2021 年 第 21 卷 第 31 期
2021, 21(31): 13374-07

科 学 技 术 与 工 程
Science Technology and Engineering

ISSN 1671—1815
CN 11—4688/T

引用格式:梁晓兵, 岑 炜, 付义伦, 等. 适用于电力物联网的安全接入认证装置设计[J]. 科学技术与工程, 2021, 21(31): 13374-13380.
Liang Xiaobing, Cen Wei, Fu Yilun, et al. Design of secure access authentication device applied to power internet of things[J]. Science Technology and Engineering, 2021, 21(31): 13374-13380.

适用于电力物联网的安全接入认证装置设计

梁晓兵[1], 岑 炜[1*], 付义伦[1], 翟 峰[1], 曹永峰[1], 孙晋凯[2]
(1. 中国电力科学研究院有限公司, 北京 100192; 2. 国网山西省电力公司营销服务中心, 太原 030000)

摘 要 针对电力物联网海量边缘侧设备接入可能导致的安全问题,首先分析了边缘设备安全接入需求;然后研究了融合协议过滤、协议适配、网络安全隔离、安全接入认证技术于一体的物联网边缘侧安全接入认证技术。基于上述技术,设计了包含外网处理单元、隔离交换单元、系统管理单元、密码运算单元和内网处理单元在内的电力物联网安全接入认证装置;最后选取某省充电桩运营系统作为试点应用场景,分别从安全性能和通信性能两方面进行测试分析。测试结果表明,该安全接入认证装置能够在基本不影响设备通信性能的前提下,实现电力物联网海量设备的安全接入认证,在面对不同类型边缘设备接入时仍具有良好的可靠性和泛化性,可有效降低核心业务系统被非法入侵的风险。

关键词 电力物联网; 边缘设备; 协议适配; 网络隔离; 接入认证
中图法分类号 TM933; **文献标志码** A

Design of Secure Access Authentication Device Applied to Power Internet of Things

LIANG Xiao-bing[1], CEN Wei[1*], FU Yi-lun[1], ZHAI Feng[1], CAO Yong-feng[1], SUN Jin-kai[2]
(1. China Electric Power Research Institute, Beijing 100192, China;
2. State Grid Shanxi Marketing Service Center, Taiyuan 030000, China)

[**Abstract**] For the security access problem of the massive edge devices in the power Internet of Things, the secure access authentication technology for edge devices in power Internet of Things was researched, which set such mechanisms as protocol filtering, protocol adaptation, network isolation, access authentication in an organic whole. Based on above technology, a secure access authentication device applied to the power Internet of Things was designed, which included external network processing unit, isolation exchange unit, system management unit, cipher operation unit and internal network processing unit. Then the pilot application and performance test analysis for the devices was carried out. The test results show that the secure access authentication device can realize the secure access authentication for massive devices in the power Internet of Things under the premise of basically not affecting the communication performance of the devices. It still has good reliability and generalization when facing the access of different types of edge devices, and can effectively reduce the risk of the core business system being illegally invaded.

[**Keywords**] power Internet of Things; edge device; protocol adaptation; network isolation; access authentication

随着移动互联、人工智能等新技术的发展,电力用户与智能电网的双向交互越来越频繁,用户对电网的服务形式和服务质量要求也越来越高。为了满足电力用户的应用需求,增强电力用户对智能电网的感知度和参与度,电力物联网随之产生[1]。电力物联网可以将电力用户与各类企业及设备灵活高效地连接起来,产生共享数据,为用户、电网、电力企业、供应商等提供统一接入及信息交互服务[2-4]。为提升电力物联网与用户的互动性,需要在电力物联网边缘侧接入充电桩、外部综合能源设备等海量安全不受控的非电网资产设备。这些设备分布较为广泛,通信方式较为多样,在很大程度上增加了电力物联网遭受伪造终端接入、木马、病毒、恶意代码等网络攻击的风险,使恶意人员更容易通过感知层入侵到整个电力网络并进行攻击破坏[5]。

针对电力物联网边缘侧海量不受控非电网资产设备安全接入问题,许多研究者在网络隔离、安

收稿日期: 2021-02-25; **修订日期**: 2021-07-30
基金项目: 国家电网公司科技资助项目(5700-202055171A-0-0-00)
第一作者: 梁晓兵(1978—),男,汉族,河南许昌人,博士,高级工程师。研究方向:信息安全技术。E-mail:liangxbg@163.com。
* **通信作者**: 岑 炜(1983—),女,汉族,河北张家口人,硕士,高级工程师。研究方向:电能计量及信息安全技术。E-mail:cenwei@epri.sgcc.com.cn。

全接入技术研究和隔离设备研制方面做了大量工作。文献[6-7]基于网络隔离和数据安全交换等技术构建了双网安全交互体系。文献[8]设计了物联网设备接入认证系统,对设备进行统一管理控制,使相关数据准确安全地传输到物联网系统应用层。文献[9]基于单向安全隔离与信息传输机制设计了安全隔离与单向导入系统,实现了代码在传输过程中的自动化访问控制和安全检查。文献[10]基于流量缓存管理、数据异或保密处理、数据帧载荷提取与重新封装等技术设计了新型网络隔离单向传输设备。文献[11]研制了集数据加解密、身份认证等功能为一体的电力专用纵向加密认证网关,以保证电力系统纵向边界及远程数据传输的安全性。

上述研究虽然在一定程度上实现了网络间的物理隔离与接入认证,增强了网络间信息交互的安全性。但是,其系统功能较为单一,接入设备体积和功耗较大,需要的计算资源相对较多,而且大多数电力终端的通信协议较为固定,上述接入认证技术及系统在协议过滤和协议适配方面考虑较少,不能满足低功耗、低成本、多分布需求的电力物联网边缘侧不受控设备信息安全交互需求。因此,亟需研究电力物联网边缘设备安全接入认证技术,研制集协议过滤、协议适配、网络隔离、接入认证于一体的电力物联网边缘接入认证装置,解决海量非电网资产设备安全接入难题。

1　边缘设备安全接入需求分析

电力物联网边缘侧是电力系统的关键用电业务处理环节,其网络环境开放复杂、访问控制灵活多变、接入的非电网资产设备种类繁多、数量巨大且安全性能参差不齐。这些设备在参与电网互动过程中将会产生大量数据,给终端信任管理、网络安全带来严峻挑战。

海量非电网资产设备大致可分为三类:内嵌安全芯片,计算能力较强且支持复杂密码算法的设备;无安全芯片,计算能力一般仅支持轻量级软密码算法的设备和不支持密码算法计算能力受限的设备三类。这三类设备主要通过 WIFI、LoRa、NB-IoT 等通信方式接入电力物联网,实现非电网资产设备用电数据的采集与信息交互。然而,WIFI 中常用的 WPA(Wi-Fi protected access)加密认证机制在密钥协商环节缺乏有效的认证机制,容易受到中间人攻击;LoRa 主要采用非授权频段的公开通信协议进行信息交互,容易受到伪造报文攻击;NB-IoT 具有连接设备众多,覆盖面积较大等特点,大规模暴露的通信网络使其面临的安全风险较多[12]。

由于海量非电网资产设备通信方式不一,安全防护强度参差不齐,很难在设备本身通信方式上保障电力物联网的接入安全。因此,需要研究海量电力物联网边缘侧设备安全接入认证技术,研制能够部署于电力物联网边界、实现协议过滤和转换的接入认证装置,在包过滤的基础上,采用密码技术实现非电网资产设备通信网络与电力物联网之间的网络隔离、协议过滤、协议适配、接入认证,保障电力物联网边界安全可靠。

2　边缘设备安全接入认证关键技术

基于第 1 节提出的问题,分别对协议过滤及适配、网络安全隔离和安全接入认证等关键技术进行研究,实现非电网资产设备通信网络与电力物联网的安全隔离、信息安全交互和传输数据的安全保护。

2.1　协议过滤及适配

协议过滤指基于特定的安全策略对应用层协议中传输的信息进行检测、解析,获取其关键数据,根据过滤条件,控制关键数据的转发。协议适配即在协议解析过滤基础上,将关键数据按照接收方要求的协议格式封装后转发[13]。

针对海量非电网资产设备通信方式不统一特征,主要采用字符串模式匹配和协议特征分析相结合的方式对非电网资产设备通信进行协议过滤和关键信息提取,从而实现与电力物联网设备的协议适配。

2.1.1　字符串模式匹配

字符串是由 $n(n \geqslant 0)$ 个字符组成的序列,它是数据元素的特殊线性表示。字符串的模式匹配是字符串最重要和最复杂的一个操作,也就是字符串的匹配查找。传统 BF(Brute-Force)算法在字符串模式匹配过程中存在重复回溯,匹配效率较低的问题。而 KMP(Knuth-Morris-Pratt)算法解决了 BF 算法在字符串模式匹配失败时出现的重复回溯问题,在面对大量字符串匹配时效率更高,因此本节采用 KMP 算法对非电网资产设备通信模式与电力物联网可接入的通信模式进行字符串匹配。

首先进行字符串模式的初始匹配,通过 next( ) 函数计算模式串的内部匹配信息。然后将目标字符串 S 的第 1 个字符和模式字符串 T 的第 1 个字符进行比对,若相等,则继续逐个比对后面的字符;若不相等,则定位到当前字符匹配失败的位置,并基于已匹配字符信息,修正 next( ) 函数指针,重新定位字符串指针到指定位置,从而有效避免重复回溯问题,实现字符串模式快速匹配[14]。

2.1.2 协议特征分析提取

协议特征是能够标识协议一个或者多个字符串的集合,协议的特征字段是协议的重要组成部分。每一种协议都包含很多类型的协议消息,由一个或者多个特征字段的组合来标识不同类型的协议消息。

协议分析主要包括协议数据帧的格式判断和信息交互模式确定,从而得到协议的数据结构、格式、信息交互双方信息内容顺序。通过协议分析可以推断出协议不同位置上字段所表达的含义。

主要基于字符串统计处理模型采用过滤和封装的技术实现协议的特征分析,即首先选取协议样本数据进行切片处理,然后进行字符串频率统计,在统计分析基础上进行字符串的排序、过滤和封装,从而提取协议关键特征信息。

2.1.3 设备协议过滤及适配过程

基于上节通信模式字符串匹配和协议特征分析方法,对非电网资产设备通信进行协议过滤和关键信息提取,从而实现与电力物联网设备的协议适配,具体协议过滤及适配流程如图 1 所示。

具体流程步骤如下。

(1)建立常用互联网设备通信协议规则集 $\{P_1, P_2, \cdots, P_n\}$。协议规则一般包括协议头 P_{Hi} ($i=1,2,\cdots,n$)和协议内容 P_{Ci} 两部分。其中,协议头包括起始字符、长度域、控制域、地址域和协议头校验码等数据信息[15-16]。协议内容包括传输数据和数据校验码信息[17]。

(2)对接收到的非电网资产设备信息 D_{re} 进行通信模式字符串匹配和特征分析,得到其协议头信息数据 P_{DH1}。将 P_{DH1} 与通信协议规则集中的协议头 P_{Hi} 进行比对和检查。

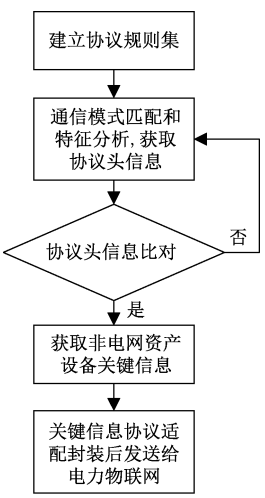


图 1 协议过滤及适配过程

Fig. 1 The process of protocol filtering and adaptation

(3)当 P_{DH1} 信息比对成功后,确定其协议规则,按照既定规则提取出协议内容 P_{DC1}。若该信息为明文数据,则 P_{DC1} 为非电网资产设备关键信息数据;若该信息为密文,则需要解密 P_{DC1} 得到明文关键信息 P'_{DC1}。

(4)分析接收方需要的协议规则,将非电网资产设备关键信息数据 P_{DC1}(或者 P'_{DC1})按照协议规则要求进行封装,得到数据 D'_{re} 之后按照相应的安全策略发送给电力物联网相关设备[18]。

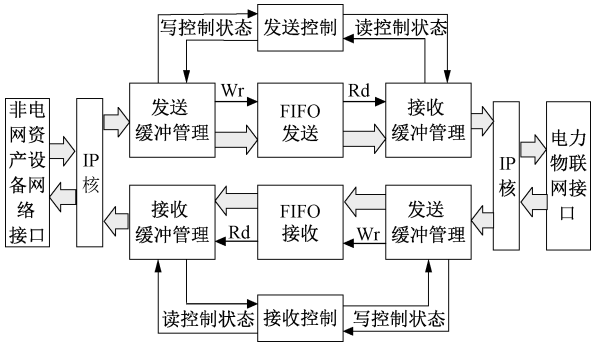
2.2 网络安全隔离

针对海量设备安全性能参差不齐,接入电力物联网后存在的安全隐患问题,本节主要采用网络双向单导通技术并基于现场可编程逻辑门阵列(field programmable gate array,FPGA)逻辑隔离电路实现非电网资产设备通信网络与电力物联网的安全隔离。

网络双向单导通技术是将内外网络间进行物理隔离,不可传输通信协议,所有交互数据需要经协议过滤后以纯数据的形式摆渡到网络的两端[19]。

基于 FPGA 逻辑隔离电路可实现接入设备与电力物联网之间的信息安全隔离交换。FPGA 逻辑隔离电路能够在网络的物理层将两端网络彻底断开,它具有两个独立的数据处理单元,每个单元对应连接一端网络[20-22],在同一时刻只能由一端网络进行数据读写,从而实现数据的安全摆渡[23]。基于 FPGA逻辑隔离电路的网络安全隔离原理如图 2 所示。

当非电网资产设备需要发送数据到电力物联网端时,FPGA 逻辑隔离电路首先将待发送数据存入缓冲区并发出发送隔离控制信号,使其与电力物联网端的网络断开。数据写到先入先出队列(first input first output,FIFO)发送模块中,这时 FIFO 接收模块处于关闭状态。当数据写完后,释放发送隔离



Wr 为数据发送信息;Rd 为数据接收信息

图 2 网络安全隔离原理

Fig. 2 The principle of network security isolation

控制信号,FPGA 逻辑隔离电路与电力物联网连通,非电网资产设备与 FPGA 逻辑隔离电路断开,FIFO 发送模块的数据经由缓冲区发送到电力物联网端。反之,当非电网资产设备需要接收电力物联网发送的数据时,开启 FIFO 接收模块,关闭 FIFO 发送模块[24]。

2.3　安全接入认证

针对海量非电网资产设备身份鉴别、安全接入问题,基于设备指纹技术,通过构建设备准入白名单的方式实现海量非电网资产设备的安全接入认证,具体流程如图 3 所示。

(1)非电网资产设备将其 MAC、IP、通信协议 P_r、有效数据 D_v、数据格式 D_f 等信息发送给电力物联网接入侧,电力物联网接入侧根据安全策略分析其合法性和有效性,如果安全合法,根据设备类型及业务需求选择相应的密码算法进行设备信息加密处理生成形成"设备指纹" D_{fp}:对于内存容量小、CPU 性能低且不含安全芯片的非电网资产设备,可采用 SM4 对称密码算法进行设备信息加密处理;对于内存容量小、CPU 性能低且包含安全芯片的非电网资产设备,采用 SM1 对称密码算法进行设备信息加密处理;对于内存容量大、CPU 性能高且包含安全芯片的非电网资产设备,采用 SM9 标识密码算法进行设备信息加密处理。

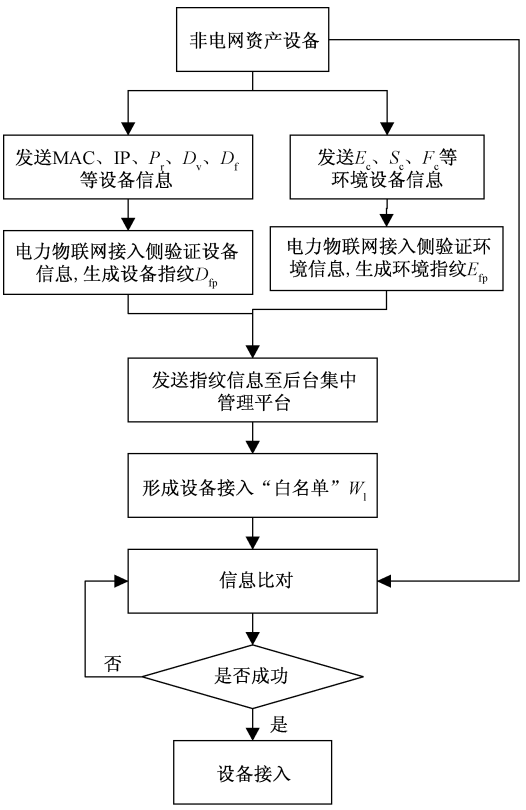


图 3　接入认证流程

Fig. 3　The access authentication process

(2)非电网资产设备将能耗变化 E_c、信号强度变化 S_c、流量变化 F_c 等环境参数信息,发送给电力物联网接入侧,电力物联网接入侧同样根据安全策略分析运算后形成"运行环境指纹" E_{fp}。

(3)电力物联网接入侧将采集到的指纹信息传输至后台集中管理平台中,形成设备准入"白名单" W_1。

(4)当设备再次接入电力物联网时,电力物联网接入侧将再次采集接入设备指纹信息,并通过集中管理平台进行指纹信息的遍历和比对,最终确认接入设备的身份信息,比对相同则准予接入,反之则接入认证失败。

3　安全接入认证装置设计

针对海量非电网资产设备安全接入问题,融合上述协议过滤及适配、网络安全隔离和安全接入认证等技术,设计了适用于电力物联网边界安全防护的接入认证装置。

接入认证装置由外网处理单元、隔离交换单元、系统管理单元、密码运算单元和内网处理单元共五部分组成,其逻辑架构如图 4 所示。

外网处理单元分别由外网数据收发单元、身份识别单元、访问控制单元、协议检测单元和升级管理单元组成。其中,外网数据收发单元主要负责接收或发送外网设备的数据报文;身份识别单元主要负责对外网非可控设备进行身份鉴别;访问控制单元主要依据访问控制策略对外网设备进行接入控制;协议检测单元主要负责对外网设备发送的报文进行格式检测,查看其是否符合电力

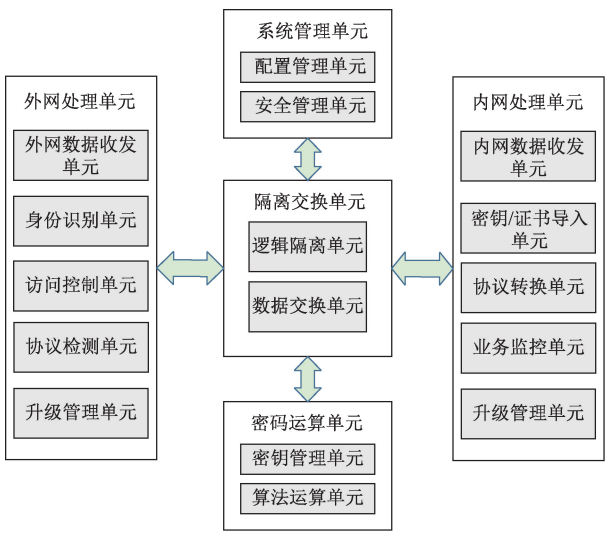


图 4　安全接入认证装置逻辑架构

Fig. 4　The logical architecture of secure access authentication device

通信网络信息交互要求;升级管理单元主要负责对外网处理单元的软件进行升级维护。

隔离交换单元由逻辑隔离单元和数据交换单元组成,负责进行协议格式检查、过滤和适配转换,将非电网资产设备通信协议转换为电力物联网专用协议实现内外网业务单元之间的信息交互[25]。

系统管理单元包括配置管理单元和安全管理单元,配置管理单元负责用户管理、密码运算单元初始化等;安全管理单元负责监控和维护其他各功能单元的安全可靠运行。

密码运算单元包括密钥管理单元和算法运算单元。密钥管理单元负责密钥全生命周期的安全管理;算法运算单元负责国密 SM1、SM2、SM3、SM4、SM7 和 SM9 等密码算法的运算。

内网处理单元分别由内网数据收发单元、密钥/证书导入单元、协议转换单元、业务监控单元和升级管理单元组成。其中,内网数据收发单元主要负责接收或发送内部通信网络数据报文;密钥/证书导入单元主要负责与电力统一密码基础设施对接,实现装置自身密钥的分发和数字证书的申请及下发;协议转换单元主要负责将外网设备的不同通信协议转换为电力网络统一的通信协议进行信息交互;业务监控单元负责监测内网处理单元内各个单元的工作状态,并守护各单元的进程运行,当部分单元出现异常运行状态时,及时处理异常事件并维护其持续服务功能;升级管理单元主要负责对内网处理单元的软件进行升级维护。

4 安全接入认证装置性能分析

选取某省电力公司充电桩运营系统,作为电力物联网边缘设备安全接入装置的试点应用场景,并验证分析安全接入装置的各项性能。试点应用系统逻辑架构如图 5 所示。

在试点应用系统中,主要采用分级接入认证机制实现非电网资产设备的接入认证和关键数据安全传输,即将本文研制的接入认证装置部署于电力物联网边界处,实现对充电桩信息的协议过滤、协议适配、网络隔离、数据摆渡和接入认证,经过转换和过滤后的关键信息,通过电力系统内部的终端表计发送给后台主站[26]。

为了验证本文设计的安全接入认证装置在电力物联网接入边缘设备时的应用效果,下面分别从安全性和通信性能两方面进行安全接入认证装置的性能分析。

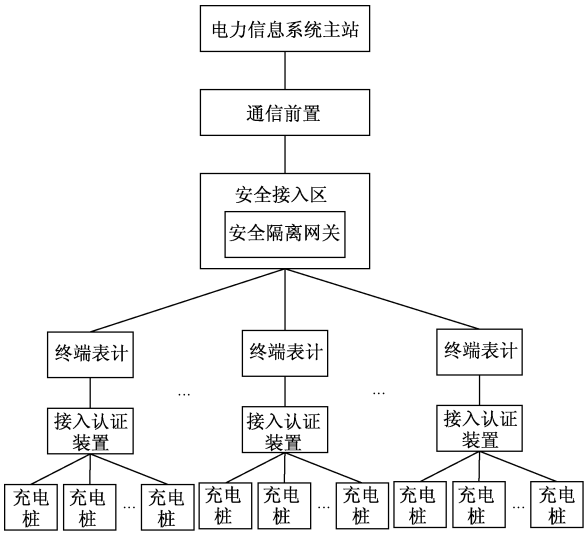


图 5 安全接入认证装置试点应用系统

Fig. 5 The pilot application system of access authentication device

4.1 安全性能分析

针对接入认证装置的安全性,主要采用端口扫描、拒绝服务攻击、漏洞攻击、仿冒攻击等攻击方式对接入认证装置应用系统进行网络攻击测试及性能分析。防攻击性能分析结果如表 1 所示。

表 1 防攻击性能分析

Table 1 The test result of anti-attack performance

攻击类型	传统隔离装置	接入认证装置
端口扫描攻击	无法避免内网信息被非法获取	内网信息对于攻击者不可见
拒绝服务攻击	网络通信性能受限	物理隔离,通信性能和处理能力不受限
漏洞扫描攻击	系统业务功能受限	系统业务不受限
仿冒攻击	接入设备易被仿冒	通过指纹校验机制实现设备的安全接入认证

在对装置进行端口扫描攻击测试时,传统隔离装置缺乏有效的抵御认证绕过、口令爆破等安全机制,系统信息无法避免被非法获取;而本文设计的接入认证装置具备协议检测、协议过滤和协议转换机制,由于内外网间协议格式不一致,网外设备很难获取电力信息系统内网数据。

在对装置进行拒绝服务攻击测试时,传统隔离装置主要通过过滤 IP 地址,限制 SYN/ICMP 流量,检查数据来源等方式抵御拒绝服务攻击,系统网络通信性能将受到一定影响;本文设计的接入认证装置主要通过硬件模块进行协议过滤,使每个攻击被限制在独立 Socket 中,限制来源地址,响应和服务,在物理隔离情况下,网络的性能和处理能力不被攻击影响。

在对装置进行漏洞扫描攻击测试时,传统隔离装置主要通过关闭一定数量的服务进程,检查漏洞来抵御漏洞扫描攻击,系统的通信性能和任务处理能力将受到一定影响;本文设计的接入认证装置主要通过数据摆渡机制抵御漏洞扫描攻击,攻击者的攻击脚本或程序将在摆渡过程中被丢弃或变为静态数据而无法执行,攻击者无法侵入系统网络,系统防御性能相对更强,且系统业务不被影响。

在对装置进行仿冒攻击测试时,传统隔离装置未校验设备指纹或运行状态信息,接入设备易被仿冒;本文设计的接入认证装置基于设备指纹与运行环境指纹信息建立感知设备准入白名单,通过设备指纹校验机制实现感知设备的接入认证,可以有效抵御仿冒攻击。

由表 1 分析结果可以看出,本文设计的安全接入认证装置在抵御端口扫描、拒绝服务攻击、漏洞攻击、仿冒攻击等攻击时,具备一定的技术优势,可以满足电力物联网安全应用需求。

4.2　通信性能分析

为了验证安全接入认证装置的通信性能,在试点应用系统中,增加了安全接入认证装置的系统数据(约 1 024 字节)明文转发延时、密文转发延时和会话密钥协商时间等通信性能测试项,并与未接入认证装置的原信息系统通信性能进行对比,测试结果如图 6 所示。

由测试结果可以看出,加上接入认证装置的测试系统的明文转发延时较原信息系统相差约 0.12 ms,密文转发延时相差约 0.75 ms,密钥协商时间相差约 71.3 ms,该通信延时在电力物联网通信指标范围内[27]。因此,本文研制的接入认证装置可以在不影响设备正常信息交互基础上,有效缓解电力物联网边界的安全性能压力,能够满足海量电力物联网设备信息安全交互需求。

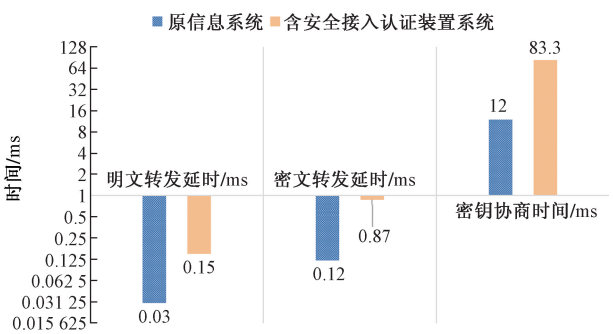


图 6　通信性能测试结果

Fig. 6　The test result of security communication performance

5　结论

为了应对电力物联网海量边缘设备安全接入问题,增强电力物联网信息交互的安全性。本文分析了电力物联网面临的安全风险及接入认证需求,研究了基于通信模式匹配、协议特征分析机制的设备协议过滤和协议适配技术,通信网络双向单导通和数据摆渡技术及设备指纹提取和白名单访问控制技术,设计了适用于电力物联网边缘侧的接入认证装置,实现了海量设备的安全接入认证。目前该装置已在某省电力公司充电桩运营系统中试点应用,应用结果表明,该安全接入认证技术及装置能够在基本不影响系统通信性能的前提下,实现海量电力物联网非电网资产设备的安全接入认证,有效降低核心业务系统被非法入侵的风险。后期,项目组将根据试点应用情况不断完善装置的性能和功能,并推广应用于其他信息系统。

参　考　文　献

[1] 王　琼. 基于物联网的电力设备信息管理研究与实现[D]. 北京: 华北电力大学, 2013.
Wang Qiong. Research and implementation of power equipment information management based on Internet of Things[D]. Beijing: North China Electric Power University, 2013.

[2] 时　下. 国家电网 2024 年建成泛在电力物联网[J]. 电力系统装备, 2019, 7: 28-29.
Shi Xia. The state grid will finished building the power of the Internet of Things in 2024[J]. Power System Equipment, 2019, 7: 28-29.

[3] 闵家新, 郎小毅, 李　洋, 等. 基于泛在物联网的继电保护设备智能运维技术[J]. 科学技术与工程, 2021, 21(3): 1024-1029.
Min Jiaxin, Lang Xiaoyi, Li Yang, et al. Intelligent operation and maintenance technology of relay protection equipment based on ubiquitous Internet of Things[J]. Science Technology and Engineering, 2021, 21(3): 1024-1029.

[4] 王　娟. "互联网 +"背景下 ZK 供电公司电力服务营销策略研究[D]. 郑州: 郑州大学, 2019.
Wang Juan. Research on the power service marketing strategy of ZK power supply company under the background of "Internet +"[D]. Zhengzhou: Zheng Zhou University, 2019.

[5] 王志良, 石志国. 物联网工程导论[M]. 西安: 西安电子科技大学出版社, 2011: 56-57.
Wang Zhiliang, Shi Zhiguo. Engineering introduction of the Internet of Things[M]. Xi'an: Xidian University Press, 2011: 56-57.

[6] 王　静, 高昆仑, 张　波. 基于网络隔离与安全数据交换的发电集团双网体系研究与设计[J]. 电信科学, 2017, 43(1): 163-172.
Wang Jing, Gao Kunlun, Zhang Bo. Research and design in dual network scheme of power corporation based on network isolation and secure data exchange[J]. Telecommunications Science, 2017, 43(1): 163-172.

[7] 骆慧勇. 基于云桌面实现网络安全隔离的应用[J]. 计算机应用与软件, 2020, 37(2): 15-17.

Luo Huiyong. Application of network security isolation based on cloud desktop[J]. Computer Applications and Software, 2020, 37(2): 15-17.

[8] 樊柯辛. 物联网设备接入系统的设计与实现[D]. 沈阳: 中国科学院大学, 2019.
Fan Kexin. Design and implementation of Internet of Things device access system[D]. Shenyang: University of Chinese Academy of Sciences, 2019.

[9] 巴连杰, 林 楠, 黄华伟, 等. 安全隔离与单向导入系统在NC代码传输中的应用[J]. 通信技术, 2019, 52(9): 2260-2266.
Ba Lianjie, Lin Nan, Huang Huawei, et al. Application of secure isolation and one-way import system in NC code transmission[J]. Communications Technology, 2019, 52(9): 2260-2266.

[10] 程 军. 一种新型网络隔离单向传输设备的设计与实现[J]. 通信技术, 2017, 50(10): 2385-2389.
Cheng Jun. Design and implementation of novel network-isolation and unidirectional transmission equipment[J]. Communications Technology, 2017, 50(10): 2385-2389.

[11] 侯立铭. 专用网络安全隔离系统的深度数据包过滤及数据审计关键技术研究[D]. 长沙: 国防科学技术大学, 2007.
Hou Liming. Research on key technologies of deep packet filtering and data audit for private Network security isolation system[D]. Changsha: National University of Defense Technology, 2007.

[12] 胡如会, 张起荣, 贺道德. 基于双线性映射直接匿名认证方案的改进[J]. 科学技术与工程, 2018, 18(3): 264-267.
Hu Ruhui, Zhang Qirong, He Daode. Improvement of direct anonymous attestation protocol based on bilinear maps[J]. Science Technology and Engineering, 2018, 18(3): 264-267.

[13] 刘以胜. 基于应用过滤技术的协议单向网闸系统研究[D]. 南京: 南京邮电大学, 2017.
Liu Yisheng. Research on the one-way net gap based on application filtering technology[D]. Nanjing: Nanjing University of Posts and Telecommunications, 2017.

[14] 朱承学, 李锡辉. 数据结构: C/C++描述[M]. 北京: 中国电力出版社, 2007: 78-79.
Zhu Chengxue, Li Xihui. Data structure: C/C++ description[M]. Beijing: China Electric Power Press, 2007: 78-79.

[15] 孙 芬. 基于嵌入式操作系统的载波抄表技术的应用研究[D]. 北京: 华北电力大学, 2014.
Sun Feng. Application research of carrier meter reading technology based on embedded operating system[D]. Beijing: North China Electric Power University, 2014.

[16] 卜 权. 基于Cortex-M3的自动抄表系统设计与实现[D]. 南京: 南京航空航天大学, 2011.
Bu Quan. Design and implementation of automatic meter reading system based on Cortex-M3[D]. Nanjing: Nanjing University of Aeronautics and Astronautics, 2011.

[17] 国家能源局. 电能信息采集与管理系统 第4-5部分 通信协议——面向对象的数据交换协议: DL/T 698.45—2017[S]. 北京: 中国电力出版社, 2017.
National Energy Administration. Data acquisition and management system for electrical energy Part 4-5: communication protocol - object oriented data exchange protocol: DL/T 698.45—2017[S]. Beijing: China Electric Power Press, 2017.

[18] 许钦百, 王彩芬. 基于密码学理论的私密信息安全风险评估方法[J]. 科学技术与工程, 2019, 19(7): 172-176.
Xu Qinbai, Wang Caifen. Privacy information security risk assessment method based on cryptography theory[J]. Science Technology and Engineering, 2019, 19(7): 172-176.

[19] 佟恒文. 基于Windows2000的网络安全技术研究[D]. 哈尔滨: 哈尔滨工业大学, 2005.
Tong Hengwen. Research on the network security technology based on Windows 2000 [D]. Harbin: Harbin Institute of Technology, 2005.

[20] 贺文华, 陈志刚. 网络安全隔离GAP技术研究[J]. 科学技术与工程, 2007, 7(15): 3774-3779.
He Wenhua, Chen Zhigang. Investigation of GAP technology in network security[J]. Science Technology and Engineering, 2007, 7(15): 3774-3779.

[21] 许艳光. 基于单向隔离网闸的数据过滤系统研究与实现[D]. 廊坊: 北华航天工业学院, 2015.
Xu Yanguang. Research and implementation of data filtering system based on one-way isolation gate[D]. Langfang: North China Institute of Aerospace Technology, 2015.

[22] 于建武, 李 征. 隔离的数据交换安全框架及其电子政务应用[J]. 科学技术与工程, 2008, 8(17): 5021-5023.
Yu Jianwu, Li Zheng. The security framework of isolated data exchange and its e-government applications[J]. Science Technology and Engineering, 2008, 8(17): 5021-5023.

[23] 贾书娟, 耿登田. 多路由协议路由管理技术研究与实现[J]. 计算机与网络, 2006, 7: 40-41.
Jia Shujuan, Geng Dengtian. Research and implementation of routing management technology for multi-routing protocol[J]. Computer and Intemet, 2006, 7: 40-41.

[24] 顾文博. SoPC总线协议跨芯片扩展的设计与实现[D]. 南京: 东南大学, 2015.
Gu Wenbo. Design and implementation of SoPC bus protocol cross-chip extension[D]. Nanjing: Southeast University, 2015.

[25] 黄中伟. 计算机网络管理与安全技术[M]. 北京: 人民邮电出版社, 2006: 28-32.
Huang Zhongwei. Computer network management and security technology[M]. Beijing: Posts and Telecom Press, 2006: 28-32.

[26] 杜 晔, 梁 颖. 网络信息对抗[M]. 北京: 北京邮电大学出版社, 2011: 128-129.
Du Ye, Liang Ying. Network information confrontation[M]. Beijing: Beijing University of Posts and Telecommunications Press, 2011: 128-129.

[27] 中国国家标准化管理委员会. 信息技术 安全技术 信息技术安全性评估准则 第2部分: 安全功能要求: GB/T 18336.2—2008[S]. 北京: 中国标准出版社, 2018.
Standardization Administration of China. Information technology security techniques evaluation criteria for IT security part 2 security functional requirements: GB/T 18336.2—2008[S]. Beijing: Standards Press of China, 2018.