的 101 规约安全机制。

关键词: 馈线终端 FTU; 101 规约; 中间人攻击; ARP 欺骗

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2018080

Security test of 101 protocol of FTU

WANG Yong¹, WANG Xiang¹, HE Wenting², ZHOU Yuhao³, CAI Yufan¹

1. Department of Information Security, Shanghai University of Electric Power, Shanghai 200090, China

2. Huaneng Shanghai Shidongkou Second Power Plant, Huaneng Shanghai Shidongkou Power Generation CO., LTD., Shanghai 200942, China

3. National Energy Distributed Energy Technology Research and Development (experimental) Center,
Huadian Electric Power Research Institute Co., LTD., Hangzhou 310030, China

Abstract: The IEC60870-5-101 protocol is mainly used for transmitting messages between the primary station and the substation of the power SCADA data monitoring and acquisition system. Since the message mainly adopts “frame check and sum” to ensure communication security, there is a common security risk among the intermediate personnel. In order to verify the communication problems of the 101 protocol, the communication system between the FTU and the main station of the feeder terminal was constructed, which collected the telemetry signal of the FTU mobile IoT card on the cloud server, and used the man-in-the-middle attack mode to use the ARP to intercept the communication data packet. To analyze the telemetry information in the data packet, try data tampering and successfully make the monitoring data not updated in time. Finally, an enhancement mechanism against external attacks was proposed.

Key words: FTU, 101 protocol, man-in-the-middle attack, ARP spoofing

收稿日期: 2018-08-09; 修回日期: 2018-09-08

通信作者: 王勇, wy616@126.com

基金项目: 国家自然科学基金资助项目 (No.61772327); 上海自然科学基金资助项目 (No.16ZR1436300); 浙江大学工业控制技术国家重点实验室开放式基金资助项目 (No.ICT1800380); 上海电力学院智能电网产学研开发中心基金资助项目 (No.A-0009-17-002-05); 上海市科委地方能力建设基金资助项目 (No.15110500700)

Foundation Items: The National Natural Science Foundation of China (No.61772327), Shanghai Natural Science Foundation (No.16ZR1436300); Zhejiang University State Key Laboratory of Industrial Control Technology Open Fund (No.ICT1800380), Smart Grid Industry-University Research and Development Center Project of Shanghai University of Electric Power (No.A-0009-17-002-05), Project of Shanghai Science and Technology Committee under Grant (No.15110500700)

1 引言

IEC 60870-5-101 规约是国际电工委员会为适应电力系统和其通信方面的工作制定的基于 EPA (enhanced performance architecture) 模型的基本远动任务的标准。它主要在具有电网数据采集和监控系统 (SCADA, supervisory control and data acquisition) 的主站和馈线远端单元 FTU (feeder terminal unit) 之间通过问答方式进行数据传输, 如总召唤、一级数据和二级数据上报、时钟同步及远端遥控等^[1]。

由于 101 规约在制定时仅仅考虑了功能的完整性, 并未对其通信的安全性加以考虑, 攻击者很容易利用规约的漏洞对通信系统造成攻击, 截获并篡改通信数据, 甚至能使通信系统瘫痪而无法正常工作。因此, 研究和分析 101 规约的安全性对提高主从站之间的通信安全具有重要意义。

本文主要做了以下工作。

1) 搭建了真实的实验环境, 使用真实的 FTU 设备与云服务器主站进行硬件连接并实现, 能够遥测到 FTU 的工作电压。

2) 针对 101 规约本身存在的安全漏洞进行分析, 发现其存在的若干安全性问题, 并通过主从站通信的真实实验结果验证规约存在明文传输这一安全漏洞。

3) 通过中间人攻击手段对系统进行攻击测试, 实施 ARP 欺骗, 能够成功截获主站与 FTU 之间的通信报文, 加以分析得到主从站之间的通信内容。在中间人攻击测试成功之后, 本文还进行了数据篡改测试实验, 并能够使监控端软件上的遥测数据得不到及时更新, 但还不能真正修改通信数据。

4) 为了加强 101 规约通信的安全性, 本文以 Hash 函数和数字签名为基础, 提出了一种增强 101 规约安全性的安全机制。

本文实验的结论对提高 101 规约的安全性有一定的帮助, 并为后续篡改通信数据的研究提供基础, 以期更好地保护 101 规约通信的安全。

2 国内外研究现状

针对 IEC60870-5-101 规约的安全性相关问题, 国内外研究人员做了诸多研究。闫飞飞^[1]设

计了一款以 32 位 DSP 浮点 CPU(TMS320F28335) 为基础的新型 FTU, 并且在新型 FTU 的 $\mu\text{C}/\text{OS-II}$ 上对 101 规约通信进行测试, 结果表明, 101 通信程序能精准快速地上传通信数据, 满足馈线自动化对 FTU 通信的要求。刘柳^[2]针对 101 规约的帧格式和传输特性, 进行了多方面的安全性分析, 得出了 101 规约本身的脆弱性问题, 同时还分析了可能存在的攻击手段。刘柳针对 101 规约的安全性问题, 建立了一种以攻击树为基础的防御图模型, 并利用防御图对通信的安全等级进行推断, 推断的依据是预期的攻击成功率。王昕等^[3]以云南电网调度系统中远动设备的真实运行情况为基础, 利用 C++ 编程语言设计了基于 101 规约远动设备的测试分析系统, 能够互联不同的基于 101 规约的远动设备, 不但实现了对测试报文和测试数据的分析处理, 同时还通过 Access2003 软件进行数据库建立, 用来存储程序运行过程中 101 规约的报文转换结果数据。杨艳华^[4]提出并设计一种 Modbus RTU-IEC60870-5-101 数据汇集与规约转换装置, 不但解决了 2 种协议之间通信的转换问题, 而且克服了主站同时向多个从站采集数据时效率低的问题。目前该装置已经成功被实际应用到多种配电自动化控制系统中。李克文等^[5]根据配电自动化通信的特点, 对 101 规约的平衡式传输方式或非平衡式传输方式进行选择和补充, 并加以多次测试和修改, 提出了一种基于 IEC60870-5-101 规约的数据传输协议, 并成功应用到配电自动化的无线公网通信系统。唐明等^[6]以 101 规约一致性测试要求和测试系统功能需求为基础设计了一个一致性测试系统, 使用 UML 设计和实现了系统的软件架构和组成, 并针对一致性测试所要求的动态、静态测试给出了相应的测试办法。该系统已经成功应用到馈线终端 FTU 的开发测试和工厂测试。

综上所述, 目前国内外研究很少真正关注 101 规约安全性, 主要着眼于 101 规约的实际应用, 多是将 101 规约与新型 FTU 或者新型远动设备相结合应用, 虽然能够成功在电力系统中使用, 但 101 规约本身存在的安全性问题仍会影响它们的安全通信; 虽然也有研究人员对 101 规约的安

全性和可能遭受的攻击进行了分析,但其分析仅仅停留在理论阶段,并未通过实验对101规约进行实际的安全性测试,无法真实反应101规约的安全性问题。本文研究的重点是101规约的安全性,首先在理论上分析101规约可能存在的安全性问题,并通过真实的实验环境验证101规约的明文传输漏洞,其次是对系统进行安全性测试,成功实现ARP欺骗和造成监控端遥测数据得不到及时更新,最后提出相应的防御措施加强101规约的安全性。

3 IEC 60870-5-101 规约存在的安全问题

IEC60870-5-101规约主要用于电力SCADA数据监控采集系统主站和子站之间传输报文,主站和子站之间进行101规约的传输过程如图1所示。其存在的安全问题主要体现在几个方面:数据校验问题;明文传输;数据流的控制方式。

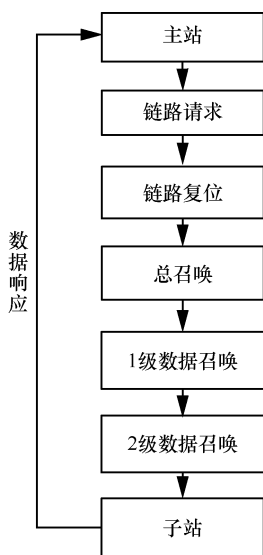


图1 主从站之间的通信流程

1) 数据校验:为了确保数据传输的完整性,传输方指定一种算法对原始数据求取一个校验值,接收方在相同的算法下也计算一个校验值,如果传输和接收双方的校验值相同,则证明数据传输是完整的。101规约有2种帧长结构,即可变帧长结构和固定帧长结构。在可变帧长帧中,帧校验和是控制域、地址域以及用户数据区8位位组的算术和(不考虑溢出位,即256模和);在固定帧长帧中,帧校验和是控制域与地址域的算

术和(不考虑溢出位,即256模和)^[2]。这2种帧长结构中的校验和算法只是进行极为简单的算术和计算,这样仅仅能够保证数据正确传输,并不能够保证其传输安全不被攻击者篡改,所以这种校验和算法并不具备安全性。

2) 明文传输问题:101规约的传输报文采用的是明文传输方式,没有使用加密技术和身份认证技术,报文内容完全没有安全性保障,攻击者能轻松地实施嗅探,通过数据抓包可以对报文进行截获并解析出其中的数据。一旦遭受中间人攻击,通信双方的数据将先传递到攻击者的计算机再转发,此时攻击者能够轻易地获得通信数据并篡改数据内容再进行传递,从而达到攻击目的。

通过使用gcpdbg工具,可以获取主从站之间的通信报文,如图2所示。

[2017-10-21] 16:53:39.318 发送>>>	帧类型 [reset link confirm. (字节数:6)]
10 80 01 00 81 16	
[2017-10-21] 16:53:39.341 接收<<<	帧类型 [init finish frame, typeId=70. (字节数:18)]
68 0C 0C 68 73 01 00 64 01 04 00 01 00 00 02 C2 16	
[2017-10-21] 16:53:39.341 发送>>>	帧类型 [link confirm. (字节数:6)]
10 80 01 00 81 16	
[2017-10-21] 16:53:39.374 发送>>>	帧类型 [gi. (字节数:18)]
68 0C 0C 68 73 01 00 64 01 06 00 01 00 00 00 14 74 16	
[2017-10-21] 16:54:19.371 发送>>>	帧类型 [resend. (字节数:18)]
68 0C 0C 68 73 01 00 64 01 06 00 01 00 00 00 14 74 16	
[2017-10-21] 16:54:20.649 接收<<<	帧类型 [(字节数:6)]
10 00 01 00 01 16	
[2017-10-21] 16:54:20.681 接收<<<	帧类型 [gi ack, typeId=100. (字节数:18)]
68 0C 0C 68 73 01 00 64 01 07 00 01 00 00 00 14 D5 16	
[2017-10-21] 16:54:20.681 发送>>>	帧类型 [link confirm. (字节数:6)]
10 80 01 00 81 16	
[2017-10-21] 16:54:21.162 接收<<<	帧类型 [sse, sseNum=11. (字节数:28)]
68 16 16 68 73 01 00 01 88 14 00 01 00 01 00 01 00 00 00 00 00 18 16	
[2017-10-21] 16:54:21.162 发送>>>	帧类型 [link confirm. (字节数:6)]
10 80 01 00 81 16	
[2017-10-21] 16:54:21.641 接收<<<	帧类型 [response, typeId=6. (字节数:36)]
68 1B 1B 68 73 01 00 09 86 14 00 01 00 01 40 88 00 00 00 00 00 00 00 00 00 00 00 00 00 00 21 16	
[2017-10-21] 16:54:21.641 发送>>>	帧类型 [link confirm. (字节数:6)]
10 80 01 00 81 16	
[2017-10-21] 16:54:22.114 接收<<<	帧类型 [gi term, typeId=100. (字节数:18)]
68 0C 0C 68 73 01 00 64 01 0A 00 01 00 00 00 14 F8 16	
[2017-10-21] 16:54:22.114 发送>>>	帧类型 [link confirm. (字节数:6)]
10 80 01 00 81 16	
[2017-10-21] 16:54:31.427 发送>>>	帧类型 [req link state. (字节数:6)]
10 C9 01 00 CA 16	

图2 101规约通信报文

为了验证能够抓到FTU通过明文方式向主站发送的数据报文,笔者在已知图2中某条报文的基础上,以方框中选中的报文为例,发现wireshark获取的报文中确实存在此条报文,并是以明文传输的,图3方框中的数据就是所采集到的报文。

0000	00 16 3e 02 b9 40 ee ff ff ff ff ff 08 00 45 14
0010	00 4b bd 32 00 00 f3 06 69 63 df 68 ff 64 c0 a8
0020	01 8d be 9c 1e c6 00 07 90 cf 24 fa 98 ad 50 18
0030	0a 74 22 a2 00 00 68 1d 1d 68 53 01 00 09 86 14
0040	00 01 00 01 40 e8 00 00 00 00 00 00 00 00 00 00
0050	00 00 00 00 00 00 00 21 16

图3 验证结果

3) 数据流的控制方式问题: 101 规约传输报文的数据流控制方式采用位 DFC。当 DFC=0 时, 表示子站可以继续接收数据; 当 DFC=1 时, 表示子站的数据缓冲区已满, 无法接收新数据。一旦攻击者截取主站向子站发送的报文之后, 可以将报文的 DFC 设置为 1, 并作为应答报文返回给主站, 这样可以使主站认为子站的数据缓冲区已满, 无法得到所请求的数据, 最终导致无法正常进行调度工作。

除此之外, 101 规约中的广播命令通常用于主站向所有子站发送用户的数据报文, 其链路地址域为 255 或者 65535。一旦攻击者向所有子站发送数量庞大的广播报文, 使子站的数据缓冲区全部被攻击者的广播报文所填充, 最终会导致子站无法正常接收主站所发送的数据。

4 安全性测试分析

FTU 作为馈线自动化系统的重要组成部分, 主要通过 GPRS 模块进行数据通信, 通过 101 规约进行数据传输。然而, 由于操作需要在云端和监控端两端进行, 攻击者可以通过中间人攻击, 对监控端进行 ARP 欺骗, 导致监控端与云端无法进行通信, 对系统正常运行造成影响。

4.1 实验环境

本实验以阿里云 ECS 服务器作为主站, FTU 作为从站, 通过中国移动物联网卡以 GPRS 无线通信方式进行通信, 101 规约采用平衡传输模式, 通过配置 FTU 和主站软件的参数, 以端口映射的方法, 实现主站和从站的通信, 在本机的监控端可以采集到 FTU 的电压、电流以及报文信息。FTU 馈线终端 101 规约的通信环境如图 4 所示。

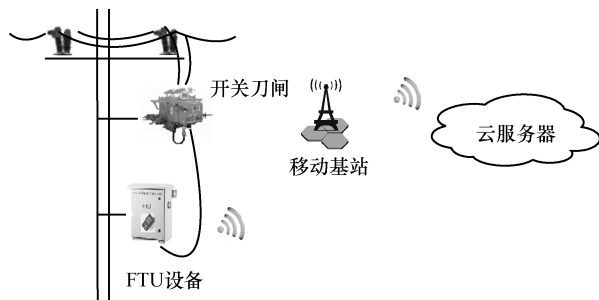


图 4 FTU 馈线终端 101 规约的通信环境

本次实验环境的拓扑结构如图 5 所示。

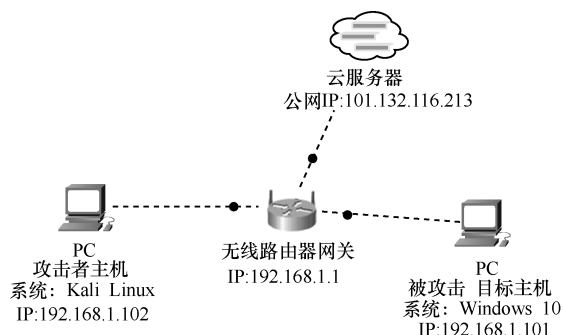


图 5 实验拓扑结构

本次实验所用的是 FTU 设备, 主要安装在架空配电线路的责任分界点处, 与分界开关等设备配合使用, 对分支线路实施保护, 能自动切除线路的相间接地、相间短路、过流等故障, 确保非故障用户的用电安全。采用 32 位 ARM 高速单片机作为主控芯片, 运行速度快、检测灵敏准确、保护动作及时迅速。产品具有无线遥控分合闸、本地串口参数设置、GSM 短信控制、GPRS 无线通信、PDA 掌机通信等通信方式可供选择, 广泛适用于城乡 10KV-66KV 架空配电线路的控制和保护。

本次实验使用 GCP 软件, 有数据库配置工具 (gcpcfg)、gpcpcom.exe 运行软件、实时监控与调试工具 (gcpdbg)。GCP 的作用是连接现场下行设备的物理接口、使用现场设备的通信协议、采集现场设备的数据, 以用户规定的物理接口和通信协议转发数据到本地或远方后台。GCP 平台适应各种通信环境, 满足各种数据交换的需求, 为数据交换提供灵活的解决方案。通常的用法是一路或者多路通信协议采集数据, 数据汇集到一路或者多路通信协议转发。

本实验采用的 GPRS 工具为 ZLAN8100。ZLAN8100 是一款 GPRS 远程无线传输设备, 采用嵌入式设计, 内嵌 TCP/IP 栈。提供标准 RS232/485 数据接口, 可以方便地连接 RTU、PLC、工控机等设备, 并与数据中心通过 GPRS 无线网络建立连接, 实现数据的全透明传输。通过 ZLAN8100 将目的 IP 配置为申请的公网 IP 地址 101.132.116.213, 选择相应的目的端口为 4196。

4.2 安全性测试

4.2.1 第一步: 中间人攻击测试

本文使用中间人攻击的方法实现 ARP 欺骗,

欺骗本机实现拦截正常的网络通信数据,使本机的监控端无法接收到云端的数据,从而导致无法正常采集到 FTU 的电压、电流以及报文信息。

中间人攻击是指攻击者与通信的两端分别建立独立的联系,并交换其所收到的数据,使通信的两端认为它们正在通过一个私密的连接与对方直接对话,但事实上整个会话被攻击者完全控制^[7]。由于 101 规约缺乏身份认证机制,攻击者能够利用这一漏洞,将自己伪装成会话的参与者,最终获取通信双方的通信内容。实现中间人攻击的方式有很多种,但随着技术的发展,中间人攻击已经不能仅靠简单的嗅探攻击实现,必须进行 ARP 欺骗才能使攻击成功。

ARP 欺骗是一种用于内网环境的中间人攻击方式,其优势是通过 ARP 欺骗,能够欺骗整个网络。本次实验采用 Kali Linux 系统中的 ettercap 工具对目标进行 ARP 欺骗攻击。

本次实验的网络环境配置如下。

攻击者主机的 IP 地址: 192.168.1.102; MAC 地址: 3c-a8-2a-b6-cf-b2。

被攻击目标主机的 IP 地址: 192.168.1.101。

路由网关 IP 地址: 192.168.1.1; MAC 地址: 50-fa-84-07-fa-f3。

在攻击之前,通过 `arp -a` 命令查看目标主机的 ARP 表,如图 6 所示。

```
C:\Users\wy616>arp -a
```

接口: 192.168.1.101 --- 0xb	Internet 地址	物理地址	类型
192.168.1.1	50-fa-84-07-fa-f3	动态	动态
192.168.1.100	02-00-02-aa-5b-76	动态	动态
192.168.1.105	28-4e-bf-03-45-01	动态	动态
192.168.1.106	28-4e-ce-2e-98-f0	动态	动态
192.168.1.107	28-4e-a0-03-2e-00	动态	动态
192.168.1.255	ff-ff-ff-ff-ff-ff	静态	静态
224.0.0.22	01-00-5e-00-00-16	静态	静态
224.0.0.252	01-00-5e-00-00-fc	静态	静态
239.11.20.1	01-00-5e-0b-14-01	静态	静态
239.255.255.250	01-00-5e-7f-ff-fa	静态	静态
255.255.255.255	ff-ff-ff-ff-ff-ff	静态	静态

图6 攻击前目标主机 ARP 表

在攻击前通过 `gcpdbg` 工具可以获取遥测数据报文为 68 1D 1D 68 53 01 00 09 86 14 00 01 00 01 40 E8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 21 16。其中,十六进制 E8 转换为十进制后的数值为 232,正是遥测到的 FTU 电压 232 kV,证明攻击前通信功能正常。

配置 Linux 系统的 IP 转发功能,首先保证硬

件连通,然后打开系统的转发功能。打开 `ettercap` 软件,选择 `eno1` 网卡,并开始扫描主机 Hosts-scan for hosts。

扫描完成之后,Hosts-hosts list 将打开主机列表,在主机列表中选择目标主机 IP,单击 Add to Target 1,将其添加到目标 1,告诉目标主机“我是网关”。在主机列表中选择网关地址 192.168.1.1,单击 Add to Target 2,将其添加到目标 2,欺骗网关“我是目标主机”,如图 7 所示。

IP Address	MAC Address	Description
192.168.1.1	50:FA:84:07:FA:F3	
192.168.1.100	02:00:02:AA:5B:76	
192.168.1.101	FC:4D:D4:DA:4B:EB	
192.168.1.105	28:4E:BF:03:45:01	
192.168.1.106	28:4E:CE:2E:98:F0	
192.168.1.107	28:4E:A0:03:2E:00	

图7 主机列表

开启 ARP 投毒功能,通过再次查看目标主机的 ARP 表可以清楚地发现,网关的 MAC 地址已经由攻击之前的 50-fa-84-07-fa-f3 改为攻击者主机的 MAC 地址 3c-a8-2a-b6-cf-b2,如图 8 所示。也就是说,攻击者成功地实施了 ARP 欺骗,充当了目标主机和网关之间通信的中间人,理论上,目标主机与网关的所有通信数据流量都将发送到攻击者主机上,被攻击者窃听。

```
C:\Users\wy616>arp -a
```

接口: 192.168.1.101 --- 0xb	Internet 地址	物理地址	类型
192.168.1.1	3c-a8-2a-b6-cf-b2	动态	动态
192.168.1.100	02-00-02-aa-5b-76	动态	动态
192.168.1.102	3c-a8-2a-b6-cf-b2	动态	动态
192.168.1.105	28-4e-bf-03-45-01	动态	动态
192.168.1.106	28-4e-ce-2e-98-f0	动态	动态
192.168.1.107	28-4e-a0-03-2e-00	动态	动态
192.168.1.255	ff-ff-ff-ff-ff-ff	静态	静态
224.0.0.22	01-00-5e-00-00-16	静态	静态
224.0.0.252	01-00-5e-00-00-fc	静态	静态
239.11.20.1	01-00-5e-0b-14-01	静态	静态
239.255.255.250	01-00-5e-7f-ff-fa	静态	静态
255.255.255.255	ff-ff-ff-ff-ff-ff	静态	静态

图8 ARP 欺骗成功后目标主机 ARP 表

4.2.2 中间人攻击测试结果分析

为了验证攻击成功,通过使用 `ip.addr==192.168.1.101` 命令对数据分组进行筛选,可以看到目标主机和云端之间传输的数据分组全部传输到攻击者的主机上,攻击者可以获取它们之间的通信报文和采集到的数据信息等,如图 9 所示。

No.	Time	Source	Destination	Protocol
43083	887.600658546	192.168.1.101	115.239.210.27	TCP
43086	888.011952310	192.168.1.101	115.239.210.27	TCP
43087	888.011976641	192.168.1.101	115.239.210.27	TCP
43088	888.016699553	192.168.1.101	115.239.210.27	TCP
43093	888.153113407	192.168.1.101	124.74.58.14	ICMP
43094	888.153140710	192.168.1.101	124.74.58.14	ICMP
43095	888.159843733	124.74.58.14	192.168.1.101	ICMP
43096	888.159855867	124.74.58.14	192.168.1.101	ICMP
43097	888.164605188	192.168.1.101	124.74.58.14	ICMP
43098	888.164722162	124.74.58.14	192.168.1.101	ICMP
43099	888.165249100	192.168.1.101	124.74.58.14	ICMP
43100	888.165255318	192.168.1.101	124.74.58.14	ICMP
43101	888.172765851	124.74.58.14	192.168.1.101	ICMP
43102	888.172773433	124.74.58.14	192.168.1.101	ICMP

图 9 筛选后的 101 规约数据分组

在目标主机的监控端打开软件，可以看到，由于受到 ARP 欺骗，目标主机与云端的数据无法正常通信，地址为 101.132.116.213 的云端无法连接，表示攻击成功，如图 10 所示。

4.2.3 第二步：篡改数据测试

经过中间人攻击后，已经能够得到主站（云服务器）传输给监控端的通信数据，由此可以对数据分组进行代理转发或者修改数据分组的内容。本实验目的是依据 IEC60870-5-101 规约的安全漏洞（如数据以明文进行传输、缺乏消息认证、校验方式简单等缺陷）来篡改主站发送给监控端的有关采集电压电流的数据分组，导致在监控端上的数值显示错误。

首先找到包含 FTU 所采集的电压电流的数据分组，通过过滤语句 `ip.addr==101.132.116.213&&tcp contains 01:00:09`（依据地址域和类型标识符）所过滤到的语句如图 11 所示；再将此条报文保存为 .pcap 格式，使用 hexedit 软件，修改数据分组字段，替换掉报文中的信息元素集部分，由于篡改了应用服务数据单元的数据，所以需重新计算校验和，以免校验和错误导致分组丢失。

[illegible]

图 11 过滤遥测数据分组

篡改数据代码使用的是 Python 语言，并应用 raw_socket 函数构造数据分组发送数据，相比普通的 socket，raw_socket 工作在网络层或数据链路层，用来发送一些自己制定源地址特殊作用的 IP 分组。

在 Python 下创建一个 raw socket, 如下。

```
s=socket.socket(socket.AF_INET, socket.SOCK_
RAW, socket.IPPROTO_RAW)
```

根据需要，原数据分组构造 IP header 和 TCP header，如下。

构造 data 部分，将 wireshark 中过滤的包含 FTU 所采集的电压电流的数据分组保存为 .pcap 的文件，但 pcap 文件的格式由文件头（24 byte）+ packet 数据分组头（16 byte）+ packet data 组成，由于本文篡改的数据分组的 IP 头部和 TCP 头部由自己定义，所以只选取 pcap 文件中的 data 字段。

checksum 的计算方法：先将 checksum 的值置 0，将数据以每 2 个字节划分组成一个 16 bit 的值，不够补 0，将所有的 16 bit 相加得到一个 32 bit 的值，将 32 bit 中的高 16 bit 与低 16 bit 相



图 10 中间人攻击导致通信中断

加得到一个新的值,若新的值大于 0xffff,再进行前面的步骤,将最后得出的 16 bit 值按位取反,得到 checksum 的值。

IP 头的 checksum 使用 IP 头数据进行计算, TCP 头的 checksum 包含伪头部加 TCP 头部加 TCP 数据进行计算。

4.2.4 篡改数据测试结果分析

本文的实验目的是修改数据分组中的信息元素集部分,篡改遥测值字段。我们直接使用 hexedit 软件,修改数据分组字段,将原始的电压 223 V (0xDF) 修改为 100 V (0x64),并修改校验和部分,具体帧变化如图 12 所示。



图 12 使用 hexedit 软件篡改数据分组值

在攻击者端运行 tcpattack.py 程序后,可以在监控端抓到所发送的篡改数据分组。但通过实验对比发现,即使发送篡改数据分组的方式相同,

也可能出现多个实验结果。

情况 1 (如图 13 所示): 监控端接收了攻击端发送的篡改数据分组,图中方框内的 seq 和 ack 的数值都等于 1,这不符合逻辑,所以该篡改数据分组并未对主站与监控端的通信产生任何影响。

情况 2 (如图 14 所示): 此次攻击测试所发送的篡改分组被认定为重传分组,而且这一重传分组对主站与监控端的通信造成了影响,出现了多条 ACK 分组,而原本监控端软件设定为 5 min 遥测一次馈线终端 FTU 数据,也未及时更新。

通过篡改数据测试实验可以发现电力系统所存在的不确定性,而本文所搭建的模拟配电网系统也由于实验经费和环境的影响,不是十分完善,所以实验结果存在不确定性。虽然篡改数据测试实验只能造成监控端软件上的遥测数据未得到及时更新,并未达到理想效果,即成功篡改监控端显示的数据,但也能够在一定程度上对电力系统造成影响,因为真实的电力系统安全运行是不允许受到任何因素影响的,即使只是数据未得到及时更新。

4.3 基于 Hash 签名的 101 规约安全机制

针对 101 规约的不足,本文提出了一种基于 Hash 函数和数字签名的增强 101 规约安全性的安全机制,其初始化工作为:密钥生成中心 (KGC) 生成一对公私钥 K_o 和 K_q ,选择一个安全的 Hash 函数 H (可使用 SHA-1 或国密杂凑 SM3 算法等)。

以主站 (S) 发送消息给终端设备 (D) 为例,其过程如图 15 所示。

No.	Time	Source	Destination	Protocol	Length	Info
8158	107.561296	101.132.116.213	192.168.0.10	TCP	892	3400 → 55739 [PSH, ACK] Seq=13806 Ack=2 Win=516 Len=838
9529	232.746433	101.132.116.213	192.168.0.10	TCP	892	3400 → 55739 [PSH, ACK] Seq=1 Ack=5 Win=516 Len=838

图 13 监控端上抓到的由攻击者发送的篡改分组

No.	Time	Source	Destination	Protocol	Length	Info
1214	28.377630	101.132.116.213	192.168.0.10	TCP	892	3400 → 65291 [PSH, ACK] Seq=2261 Ack=19 Win=516 Len=838
2103	54.283592	101.132.116.213	192.168.0.10	TCP	892	3400 → 65291 [PSH, ACK] Seq=11228 Ack=19 Win=516 Len=838
5292	158.349536	101.132.116.213	192.168.0.10	TCP	892	3400 → 65291 [PSH, ACK] Seq=30688 Ack=19 Win=516 Len=838
33732	1009.670786	101.132.116.213	192.168.0.10	TCP	892	[TCP Spurious Retransmission] 3400 → 65291 [PSH, ACK] Seq=11228 Ack=19 Win=516 Len=838
36453	1097.268515	101.132.116.213	192.168.0.10	TCP	1506	3400 → 49480 [ACK] Seq=16049 Ack=43 Win=132096 Len=1452 [TCP segment of a reassembled PDU]
36454	1097.277961	101.132.116.213	192.168.0.10	TCP	1506	3400 → 49480 [ACK] Seq=17501 Ack=43 Win=132096 Len=1452 [TCP segment of a reassembled PDU]
36462	1097.552367	101.132.116.213	192.168.0.10	TCP	1506	3400 → 49480 [ACK] Seq=21857 Ack=43 Win=132096 Len=1452 [TCP segment of a reassembled PDU]
38028	1157.405015	101.132.116.213	192.168.0.10	TCP	892	3400 → 49480 [PSH, ACK] Seq=30249 Ack=43 Win=132096 Len=838 [TCP segment of a reassembled PDU]
41784	1281.362829	101.132.116.213	192.168.0.10	TCP	1506	3400 → 49480 [ACK] Seq=35200 Ack=43 Win=132096 Len=1452 [TCP segment of a reassembled PDU]
45095	1403.460591	101.132.116.213	192.168.0.10	TCP	892	3400 → 49480 [PSH, ACK] Seq=39462 Ack=43 Win=132096 Len=838 [TCP segment of a reassembled PDU]

图 14 TCP 虚假重传

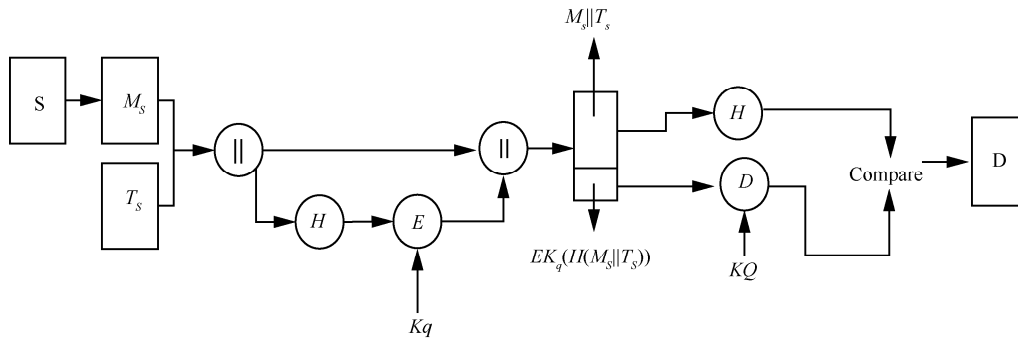


图 15 主站 (S) 发送消息给终端设备 (D)

具体步骤如下。

1) 在主站 (S) 发送消息 M_s (采用 101 通信规约) 的基础上增加时间戳 T_s 以防止重放攻击 $M_s || T_s$ 。

2) 使用已选定的 Hash 函数 H 将其转换成一个定长的消息摘要 $H(M_s || T_s)$ 。

3) 使用之前已分配的私钥 K_q 对消息摘要进行加密, 生成数字签名 $D_s = EK_q(H(M_s || T_s))$ 。

4) 将 T_s 和 D_s 组合在消息 M_s 上, 发送给终端设备 (D): $S \rightarrow D: (M_s || T_s || D_s)$ 。

5) 终端设备 (D) 接收到消息 $(M_s || T_s || D_s)$ 后, 先对时间戳 T_s 进行核对, 确保没有收到重放攻击, 若 T_s 无效则将此消息丢弃。

6) 使用公钥 K_Q 对数字签名 D_s , 并使用已选定的 Hash 函数 H 计算 $M_s || T_s$, 以验证等式 $DK_Q(D_s) = H(M_s || T_s)$ 是否成立, 若成立则消息验证成功, 终端设备 (D) 执行此消息, 否则丢弃此消息。

通过分析以上基于 Hash 函数和数字签名的增强 101 规约安全性的安全机制, 可以防范假冒攻击, 如攻击者假冒主站 (S) 向终端设备 (D) 发送消息, 他随机选择了私钥 K'_q 、散列函数 H' 、当前时间戳 T'_s 以及消息 M'_s 得出数字签名 D'_s , 攻击者将 T'_s 、 M'_s 和 D'_s 组合, 发送给终端 D, 但由于等式 $DK_Q(D_s) = H(M_s || T_s)$ 无法验证通过, 即 $DK_Q(D'_s) \neq H(M'_s || T'_s)$, 所以消息被丢弃。类似地, 攻击者也无法冒充终端设备向主站进行攻击, 无法假冒和篡改协议内容。同时它也可以防范中间人攻击, 如攻击者窃取了主站 (S) 和终端设备 (D) 之间的消息 $(M_s || T_s || D_s)$, 但

由于 hash 函数是单向密码体制, 具有不可逆性, 所以无法得到 hash 函数 H , 同样也无法进行协议内容的篡改。重放攻击也由于时间戳不对应, $DK_Q(D_s) \neq H(M_s || T'_s)$, 而使等式 $DK_Q(D_s) = H(M_s || T_s)$ 无法验证通过。

5 结束语

本文对 FTU 中 101 规约的通信安全性问题进行了分析, 搭建了真实的电力系统馈线终端通道环境, 在云服务器上采集 FTU 移动物联卡的遥测信息, 对于登录到阿里云的目标主机进行了 ARP 欺骗攻击, 可以截获目标主机和云端之间数据分组, 如果馈线终端 FTU 系统遭到大面积 DDoS 攻击, 将会对电力控制系统造成严重影响。

本文也对通信数据进行了篡改攻击尝试, 但实验效果并不理想, 只是使数据得不到及时更新, 尚无法达到最佳的攻击实验效果, 最后提出了一种 101 规约可增强的安全机制对外在的攻击进行防御。

参考文献:

- [1] 闫飞飞. 基于 IEC60870-5-101 规约和 104 规约的 FTU 的设计与实现[D]. 西安: 西安科技大学, 2012.
YAN F F. Design and realization of feeder terminal unit based on IEC60870-5-101 protocol and 104 protocol[D]. Xi'an: Xi'an University of Science and Technology, 2012.
- [2] 刘柳. 面向 SCADA 业务的电力通信传输网安全性评[D]. 北京: 华北电力大学, 2013.
LIU L. SCADA services oriented security evaluation for electric power communication networks[D]. Beijing: North China Electric Power University, 2013.
- [3] 王昕, 曹敏, 李仕林, 等. 远动设备 IEC60870-5-101 非平衡规约

的测试研究[J]. 化工自动化及仪表, 2016 (3): 308-312.

WANG X, CAO M, LI S L, et al. Test and research on unbalanced protocol of IEC60870-5-101 remote control equipment[J]. Control and Instruments in Chemical Industry, 2016(3):308-312.

- [4] 杨艳华, 周永录, 苏红军, 等. Modbus RTU-IEC60870-5-101 数据汇集与规约转换装置设计[J]. 全国冶金自动化信息网 2016 年论文集, 2016: 425-429.

YANG Y H, ZHOU Y L, SU H J, et al. Modbus RTU- IEC60870-5-101 data collection and protocol conversion device design[J]. Annual Conference Proceedings of the National Metallurgical Industry Automation Information Network. 2016:425-429.

- [5] 李克文, 莫凤芝, 吴丽芳, 等. IEC60870-5—101 在配电自动化无线公网通信中的应用[J]. 电力系统通信, 2012, 33(10): 39-43.

LI K W, MO F Z, WU L F, et al. Application of IEC60870-5-101 in distribution automation wireless public network communication[J]. Telecommunications for Electric Power System, 2012, 33(10): 39-43.

- [6] 唐明, 胡勇, 何霄鹏, 等. 配电自动化设备通信协议的一致性测试系统设计与实现[J]. 电气技术, 2014, 15(08): 24-27.

TANG M, HU Y, HE X P, et al. Design and implementation of conformance test system for distribution automation equipment communication protocol[J]. Electrical Engineering, 2014, 15(8): 24-27.

- [7] 张恺. 基于高级量测体系的智能电表双向通信研究[D]. 太原: 太原理工大学, 2011.

ZHANG K. Research on two-way communication of smart meter based on advanced measurement system[D]. Taiyuan: Taiyuan University of Technology, 2011.

- [8] 沈祥, 张俊伟. 基于电力系统 IEC101 规约流程的运维解析[J]. 电气工程与自动化, 2017, 36:21-22.

SHEN X, ZHANG J W. Operation and maintenance analysis based on IEC101 protocol process of power system[J]. Electrical Engineering and Automation, 2017, 36: 21-22.

- [9] CHEN B, CHEN M, TIAN H, et al. Advanced application of IEC60870-5-101 protocol on feeder terminal unit[C]// 11th IEEE International Conference on Anti-counterfeiting, Security, and Identification (ASID). 2017:142-145.

- [10] 邱凯翔, 金宇. IEC101 规约的结构性认识与案例分析[J]. 电工电气, 2018 (6): 62-64.

QIU K X, JIN Y. Structural understanding and case analysis of IEC101 Statute[J]. Electrotechnics Electric, 2018 (6): 62-64.

[作者简介]



王勇 (1973-), 男, 河南确山人, 博士, 上海电力学院教授, 主要研究方向为电力信息安全、电力系统病毒分析、工业控制系统安全。



王相 (1994-), 男, 江苏无锡人, 上海电力学院硕士生, 主要研究方向为电力系统通信协议安全。



贺文婷 (1996-), 女, 浙江镇海人, 主要研究方向为电力系统通信协议安全。



周宇昊 (1983-), 男, 浙江义乌人, 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)中心高级工程师, 主要研究方向为分布式能源政策、产业发展战略、系统集成技术、性能测试评估、检测技术及标准制定。



蔡雨帆 (1997-), 男, 四川内江人, 上海电力学院本科生, 主要研究方向为网络协议安全。