计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2021,30(5):262−268 [doi: 10.15888/j.cnki.csa.007890]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

配电网自动化 DTU 终端的 103 规约的安全性分析①

余　鹏[1], 王　勇[1], 王　相[2], 王　敏[1]

[1](上海电力大学 计算机科学与技术学院, 上海 201306)
[2](国家电网 上海市电力公司检修公司, 上海 200063)
通讯作者: 余　鹏, E-mail: yupeng0201@126.com

摘　要: IEC 60870-5-103 规约是应用于继电保护设备的信息接口配套标准, 传输的主要内容是与继电保护有关的信息. 该报文进行的是明文传输, 缺乏加密措施和数字签名机制, 安全性较低. 为了验证以太网传输的 103 规约存在安全隐患和风险, 搭建了主站与配电网自动化 DTU 终端的通信实验环境. 运用 ARP 欺骗手段对系统进行了中间人攻击测试, 实验的结果表明以太网传输的 103 规约具有中间人攻击的风险. 为了提高协议的安全性, 提出了一种基于非对称密码算法的双向身份认证机制, 并采用对称加密机制、数字签名技术确保传输报文的机密性和完整性, 最后通过仿真测试验证该方法的有效性.

关键词: DTU; 103 规约; ARP 欺骗; 中间人攻击; 身份认证

引用格式: 余鹏,王勇,王相,王敏.配电网自动化 DTU 终端的 103 规约的安全性分析.计算机系统应用,2021,30(5):262–268. http://www.c-s-a.org.cn/1003-3254/7890.html

Security Analysis of 103 Protocol of DTU Terminal in Distribution Network Automation

YU Peng[1], WANG Yong[1], WANG Xiang[2], WANG Min[1]

[1](School of Computer Science and Technology, Shanghai University of Electric Power, Shanghai 201306, China)
[2](Shanghai Electric Power Company Maintenance Company, State Grid Corporation of China, Shanghai 200063, China)

Abstract: The IEC 60870-5-103 protocol is an information interface supporting standard applied to relay protection equipment and transmits mainly the information related to relay protection. The message is transmitted in plain text and has poor security for a lack of encryption measures and digital signature mechanism. A communication experiment environment between the master station and the DTU terminal is built to verify that there are hidden dangers in the 103 protocol of Ethernet transmission. A man-in-the-middle attack test is carried out on the system by detecting ARP spoofing. The experimental results show that the 103 protocol of Ethernet transmission faces the risk of man-in-the-middle attack. In order to improve the security of the protocol, we propose a two-way identity authentication mechanism based on an asymmetric cryptographic algorithm and rely on a symmetric encryption mechanism and digital signature technology to ensure the confidentiality and integrity of the transmitted message. Finally, the method is validated through simulation tests.

Key words: DTU; 103 protocol; ARP spoofing; man-in-the-middle attack; authentication

① 基金项目: 国家自然科学基金面上项目 (61772327); 上海自然科学基金面上项目 (20ZR1455900); 奇安信大数据协同安全技术国家工程实验室开放课题 (QAX-201803); 浙江大学工业控制技术国家重点实验室开放式基金 (ICT1800380)
Foundation item: General Program of National Natural Science Foundation of China (61772327); General Program of Natural Science Foundation of Shanghai (20ZR1455900); Open Project of Qi-Anxin National Engineering Laboratory of Big Data Collaborative Security Technology (QAX-201803); Open Fund of State Key Laboratory of Industrial Control Technology, Zhejiang University (ICT1800380)
收稿时间: 2020-09-03; 修改时间: 2020-09-25; 采用时间: 2020-10-09; csa 在线出版时间: 2021-04-28

IEC 60870-5-103 规约 (以下统称为 103 规约) 是国际电工委员会根据 IEC 60870-5 系列基本标准而制定的, 是用于继电保护设备信息接口的配套标准[1]. 103 规约对变电站自动化系统、厂站自动化系统中的控制系统以及继电保护设备或者间隔单元的信息传输做出了明确规范, 可以用于配电网自动化主站和站所终端单元 (Distribution Terminal Unit, DTU) 之间的数据传输. 由于 103 规约主要考虑的是信息交换数据格式的统一, 不同地区和不同的厂家有着不同的具体实现方式, 有的采用串口通讯, 有的采用以太网 TCP/IP或者是采用以太网 UDP/IP, 甚至可以采用二者结合的方式[2].

103 规约在设计之初并没有考虑到其安全性, 使得攻击者很容易利用规约的漏洞进行攻击, 拦截甚至篡改通信内容, 一旦通信主站接收错误指令或者通信系统崩溃将会给电力系统带来巨大损失. 文章针对基于 TCP/IP 的以太网 103 规约存在的明文传输、易受中间人攻击等漏洞进行分析, 并进一步搭建具体的实验环境进行验证, 最后设计了一种数据安全传输机制, 能很好地抵挡中间人攻击以及明文传输存在的威胁, 一定程度上可以增强该以太网 103 规约的安全性.

本文做以下工作:

(1) 针对 103 规约进行了安全性分析, 指明其存在的若干安全隐患. 并采用 PMA 通信协议分析及仿真软件进行了仿真实验, 获得了 103 规约的通信报文, 验证了该规约的明文传输特性.

(2) 搭建了真实的通信实验环境, 构建基于以太网 103 规约的 DTU 设备与主站的硬件连接, 通过软硬件结合可以遥测到 DTU 设备所采集的电压电流等真实数据.

(3) 使用中间人攻击的方式对系统进行了安全性测试, 可以成功对主站与 DTU 设备通信的网关进行欺骗, 证明该规约存在中间人攻击隐患.

(4) 为增加规约的通信安全性, 提出了一种基于 RSA 非对称密码算法的双向身份认证机制, 并运用高级加密标准 (Advanced Encryption Standard, AES) 和安全散列算法 1(Secure Hash Algorithm 1, SHA-1) 保证传输数据的机密性和完整性, 最后通过 socket 编程进行实现.

1 研究现状

针对 103 规约的研究,国内外学者做了诸多研究. 姬希娜等[3] 针对国家电网以太网 103 规约设计了一种可用于测试规约子站的工具, 该工具既能作为 TCP 连接的客户端, 还可实现 LPCI 测试和基于测试 用例集的应用功能的自动测试, 能有效提高用例错误检测能力. 张磊等[4] 针对日渐复杂和受到限制的装置人机接口, 针对 103 规约的功能不足, 在其基础上扩展了装置菜单读取、权限控制、装置命令等功能, 有效弥补了人机交互功能差, 并在保护装置中进行实际使用. 李鹏等[5] 为解决当前牵引变电站综合自动化系统在高精度实时负荷录波方面存在的诸多不足, 提出一种基于 103 规约扩展的实时负荷录波设计实现方案, 并在实际使用中获得了很好的效果. 韦宇等[6] 采用 103 规约结合 UDP 报文和 TCP 报文建立发电机原有的主保护装置与上位机的通信, 用于保护装置的数据传输, 对发电机实施计算机控制, 经过改造后可实现少人值守甚至无人值班的目标. 雷林绪等[7] 针对输电线路的故障诊断, 为了在修复过程中提高故障定位的准确性, 提出一种应用 103 规约将行波故障测距装置连接到继电保护信息管理系统和变电站监控系统的设计方案, 并介绍了实现的方法和思路. 余梦泽等[8] 对 103 规约在 110 kV 裂心式高压并联可控电抗器控制装置中的一些应用进行介绍, 并对可控电抗器的运行数据结构进行分析, 最后给出在可控电抗器的控制装置中的具体实现方法. 刘亮亮等[9] 肯定了以太网 103 规约对提高继保装置效率和可靠性的作用, 同时浅析了以太网 103 规约在实际中的优点和不足, 并给出一些以太网 103 规约在实际使用中的建议.

综上所述内容, 目前国内外研究人员针对 103 规约的研究大部分还是在实际应用中, 很少关注到安全性方面. 本文通过实验环境的搭建, 重点分析 103 规约存在的安全隐患.

2 103 规约存在的安全问题

2.1 未采用加密通信

103 规约的通信报文进行的是明文传输, 未使用任何有效的加密措施和数字签名机制, 这使得该规约存在一定的安全风险. 攻击者可以通过嗅探方式很容易获得并轻松解析出其中的数据. 如果遭受到中间人攻击, 攻击者很容易对截获的报文进行篡改再转发, 将导致系统的错误决策从而造成经济损失.

为验证 103 规约采用的是明文传输, 我们使用 PMA 通信协议及仿真软件进行仿真实验, 这个软件可以模拟主从站的通信过程. 首先我们在软件中选取相应的规约并分别对通信的主从站进行相关设置, 配置完成后主从站就可以进行通信, 如图 1 所示. 从图中我们可以看到该规约确实采用明文传输, 其通信安全存在隐患.

图 1 主从站通信报文界面

2.2 数据校验方式简单

数据校验是为了确保数据正确传输, 检验数据是否完整的一种验证操作. 首先发送方用指定的算法对原始的通信数据进行计算得出一个校验值, 接收方接收数据后采用相同的算法计算出一个校验值, 然后对比接收到的校验值和自己计算的检验值是否相同, 如果校验值相同, 则数据是正确传输, 没有出现丢失情况. 103 规约是采用简单的帧校验和的方式进行数据校验的. 对于固定帧长格式, 帧校验和为控制域与地址域算术和 (不考虑溢出位,即 256 模和); 对于可变帧长,帧校验和为地址域、控制域及应用服务数据单元算术和 (不考虑溢出位,即 256 模和). 这种校验和算法过于简单, 虽然可以一定程度保证数据传输过程中的正确性, 但是一旦攻击者篡改数据之后对校验位进行重新计算, 很容易可以达到欺骗的目的.

2.3 缺少身份认证机制

以太网 103 规约大都是基于 TCP/IP 协议进行设计的, 在 103 规约的基础上使用 TCP 协议进行数据传输, 导致以太网 103 规约缺乏身份认证机制. TCP 协议的可靠连接是进行以太网 103 规约数据传输的前提, 但是在进行 TCP 连接的时候, 只要知道目的 IP 就可以发起请求从而确定目的 MAC 地址. 攻击者可以利用这一漏洞, 通过伪造 ARP 数据包把自己伪装成目的机, 进而发起中间人攻击截获通信数据包, 攻击者甚至可以对通信数据进行恶意转发和非法篡改操作.

3 安全性测试与分析

3.1 实验环境

本实验系统采用的是某品牌的 DTU 设备、路由器和终端电脑构成, 系统硬件连接图如图 2 所示.

在终端电脑安装 DTU 配套软件并进行相关配置, 将终端电脑 IP 地址设置为 198.120.0.100, 网关设置为 198.120.0.2, 子网掩码为 255.255.0.0. 将 DTU 设备 IP 地址配置为 198.120.0.1, 网关与子网掩码的配置与终端电脑是一样的. 进行连接以后, 使用 wireshark 软件可看到电脑终端与 DTU 设备的通信数据包如图 3 所示, 从图中可看出该以太网 103 规约是基于 TCP 协议的.

图 2 系统硬件连接图

No.	Time	Source	Destination	Protocol
25	0.541274	198.120.0.100	198.120.0.1	TCP
26	0.541351	198.120.0.100	198.120.0.1	TCP
27	0.541495	198.120.0.1	198.120.0.100	TCP
28	0.569659	198.120.0.100	198.120.0.1	TCP
29	0.578282	198.120.0.1	198.120.0.100	TCP
30	0.849768	198.120.0.100	198.120.0.1	TCP
31	0.850362	198.120.0.1	198.120.0.100	TCP
32	0.899650	198.120.0.100	198.120.0.1	TCP
33	0.980519	198.120.0.100	198.120.0.1	TCP
34	0.980850	198.120.0.1	198.120.0.100	TCP
35	0.981182	198.120.0.1	198.120.0.100	TCP
36	0.981375	198.120.0.100	198.120.0.1	TCP
37	0.981700	198.120.0.1	198.120.0.100	TCP

图 3 终端电脑与 DTU 设备的通信数据包

3.2 中间人攻击测试

中间人攻击是一种历史悠久的网络入侵方式, 并且由于它存在巨大的继续开发潜力, 使得它一直以来都是信息安全领域的重要隐患. 中间人攻击的具体攻击方式有 SMB 会话劫持、ARP 欺骗、DNS 欺诈等. 简单来说, 中间人攻击就是在通信双方不知情的情况下, 分别与通信的两方进行单独连接, 拦截和获取网络通信数据, 并可以对通信数据进行嗅探和篡改.

文章使用的是 ARP 欺骗的方式实现中间人攻击,本实验的网络配置情况如下:

攻击者的 IP 地址: 198.120.0.101; MAC 地址: 00-0c-29-b5-48-cc.

路由器的网关 IP 地址: 198.120.0.2; MAC 地址: 48-0e-ec-0c-d7-b4.

目标主机的 IP 地址: 198.120.0.100.

网络拓扑结构如图 4 所示.

在进行攻击实验之前, 在目标主机的 cmd 窗口下使用 arp -a 命令查看 ARP 列表, 如图 5 所示.

本次 ARP 攻击测试实验所采用的工具是 Kali Linux 操作系统中自带的 ettercap 软件进行. 攻击完成以后, 再查看 ARP 列表会发现网关的 MAC 地址已经由原来的 48-0e-ec-0c-d7-b4 变为攻击者的 MAC 地址

00-0c-29-b5-48-cc, 结果如图 6 所示. 这说明攻击者实施 ARP 欺骗成功, 成功地在目标主机与 DTU 设备中间充当了中间人. 当实现 ARP 欺骗后, 监控端与 DTU 设备不能继续通过网关建立正常的连接, 从而导致系统的崩溃.

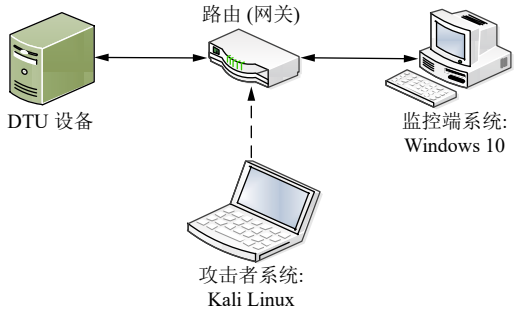

图 4 网络拓扑连接图

```
接口: 198.120.0.100 --- 0x7
  Internet 地址         物理地址              类型
  198.120.0.1           b4-4c-c2-78-00-01     动态
  198.120.0.2           48-0e-ec-0c-d7-b4     动态
  198.120.0.101         00-0c-29-b5-48-cc     动态
  198.120.255.255       ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态
```

图 5 攻击前目标主机的 ARP 列表

```
接口: 198.120.0.100 --- 0x7
  Internet 地址         物理地址              类型
  198.120.0.1           b4-4c-c2-78-00-01     动态
  198.120.0.2           00-0c-29-b5-48-cc     动态
  198.120.0.101         00-0c-29-b5-48-cc     动态
  198.120.255.255       ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态
```

图 6 攻击后目标主机的 ARP 列表

4 数据安全传输机制

4.1 双向身份认证算法

通过以上实验, 我们验证了采用以太网 103 规约的 DTU 设备存在中间人攻击的风险. 现在的配电网终端设备通常都是在线自动注册的, 这给不法分子有可乘之机, 部分非法用户在系统重启时自动连接到系统,所以在主站和配电终端之间进行数据传输之前验证对方身份的合法性很有必要[10]. 针对冒充攻击、中间人攻击等威胁, 文献 [11] 设计了一种基于身份密码体制的挑战/应答式双向身份认证协议, 解决了使用数字证书的身份认证机制中的证书难管理、宽带消耗大等缺点. 文献 [12] 针对传统的公钥基础设施 (Public Key Infrastructure, PKI) 中证书颁发、撤销以及难以实现交叉认证等缺陷, 提出了基于智能合约的去中心化的身份认证机制, 可以实现交叉认证以及满足不同场景下的实际需求. 身份认证是网络安全的第一道防线, 具有非常重要的作用. 我们设计了一种基于 RSA 密码算法双向身份认证机制, 我们将双向身份认证的 Server 端和 Client 端程序部署到相应的终端设备上. 在进行电力数据传输之前首先验证设备的合法性, 从而保证接下来通信的可靠性.

(1) 注册阶段

注册阶段是使 Server 端和 Client 端建立初始信任的过程, 整个过程可以描述为 Server 端和 Client 端在离线过程中交互各自的公钥, 这种直接信任的过程也是最简单直接的方式, 具体注册过程如图 7 所示.

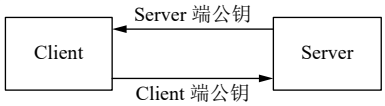

图 7 离线注册过程

(2) 双向身份认证过程

符号说明:

K_{pubc} 表示 Client 端公钥, K_{pric} 表示 Client 端私钥.

K_{pubs} 表示 Server 端公钥, K_{pris} 表示 Server 端私钥.

$EK()$ 表示使用密钥对括号内容进行加密.

$DK()$ 表示使用密钥对括号内容进行解密.

双向身份认证详细步骤如下:

① Client 端生成随机数 N_1, 使用 Server 端公钥 K_{pubs} 对 N_1 进行加密后发送给 Server 端.

② Server 端收到后进行解密得 N_1 并随机生成 N_2, 将 N_1 与 N_2 进行合并得 $N_1||N_2$, 使用 Client 端的公钥 K_{pubc} 进行加密得 $E_{K\text{pubc}}(N_1||N_2)$, 将密文数据发送给 Client 端.

③ Client 端接到数据以后, 首先用自己的私钥 K_{pric} 对密文进行解密, 查看第一个分量是否为 N_1, 如果第一个分量为 N_1 则 Client 端对 Server 端身份认证成功, 否则身份认证失败.

④ Client 端解密得到的第二个分量 N_2 使用 Server 端的公钥 K_{pubs} 进行加密得 $E_{K\text{pubs}}(N_2)$ 发送给 Server 端.

⑤ Server 端对密文解密验证明文是否为 N_2, 如果明文是 N_2 则 Server 端对 Client 端身份认证成功, 也就是双向身份认证成功, 否则身份认证失败.

双向身份认证的流程图如图 8 所示.

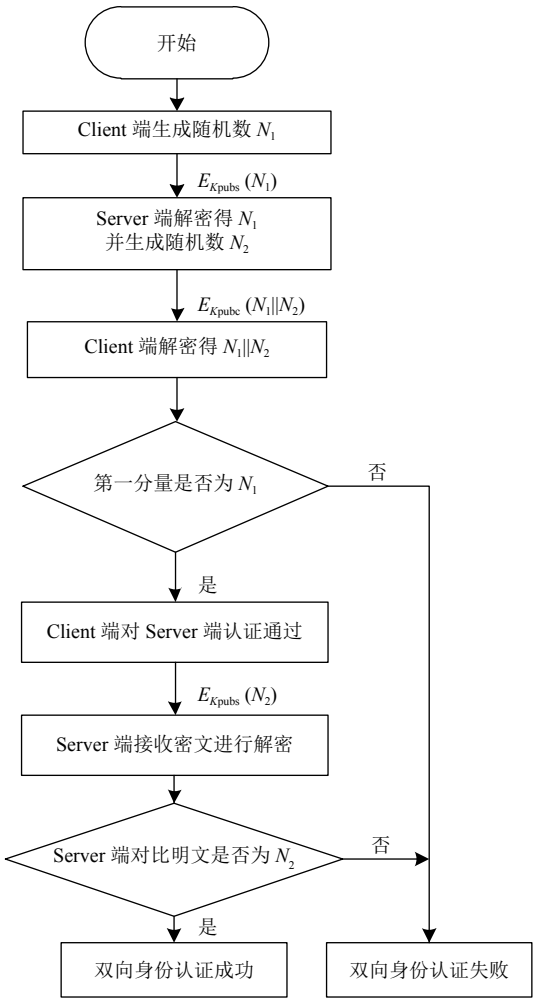

图 8 双向身份认证流程图

4.2 数据加密与签名

103 规约主要用于传输继电保护相关数据, 对数据的完整性保护和来源可靠性具有较高要求[13], 并且该规约采用的是明文传输容易被他人窃听[14,15]. 于是我们采用通信双方协商的规则来确定出后续用于数据加密的对称密钥[16], 文章利用注册阶段互换的 RSA 算法的公钥和 SHA-1 散列算法协商出数据加密密钥 key, 协商具体过程如图 9 所示. 首先由 Server 端生成 AES 加密密钥 key 并利用对方的公钥将其加密发送给 Client 端, Client 端解密后利用自身私钥 K_{pric} 和 SHA-1 散列算法对 key 签名 Sign1(key) 发送给 Server 端, Server 验证签名正确则用自己的私钥 K_{pris} 和 SHA-1 散列算法生成签名 Sign2(key) 发送给 Client, 如果两次签名都验签都正确, 则双方成功协商出数据加密密钥 key. Server 端和 Client 端双方建立通信之前协商出会话密钥的目的是为了保证前向安全, 同时也起到了功能隔离的作用, 在 Client 端和 Server 端虽然存在注册密钥, 如果用注册密钥进行加密通信数据, 一旦密钥泄露将导致所有时间的会话内容泄露, 恰当地使用会话密钥可以有效避免这一点.

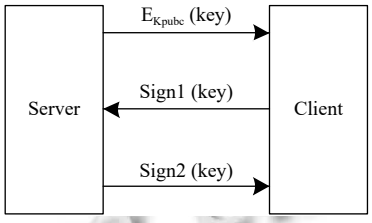

图 9 密钥协商过程

双方协商出密钥 key 后, 发送方使用密钥 key 对数据进行 AES 对称加密, 并同时利用 SHA-1 散列算法和自身私钥生成签名. SHA-1 是一种密码散列函数, 可以将一段明文以不可逆的方式将它转换成一段固定长度的输出也就是消息摘要, 只要原文被篡改将导致消息摘要发生巨大变化. 数字签名是在消息摘要的基础上利用私钥进行再次加密从而形成数字签名, 验签者则需要利用对方的公钥进行验签得到消息摘要, 由于非法者不能拥有合法用户的私钥, 所以这就能够保证数据来源的真实性, 同时也能验证数据在传输过程中是否被篡改, 具体的数字签名过程如图 10 所示.

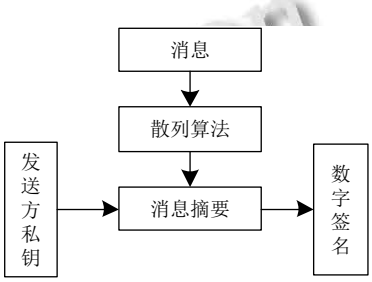

图 10 数字签名过程图

发送方对原始数据进行处理, 进行对称加密得到密文并生成数字签名, 随后将密文和数字签名一起发送给接收方, 数据发送流程图如图 11 所示.

数据接收过程流程图如图 12 所示, 接收方收到密文块和签名块. 接收方使用对称密钥 key 进行解密得到明文 M 并使用与发送方相同的 SHA-1 散列算法进行计算消息摘要, 将计算的消息摘要与运用发送方公钥进行验签得到消息摘要进行对比, 如果一致则认为消息是安全的未被篡改, 同时也能确定数据发送方的身份真实性, 否则数据通道存在不安全因素.

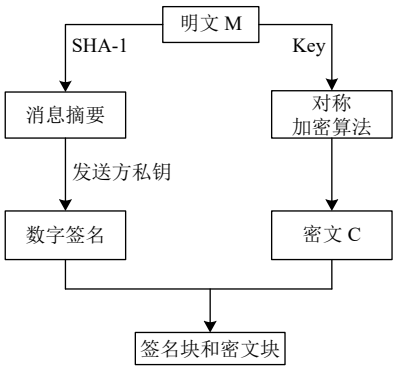

图 11 数据发送流程图

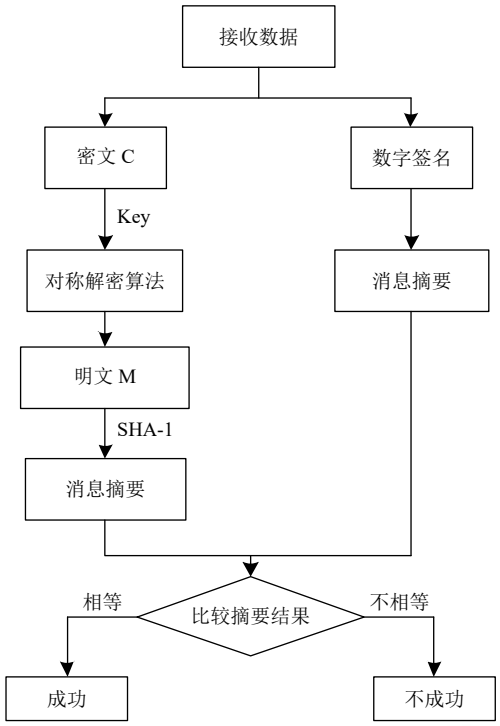

图 12 数据接收流程图

4.3 实验分析

本实验以 socket 为基础设计了能够进行双向身份认证以及数据加密和签名传输的 Server 端和 Client 端的 Python3 程序, 我们可以将相应的程序部署在相应的终端设备上. 通信双方按照我们设定的规则进行数据的交换就可以保证系统通信的安全性, 使得攻击者无法假冒身份进行接入系统, 同时所传输数据的保密性和完整性得到很好的保证, 能够及时发现数据传输过程中导致的误差, 实验的网络环境配置如下:

Client IP: 192.168.1.103.

Server IP: 192.168.1.102.

网关 IP: 192.168.1.1.

非法 Client IP: 192.168.1.105.

仿真实验网络拓扑结构如图 13 所示.

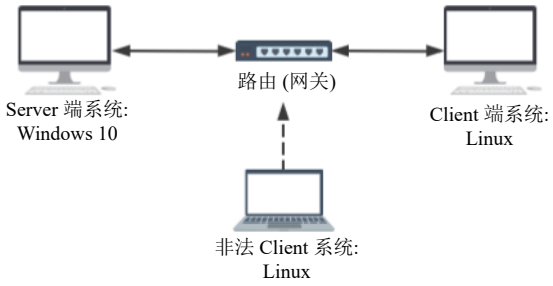

图 13 仿真实验网络拓扑结构

(1) 双向身份认证仿真实验

当且仅当 Client 端和 Server 端互相通过身份认证,才可以建立连接进行数据的传输, 一旦某一方对另外一方身份认证不通过则连接失败, 通信断开无法进行后续的数据传输通信. Server 端与 Client 端身份认证程序运行结果如图 14、图 15 所示, 当两端都认证成功才算是双向身份认证完成.

```
C:\Users\DELL\Anaconda\python.exe F:/chengxu3/B/server.py
----------Two-way identity authentication begins----------
接收一个客户端连接： ('192.168.1.103', 51931)
服务器端解密得第一个分量N1： 263
服务器产生第二分量为N2： 838
生成N1和N2合并向量:263838

服务器端解密得第二分量N2： 838
第二分量N2相同
Authentication success
```

图 14 Server 端对 Client 认证结果

```
yu@linux:~/桌面/chengxu3/A$ python3 client.py
----------Two-way identity authentication begins----------
客户端产生第一个分量为N1:263
解密得到合并分量N1_2: 263838
对比第一分量N1相同
Authentication success

返回第二分量： 838
```

图 15 Client 端对 Server 端认证结果

当某个非法 Client 端试图与 Server 端进行连接,即使它获得合法 Client 端的公钥但由于没有匹配的私钥进行解密, 所以无法进行假冒身份接入系统, 非法 Client 端试图与 Server 端连接结果如图 16 所示.

```
yu@linux:~/桌面/chengxu3/C$ python3 client1.py
----------Two-way identity authentication begins---------
客户端产生的随机数为309
connect error
```

图 16 非法 Client 端对 Server 端身份认证结果

(2) 数据加密和签名传输仿真

为了保证数据传输过程中的机密性和完整性, 我

们采用对称加密和数字签名结合的方式进行保证数据的传输安全. 使用文章的传输机制后攻击者就无法获知具体的内容同时也能够及时发现数据在传输过程中是否被篡改或者出现传输错误, 具体的报文加密和签名以 PMA 软件仿真得到的报文为例进行实验分析, 对召唤用户 2 级数据加密和签名的程序运行结果如图 17、图 18 所示.

图 17 数据发送端运行结果

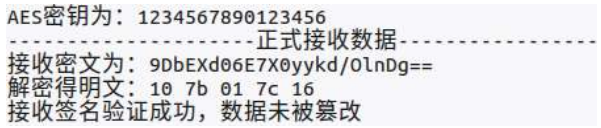

图 18 数据接收端运行结果

报文经过 AES 加密算法前后数据的对比如表 1 所示, AES 算法密钥设为 1234567890123456.

表 1 AES 加密前后数据的对比

明文数据	密文数据
10 7b 01 7c 16	9DbEXd06E7X0yykd/OlnDg==
10 5a 01 5b 16	0lw7xQML2EAmhM+0tQuWgw==
68 0e 0e 68 08 01 01	eVpH3eN6RLqPVPyZZkNXpAIB/WWHfPaN
81 01 01 f1 01 02 d8	DEk+v9h85RLBbMCky9olMAO+TpzzlyeWB
59 32 11 01 f6 16	U2tvxdorQOBICT1hSIByQ==

5 结论

文章首先对 103 规约进行了安全性分析, 分析其可能存在的安全威胁. 针对采用以太网 103 规约进行数据通信的 DTU 设备进行 ARP 攻击并成功. 如果实际情况中发生这种事件, 将给配电网自动化系统带来严重威胁. 针对中间人攻击, 本文设计了一个双向身份认证机制对设备的合法性进行辨认, 并使用对称加密手段和数字签名技术对通信数据进行机密性和完整性保护. 最后通过仿真实验验证了该方法的有效性.

参考文献

1 张嘉辉. 基于 IEC60870-5-103 规约的母线弧光保护的研究 [硕士学位论文]. 长沙: 湖南大学, 2017.
2 邓素碧, 赵振龙, 陈军, 等. 以太网 103 规约及其在水电厂自动化系统中应用. 电力自动化设备, 2007, 27(4): 79–82. [doi: 10.3969/j.issn.1006-6047.2007.04.020]
3 姬希娜, 浮明军, 杨生苹. 国家电网以太网 103 规约测试工具的设计与实现. 测控技术, 2016, 35(12): 114–117. [doi: 10.3969/j.issn.1000-8829.2016.12.027]
4 张磊, 陈宏君, 吴相楠, 等. 基于扩展 103 规约的保护装置通信与调试系统设计. 电力系统保护与控制, 2015, 43(21): 126–130.
5 李鹏, 范三龙. 基于 IEC 60870-5-103 规约扩展的牵引供电实时负荷录波设计与实现. 电气技术, 2015, (10): 117–119. [doi: 10.3969/j.issn.1673-3800.2015.10.027]
6 韦宇, 莫仕勋. 基于以太网 103 规约发电机主保护装置的监控系统实现. 电工技术, 2020, (13): 94–96, 100.
7 雷林绪, 覃剑, 刘靖. IEC60870-5-103 传输规约在行波故障测距装置中的应用. 电网技术, 2007, 31(S2): 252–255.
8 余梦泽, 田翠华, 陈柏超, 等. IEC60870-5-103 规约在 110 kV 可控电抗器控制装置中的应用. 继电器, 2008, 36(5): 63–66.
9 刘亮亮, 杨启, 沈泽明. 浅谈网络 103 规约在监控系统中应用优势及存在的问题. 中国电机工程学会电力系统自动化专业委员会 2012 年学术交流会论文集. 厦门, 中国. 2012. 1–5.
10 Sun ZW, Ma YN, Guo QR, *et al*. Security mechanism for distribution automation using EPON. 2009 IEEE International Conference on Network Infrastructure and Digital Content. Beijing, China. 2009. 581– 585.
11 马春波, 杜以聪, 曾坤. 基于 IBC 体制的挑战/应答式双向身份认证协议. 计算机工程与设计, 2017, 38(2): 345–349.
12 潘维, 黄晓芳. 基于智能合约的身份管理及认证模型. 计算机工程与设计, 2020, 41(4): 915–919.
13 周克元. 对一种改进的 ElGamal 数字签名方案的攻击与改进. 计算机应用与软件, 2019, 36(4): 323–325, 333. [doi: 10.3969/j.issn.1000-386x.2019.04.051]
14 邓真, 刘晓洁. HTTPS 协议中间人攻击的防御方法. 计算机工程与设计, 2019, 40(4): 901–905.
15 裴志江. 一种终端安全防护模型设计方法. 现代电子技术, 2020, 43(9): 75–78.
16 何文才, 李娜, 刘培鹤, 等. 一种 WSN 小数据分发安全方案的研究与设计. 计算机应用与软件, 2018, 35(2): 150–155. [doi: 10.3969/j.issn.1000-386x.2018.02.028]