DOI:10.12379/j.issn.2096-1057.2024.01.11

电力物联网零信任架构下的分布式认证模型

唐大圆　曹　翔　林　青　胡绍谦　汤震宇
（南京南瑞继保电气有限公司　南京　211102）
（tangdy@nrec.com）

Distributed Authentication Model Under Power IoT Zero Trust Architecture

Tang Dayuan, Cao Xiang, Lin Qing, Hu Shaoqian, and Tang Zhenyu
(*NR Electric Co., Ltd., Nanjing* 211102)

Abstract　Addressing the new network security challenges brought to the power system by the changing trend of a large number of distributed heterogeneous terminals such as unlimited public network access, new power interactive services, and new information technology application in the power system. This paper proposes a distributed authentication model based on the zero trust security architecture, giving full play to the advantages of zero trust security concept and technology under the overall security architecture of the power Internet of Things (IoT). The model integrates the trusted root of trust technology provided by the trusted computing module of the power terminal hardware. It also expands and extends the active security protection capabilities of power intelligent terminals and accesses networks to meet new cybersecurity challenges faced by intelligent grids. The distributed authentication model proposed in this paper sinks the dynamic trust evaluation and southbound terminal authentication module in the zero trust security architecture to the edge intelligent device, and subdivides and expands the trust and access control based on the trusted root provided by the terminal trusted module, and gives full play to the specific advantages of zero trust security concept and technology in terminal security access, security monitoring, and fine-grained business protection on the basis of compatibility with the existing power IoT authentication model, so as to improve the overall network security protection capability of the power IoT system.

Key words　power IoT; zero trust; trust computing; distributed authentication; SDP

摘　要　针对智能电网大量分布式异构终端无限公网接入、新型电力交互业务、新信息技术应用在电力系统等行业发展趋势给电力系统带来的新型网络安全挑战，基于零信任安全架构，提出一种分布式认证模型，在电力物联网整体安全架构下，充分发挥零信任安全理念和技术的优势，结合电力终端硬件可信计算模块提供的可信信任根技术，拓展和延伸电力智能终端和接入网络的主动安全防护能力，以应对智能电网所面临的新型网络安全挑战.该模型将零信任安全架构中的动态信任评估

收稿日期：2023-05-17
基金项目：国家重点研发计划项目(2021YFB2401002)
引用格式：唐大圆，曹翔，林青，等. 电力物联网零信任架构下的分布式认证模型[J]. 信息安全研究，2024，10(1)：67-74

信息安全研究 Journal of Information Security Research 第10卷 第1期 2024年1月 Vol.10 No.1 Jan. 2024

和南向终端认证模块下沉到边缘智能设备，以终端可信模块提供的信任根为基础，进行信任和访问控制的细分及扩展，在兼容现有电力物联网认证模型基础上，充分发挥零信任安全理念和技术在终端安全接入、安全监控、业务细粒度防护方面的具体优势，提升电力物联网系统整体网络安全防护能力.

关键词 电力物联网；零信任；可信计算；分布式认证；软件定义边界

中图法分类号 TP309.1

近年来，随着经济社会发展对新型电力业务的需求，电网越来越智能化.智能电网的建设适应了发电多样化、用电多元化的服务需求，同时电力业务走向开放也给电力系统的网络安全防护提出了新的挑战.当前电力系统的网络安全防护秉承“安全分区、网络专用、横向隔离、纵向认证”的总方针，以“纵向防御＋边界防御”为主的安全防御体系，在配用电力终端和边缘侧电力设备安全防护上难以全面覆盖.一方面，“大云物移智链边”新技术促进了智能电网与物联网、互联网的深度融合，也在一定程度上模糊了网络边界；另一方面，分布式新能源业务的发展，海量异构智能化终端的接入，增加了终端信息泄露、非法接入、失陷控制的风险.

相较于硬件芯片身份的物联终端安全接入模型，本文零信任认证模型采用软件数字身份和持续监测的方式实现终端接入认证，降低了对终端设备的侵入改造.相对于外置加密认证装置方案，内置于终端设备的认证模型能基于访问控制防御来自开放网络的攻击行为，提升设备内生安全能力.

本文提出的电力物联网零信任架构下的分布式认证模型，采用零信任安全理念和安全技术，对认证模型进行动态扩展，屏蔽了异构终端在接入能力上的差异，形成向上统一、向下兼容的分布式认证模型.无论边缘设备还是异构物联终端均可实现安全接入和持续信任监测，将网络安全防护框架延伸到边缘侧和感知层设备，提升了电力物联网整体安全防护能力.

1 相关研究

随着电力物联网面临的网络安全威胁越来越广泛、越来越严峻，国内外针对电力物联网面临的新型网络安全挑战的研究也逐渐增多.近些年新能源业务快速发展，越来越多新能源企业和用户的智能电力终端通过无线公共网络接入电力系统，使得原先相对清晰的电力系统网络边界逐渐模糊，电力系统的网络安全防护也从主站、子站机房延伸到用户侧终端设备.为应对电力系统边界逐渐模糊的问题，文献[1-2]提出了一种基于零信任的安全防护框架，通过零信任安全思想和安全技术重新定义网络安全防护边界.此外，智能终端设备通过无线公网接入必然导致这些终端直接面临来自于开发网络的攻击威胁，相对于传统电力专网，这些威胁呈爆发式增长，部分智能终端遭受网络攻击失陷而被控制的情况已无法避免，为降低因终端失陷导致的大面积电力系统异常风险，文献[3]提出了一种电力物联网场景下对抗失陷终端威胁的边缘信任模型，采用零信任引擎的分布式部署和基于区块链的信任评估模型，以达到对失陷终端威胁的抑制效果.文献[4-6]分别探讨了物联网终端设备身份识别和认证方法，在众多异构物联网终端设备中，基于终端设备软硬件特点，建立终端设备的认证模型，以达到安全与业务、功能与性能的平衡.文献[7-9]介绍了零信任安全架构下终端设备的动态信任评估模型，通过持续信任评估发现电力终端设备运行状态下的网络安全风险.

2 零信任身份认证机制

零信任架构(zero trust architecture，ZTA)建立在传统网络边界信任体系逐渐失效的背景下，提倡打破单一网络边界的概念，对用户、设备和应用进行全面、动态的访问控制.通过身份识别与访问管理(identity and access management，IAM)构建统一的权限管理平台，通过定义并管理设备或用户的唯一身份，确保合适的身份在合适的时间获得合适的访问权限；使用软件定义边界(soft-

ware define perimeter，SDP)架构重构业务安全访问边界，基于5层安全访问控制(单包认证、双向传输层安全、设备认证、动态防火墙、应用绑定)，提供多层次细粒度的网络安全边界防护能力.

电力物联网应用场景下，大量分布式异构终端通过无线公共网络接入电网，这些设备没有统一的身份标识，也不具备唯一的生物特征，很难建立统一的身份管理平台和实现设备间的身份认证.

当前，电力物联网中设备和终端安全接入通常是采用导入或内置数字证书的方式为设备提供统一的身份，进而实现安全接入时的身份认证和通信加解密.然而这些数字身份证书无法覆盖所有的感知层设备，同时基于数字证书的身份认证只能解决终端设备接入时的设备身份可信问题，对于业务逻辑漏洞、设备安全状态、业务隔离等安全问题没有很好的解决方案.因此本文基于零信任安全架构，结合电力物联网“云管边端”安全分层防护特点和可信计算技术，提出采用灵活的分布式认证架构，将电力物联网场景下的设备身份认证进行分层设计，既能集中管理又易于扩展.

3 分布式认证模型

为解决电力物联网场景下边缘设备和感知终端的身份认证问题，基于电力物联网使用数字证书进行身份认证的基本要求，本文提出一种分布式认证架构，将身份认证进行时间上的动态扩展和设备类型上的横向扩展，形成包括3个层次的分布式认证架构，如图1所示：

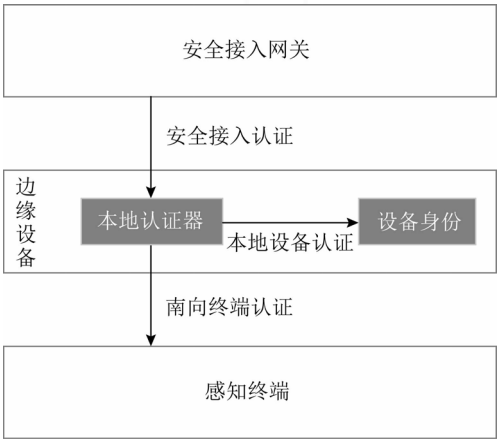

图1 分布式认证分层架构

在图1所示的分布式认证方案中，将电力物联网场景下对边缘设备和终端设备的接入认证功能拆分成由3层认证组合的分布式认证架构，包括安全接入认证、本地设备认证、南向终端认证.其中安全接入认证沿用电力物联网数字证书方式进行身份认证，由安全接入区的接入网关认证边缘代理的本地认证器，本地设备认证是边缘设备上身份认证的动态扩展，由本地认证器持续认证边缘代理设备，物联终端认证是边缘设备上对南向终端的认证类型扩展，由本地认证器认证南向感知终端设备.电力物联网采用“云管边端”业务接入和安全防护架构，“云”是指物联管理平台及上层应用；“管”指网络接入，对应安全接入区；“边”是指边缘物联代理设备；“端”则是指感知层传感设备.本文的分布式认证架构则对应其中的网络防护和终端防护，如图2所示.

3.1 安全接入认证

安全接入认证是由安全接入区的零信任控制器对边缘设备中的本地认证器进行认证，边缘设备中的本地认证器应具备零信任控制器可识别、可信赖的身份信息，通常是由公钥基础设施(public key infrastructure，PKI)颁发的数字证书身份信息，数字证书的颁发过程不在本文所讨论范围内.本地认证器的安全接入认证过程基于零信任SPA单包认证流程，如图3所示.

边缘设备在发起安全接入认证之前，先由本地认证器完成设备本地认证，本地设备认证通过后，通知SPA客户端模块发起SPA认证流程：

1) 本地认证器将接入认证请求发送给SPA客户端，携带LaID，LaTr，其中LaID是本地认证器的身份标识(数字证书)，LaTr是本地设备认证时的信任列表；

2) SPA客户端通过UDP协议将认证请求发送给零信任控制器，携带Enc((LaID，LaTr)，Pub_ctrl)，LaSign，其中Enc((LaID，LaTr)，Pub_ctrl)是使用控制器的公钥Pub_ctrl对(LaID，LaTr)进行加密后的信息，LaSign是本地认证器证书私钥对Enc((LaID，LaTr)，Pub_ctrl)的签名；

3) 零信任控制器接收到SPA认证请求消息后，使用私钥进行解密，获得LaID，使用LaID对应的公钥Pub_Laid对LaSign进行签名验证；

4) 零信任控制器SPA请求认证成功后，通知

信息安全研究 Journal of Information Security Research 第10卷 第1期 2024年1月 Vol.10 No.1 Jan. 2024

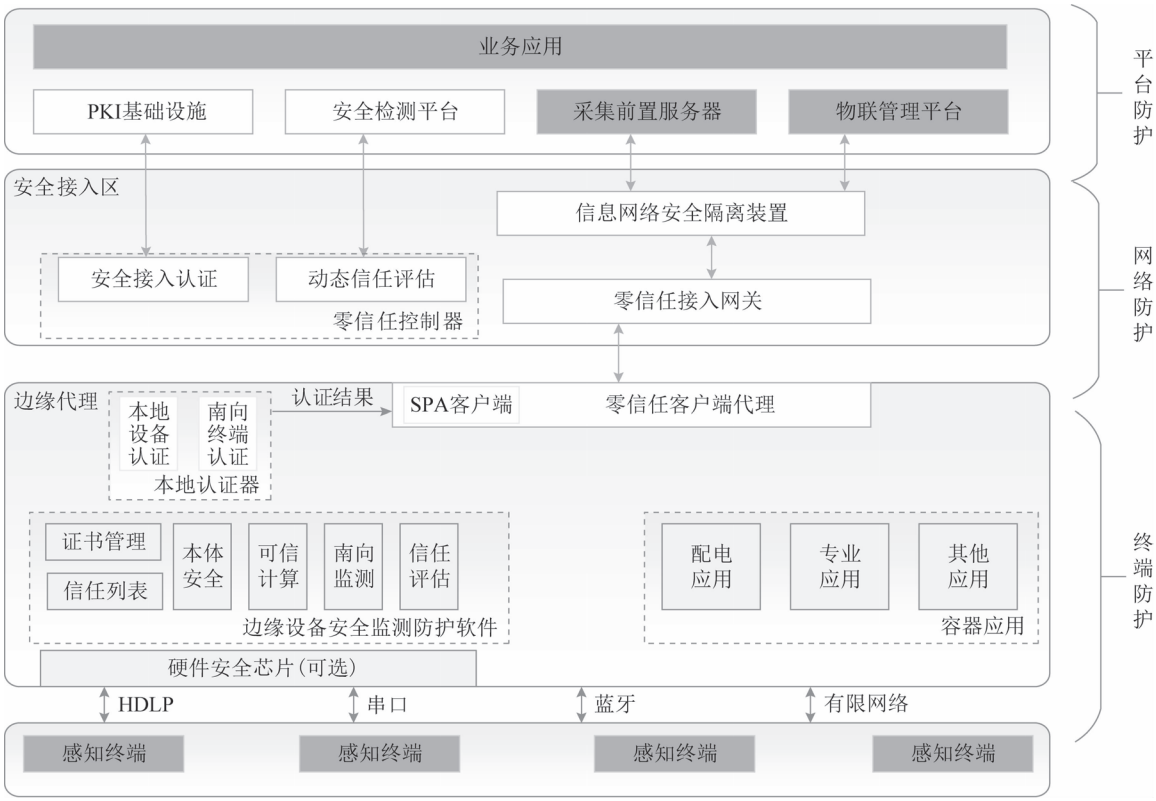

图 2　电力物联网终端接入认证架构

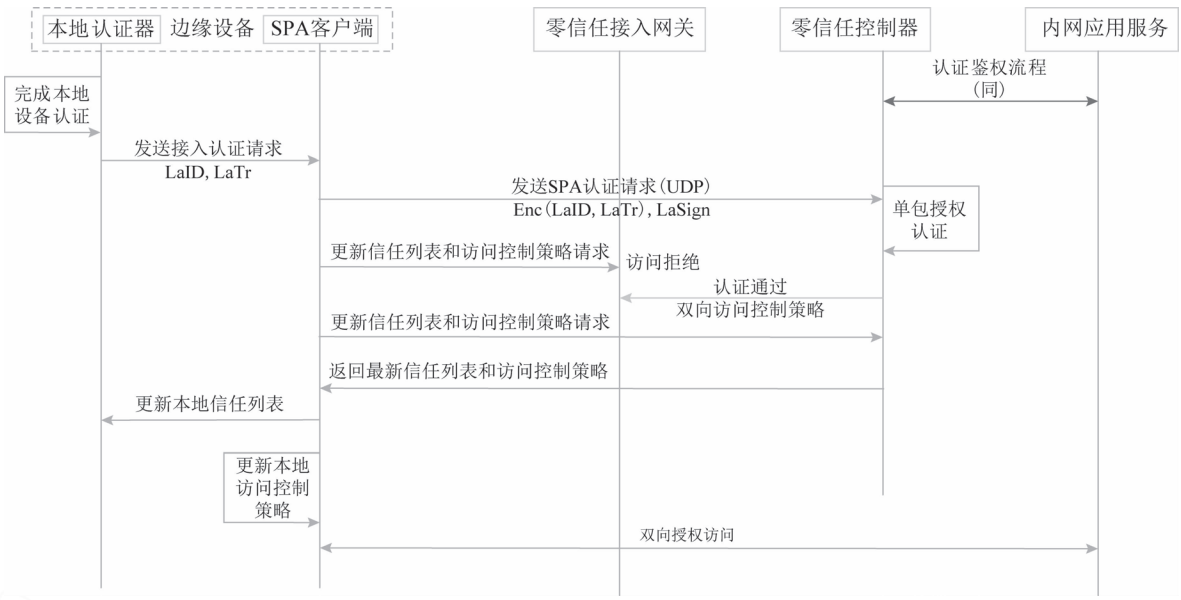

图 3　安全接入认证流程

零信任接入网关开放零信任控制器的策略更新访问端口 Port_pu；

5）SPA 客户端尝试访问零信任控制器策略更新端口 Port_pu；

6）零信任控制器接收到策略更新请求后返回最新访问控制策略和信任列表；

7）SPA 客户端向本地认证器更新信任列表，用于边缘设备本地身份的认证.

3.2 本地设备认证

本地设备认证是指本地认证器对边缘智能终端设备进行身份认证.边缘智能终端设备的身份信息不是永恒不变的,随着地理位置、网络环境、信任等级、设备硬件替换、设备归属等众多自身或外界因素发生变化而发生变化.

电力边缘智能终端北向通过无线专网或公共网络接入调度网络或其他电力业务聚合商,南向通过本地网络管理感知层终端设备,其设备本身直接面临来自公共网络的安全威胁,而缺少专业网络安全边界设备的防护,是电力物联网安全防护中的薄弱点和重要环节.通过对智能终端设备进行威胁建模分析,发现其存在的安全风险,如图 4 所示:

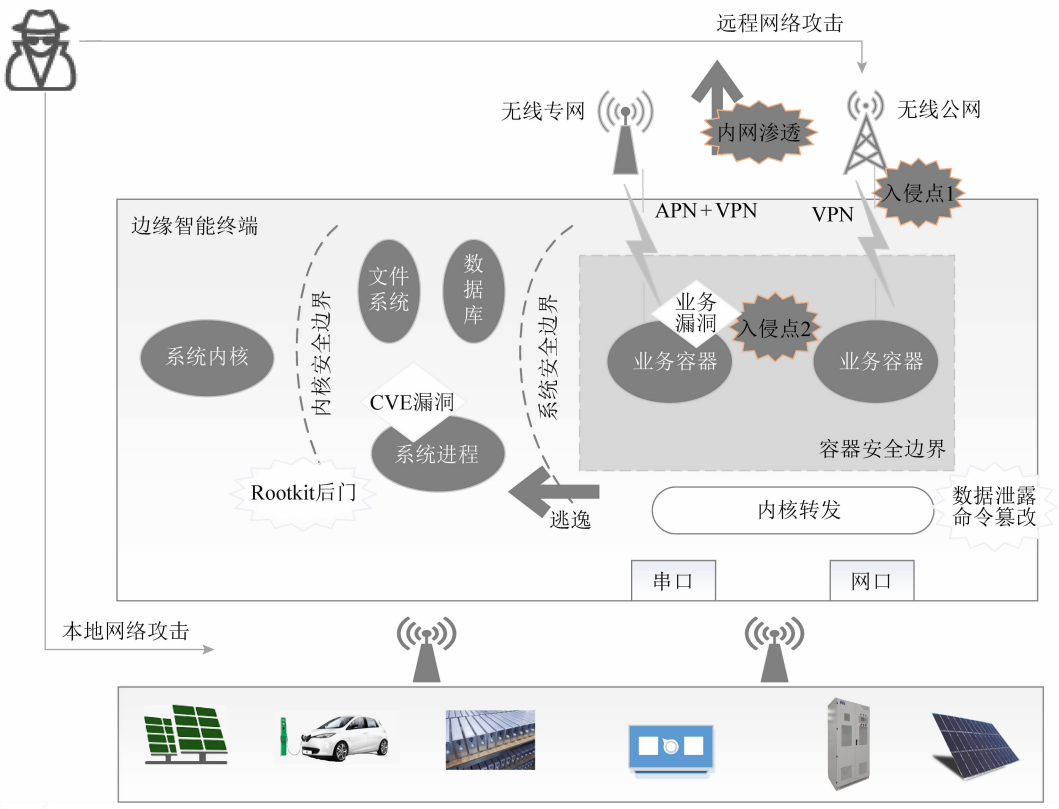

图 4 智能终端威胁模型

通过分析发现,边缘智能终端主要面临的威胁来自于远程网络攻击,远程攻击发生后,可以穿过设备内部的安全边界向系统内核渗透,甚至通过电力业务逻辑漏洞向调度主站或聚合商内网渗透.

本地认证器基于信任列表和信任策略对边缘智能设备持续进行动态信任评估.动态信任评估综合考虑影响智能终端安全的多方面因素,如网络接入环境、终端异常行为、终端数字身份等.电力业务连接一旦建立,往往会长时间保持连接状态,传统方式是在连接建立时进行身份认证,在后续的业务交互时无法识别终端实时安全状态,可能导致业务漏洞被终端上的非法程序利用,而动态信任评估是持续进行的,能及时发现智能终端上的异常行为,进而根据评估策略决定是否关闭当前的业务连接.

为节省智能终端的网络带宽和减少对零信任网关和控制器的访问请求,认证结果保存在本地认证器中,在本地业务发起 SPA 请求时(如图 3 所示),将本地设备认证结果发送给零信任控制器.

3.3 南向终端认证

南向物联终端处于电力物联网感知层,通过边缘智能终端汇聚接入,其身份认证由边缘智能终端上的本地认证器完成.物联终端类型和处理能力各异,对终端设备的身份认证难以形成统一的标准,文献[10]分析对比了南向物联终端设备的各种认证协议和认证方法,这些协议和方法各有

信息安全研究 Journal of Information Security Research 第10卷 第1期 2024年1月 Vol.10 No.1 Jan. 2024

优缺点.针对电力物联网的终端设备特点,本文采用可扩展的终端认证方案,既支持具备认证能力的接入协议,如 Lora、蓝牙等;对于无认证方式接入的终端也能通过被动指纹技术自动发现和识别,并建立设备的指纹身份信息.

本地认证器采用的被动指纹识别技术采用多层网络流量特征的识别功能,包括 MAC 指纹,系统指纹、网络指纹、电力协议指纹识别.其中 MAC 指纹属于硬件指纹,具有较高的识别度,容易被伪造,实际使用过程中需要配合其他的检测方式共同使用.系统指纹是指通过网络流量分析终端操作系统类型;网络指纹是针对工控协议业务流量比较固定的特点,对某些固定位置网络报文进行时序探测,形成设备或业务指纹;电力协议指纹是在网络指纹基础上增加具体电力网络协议报文特征进行探测,形成"特征+时序"模式,提高设备或业务指纹的准确率.不同被动指纹模型的测试结果如表 1 所示:

表 1　南向终端被动指纹检测测试结果

测试项目	识别率		
	系统指纹	CLRT	电力协议指纹
终端上电过程	0.64	0.76	0.92
业务建立过程	0.64	0.60	0.92
数据篡改	0	0.88	0.96
中间人嗅探	0	0.80	0.92

注:1)本次测试采用远动、逆变器、台区终端、交互终端、模拟终端作为南向感知终端接入设备;终端操作系统覆盖无操作系统、通用 Linux 操作系统、自主可控操作系统、容器;2)本次测试终端的接入协议使用网络 Modbus,DL/T 5104 协议;3)CLRT (cross-layer response time).

3.4　基于可信计算的信任传递

可信计算为智能终端提供了主动免疫防御能力,基于硬件的密码模块和动态度量技术为智能终端关键系统软件提供了完整性保护.

本地认证器基于可信计算提供的信任根进行信任扩展,将信任链扩展到 SPA 代理,再经 SPA 认证扩展到零信任网络的接入认证.支持可信计算的智能终端上操作系统内核是经过静态度量的,被认为是安全可靠的运行环境,本地认证器可对内核进行扩展,基于内核对本地认证器中的数据(如设备证书私钥和信任列表)进行访问控制,以实现基于 BLP 模型的安全访问.具体实施步骤如图 5 所示:

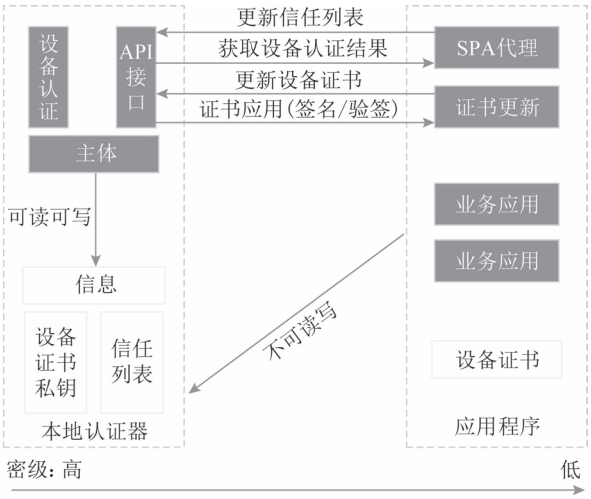

图 5　基于 BLP 模型的安全访问控制

4　实验与分析

4.1　实验环境

本文主要针对边缘智能终端设备通过不同认证方案的安全性进行测试,采用新能源光伏配电网络搭建本文实验的测试环境,配电终端作为边缘智能终端设备,通过 4G 网络接入模拟主站.配电终端与主站之间分别采用 IPsec VPN、SDP、分布式认证方案进行安全性测试,测试环境如图 6 所示.

在图 6 所示的拓扑结构中,边缘智能终端及北向网络为本文测试对象,感知终端和南向网络无关本文测试的实验结果.

4.2　实验内容

根据测试拓扑依次将智能交互终端通过 IPsec VPN、SDP、分布式认证方案接入到模拟主站的安全接入区,通过攻击终端模拟 ATT&CK 模型中的不同阶段战术措施对接入网络和边缘终端设备实施的网络攻击.

根据电力物联网对终端接入认证和业务数据安全传输的要求,本文实验在攻击战术的选择上侧重于针对设备身份认证、数据泄露和服务可靠性的攻击战术,包括身份验证、启动执行、行为隐藏、中间人攻击、服务扫描、网络数据嗅探、本地数据嗅探、C2 Channels、DDoS 攻击.

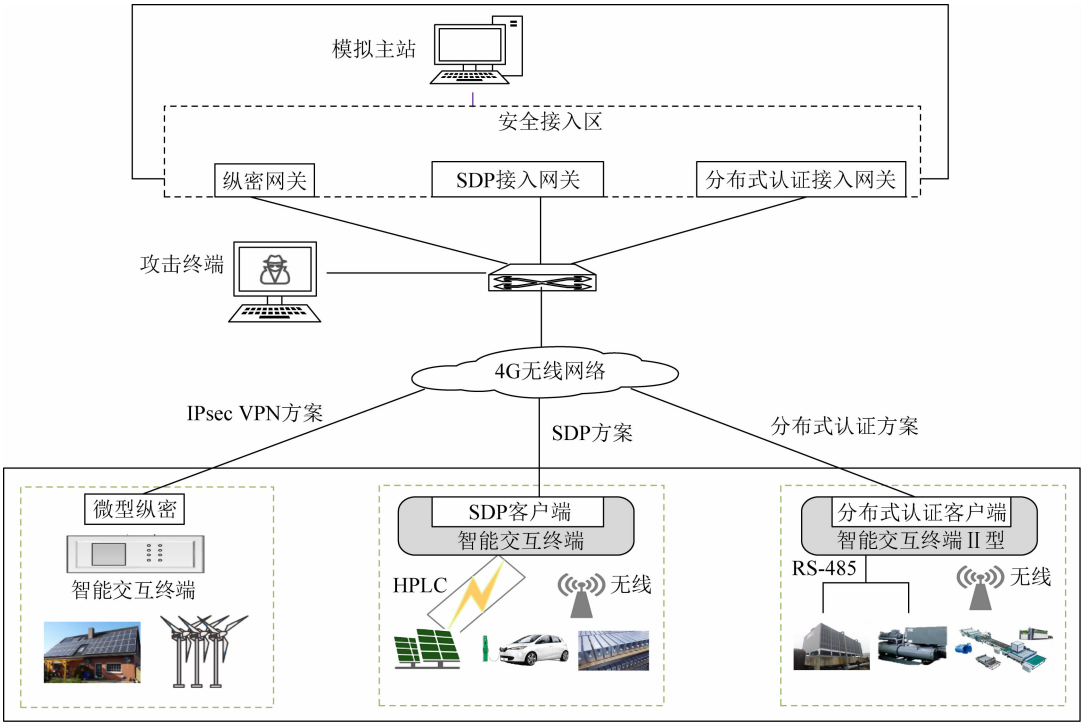

图 6　本文实验拓扑结构

4.3　实验结果分析

在 3 种安全接入方案的接入认证和接入后业务运行过程中，分别采用 3.2 节选择的攻击战术对边缘智能终端设备或接入网络进行攻击，测试结果如表 2 所示：

表 2　电力物联网安全防护方案测试结果

攻击战术	防御方案（是否支持防御或检测）		
	IPsec VPN	SDP	分布式认证（本文）
身份验证	支持	支持	支持
启动执行	不支持	不支持	支持
行为隐藏	不支持	不支持	支持
中间人攻击	支持	支持	支持
服务扫描	不支持	支持	支持
网络数据嗅探	支持	支持	支持
本地数据嗅探	不支持	不支持	支持
C2 Channels	不支持	支持	支持
本体 DDoS 攻击/pps	100	500	500
服务 DDoS 攻击/pps	2 000	50 000	50 000

注：1）本体 DDoS 攻击是针对认证架构本身的攻击行为，服务 DDoS 攻击是针对所保护的内部业务的攻击行为；2）本文测试所选用的攻击战术来自于 ATT&CK 模型.

由表 2 可知，分布式认证方案在接入认证和数据安全方面均可提供较好的防护能力.相较于传统 VPN 认证方案，SDP 能提供对服务扫描和非法数据回传通道的阻断；分布式认证方案则在 SDP 基础上提升了智能终端本地安全防护能力.另外，SDP 和分布式认证方案均基于 SPA 单包认证实现接入终端的认证，在认证流程的 DDoS 防护上，相较于 IPsec VPN 方案流程和算法上的资源消耗降低 80%，而在隧道建立后的业务 DDoS 防护上，性能提升 25 倍，因为 IPsec VPN 提供的是粗粒度的网络层隧道加密方案，业务 DDoS 攻击防护需要在解密报文后由防火墙或服务器处理，而 SDP 和分布式认证方案则是采用 mTLS 提供细粒度业务加密隧道，在接入网关上可直接对业务 DDoS 攻击进行防护阻断，无需解密报文，具有较高的防护性能.

5　结　　语

本文提出了一种基于电力物联网零信任架构下的分布式认证模型，该模型以电力物联网设备接入身份认证模型为基础，结合零信任安全理念，

信息安全研究 Journal of Information Security Research 第10卷 第1期 2024年1月 Vol.10 No.1 Jan. 2024

采用认证下沉的方式，提升对边缘智能终端设备和南向感知设备的安全防护能力.实验结果表明，该方法可有效提升终端的网络安全攻击防护和业务数据防泄露、防篡改能力，并在 DDoS 防护性能上得到大幅提升.

参 考 文 献

[1] 余海，郭庆，房利国. 零信任体系技术研究[J]. 通信技术，2020，53(8)：2021-2034

[2] 刘涛，马越，姜和芳，等. 基于零信任的电网安全防护架构研究[J]. 电力信息与通信技术，2021，19(7)：25-32

[3] 冯景瑜，于婷婷，王梓莹，等. 电力物联场景下抗失陷终端威胁的边缘信任模型[J]. 计算机研究与发展，2022，59(5)：1120-1132

[4] 刘隽良，刘羽，王月兵，等. 基于零信任软件定义边界可信设备准入认证技术[J]. 信息安全研究，2021，7(增刊 2)：110-113

[5] Shah S W，Syed N F，Shaghaghi A，et al. LCDA：Lightweight continuous device-to-device authentication for a zero trust architecture (ZTA)[J]. Computers & Security，2021，9(108)：102351

[6] Ying B，Nayak A. Anonymous and lightweight authentication for secure vehicular networks [J]. IEEE Trans on Vehicular Technology，2017，66：10626-10636

[7] 张刘天，陈丹伟. 基于零信任的动态访问控制模型研究[J]. 浙江电力，2022，8(10)：1008-1017

[8] 曹翔，姜敏. 基于业务关联模型的变电站网络安全风险评估方法[J]. 电力信息与通信技术，2022，20(11)：57-64

[9] Alagappan A，Venkatachary S K，Andrews L J B. Augmenting zero trust network architecture to enhance security in virtual power plants [J]. Energy Reports，2022，8：1309-1320

[10] 徐超，王纪军，吴小虎，等. 一种基于流量指纹的物联网设备实时自动检测及识别[J]. 信息安全研究，2021，7(6)：543-549

[11] 韩丽芳，张晓，应欢，等. 电力关键信息基础设施网络安全攻防演练研究[J]. 电力信息与通信技术，2022，20(7)：26-32

[12] 马靖，许勇刚，刘增明，等. 基于零信任框架的泛在电力物联网安全防护研究[J]. 网络安全与应用技术，2020 (1)：116-118

唐大圆

硕士，工程师.主要研究方向为电力系统网络安全攻防.

tangdy@nrec.com

曹　翔

硕士，高级工程师.主要研究方向为变电网络安全防护方案和风险评估.

caoxiang@nrec.com

林　青

硕士，高级工程师.主要研究方向为变电网络安全防护和电力设备可信计算安全.

linq@nrec.com

胡绍谦

硕士，正高级工程师.主要研究方向为变电站自动化系统和网络安全防护.

husq@nrec.com

汤震宇

硕士，正高级工程师.主要研究方向为电力监控系统网络安全防护.

tangzy@nrec.com