计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.20211129
59(5):1120-1132,2022

电力物联场景下抗失陷终端威胁的边缘零信任模型

冯景瑜[1] 于婷婷[1] 王梓莹[2] 张文波[1] 韩 刚[1] 黄文华[1]
[1](西安邮电大学无线网络安全技术国家工程实验室 西安 710121)
[2](国网江苏省电力有限公司电力科学研究院 南京 211103)
(zhangwenbo@xupt.edu.cn)

An Edge Zero-Trust Model Against Compromised Terminals Threats in Power IoT Environments

Feng Jingyu[1], Yu Tingting[1], Wang Ziying[2], Zhang Wenbo[1], Han Gang[1], and Huang Wenhua[1]
[1](*National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, Xi'an* 710121)
[2](*Electric Power Research Institute, State Grid Jiangsu Electric Power Co., Ltd., Nanjing* 211103)

Abstract With the continuous penetration of information technology into the power industry, the exposure of power IoT networks has been further increased. Attackers can use compromised terminals as the springboard to infiltrate the network, and thus stealing sensitive data or doing damage in the power industry system. Aiming at the bottleneck of zero-trust centralized deployment of massive power terminals access, an edge zero-trust model is proposed. Around the dense power terminals, zero-trust engine should be deployed in manner of distributed multi- points. Trust factors are collected in real time and stored on the blockchain. By maintaining a consortium blockchain called TF_chain, the storage edge servers can synchronously share trust factors generated by power terminals on the move, and thus facilitating traceability and preventing tampering. The abnormal and sensitive factors are extracted to carry out dynamic trust evaluation. The trust value can be rapidly attenuated by the sudden behaviors of compromised terminals, so as to fast prevent their threats during the authentication. A lightweight signcryption method is adopted to ensure the security of authentication information transmitted from edge to cloud. The simulation results show that the proposed model can disperse the zero-trust processing load of centralized deployment and effectively fight against compromised terminals threats under the condition of marginal deployment.

Key words power IoT; zero-trust; edge computing; trust evaluation; blockchain

摘 要 信息化技术在电力行业的不断深入,使得电力物联网的暴露面大幅增加.攻击者以失陷终端为跳板渗入网络内部,可以窃取电力工业系统中的敏感数据或实施破坏.面对海量电力终端接入的零信任中心化部署瓶颈,提出了一种边缘零信任模型.围绕密集的电力终端,分布式多点部署零信任引擎,实时收集信任因素并上链存储.通过维护一个联盟区块链——信任因素区块链(trust factors chain, TF_chain),存储型边缘服务器同步共享电力终端在移动中产生的信任因素,便于追踪溯源和防止信息被篡改.提取

收稿日期:2021-11-16;**修回日期**:2022-01-13
基金项目:国家自然科学基金项目(62102312);国家电网有限公司科技项目(J2021206)
This work was supported by the National Natural Science Foundation of China (62102312) and the Science and Technology Project of State Grid Co., Ltd. (J2021206).
通信作者:于婷婷(lotus_yt@163.com)

异常因子和敏感因子,进行动态信任评估,对失陷终端的突变行为实现信任值迅速衰减,在认证中及时阻断失陷终端威胁.采用轻量级签密,确保认证信息从边缘到云端传递的安全性.仿真结果表明,所提出的模型可以分散中心化部署的零信任处理负载,在边缘化部署条件下有效抗击失陷终端威胁.

关键词 电力物联网;零信任;边缘计算;信任评估;区块链

中图法分类号 TP393

电力物联网是应用于电力行业的工业级物联网,可以快速提升电网的感知、互动与调节能力,保障电力系统"发、输、变、配、用"环节的安全、稳定、持续、高效运行[1].作为关乎国计民生的重要基础设施,电力物联网一直都是网络攻击的重点目标.

随着"大云物移智链边"等新兴技术在电力行业的广泛应用,电力物联网中接入的终端种类和数量大幅增加[2].海量终端的接入进一步增加了电力物联网的暴露面,这对以边界隔离为特征的网络安全防御系统提出了严峻的挑战[3].研究表明,大部分智能终端存在着安全隐患和漏洞,相关终端的固件同时还存在厂商植入的后门[4].智能终端的安全性极大程度上决定了电力物联网的安全稳定[5],一旦遭受攻击,可能失去对电力终端的正常控制能力[6].于是,攻击者可以寻找具有脆弱性的电力终端进行入侵控制或窃取身份,绕过边界网络安全防御系统后,以失陷终端为跳板实施内部威胁.攻击者一旦通过某种跳板侵入电力网络内部,极易伪造虚假数据和发送恶意控制命令[7].

Ponemon研究所发布的《2020内部威胁成本:全球报告》[8]显示:内部威胁造成的数据泄露成本在2年间增长了31%,达到1000余万美元.现有的内部威胁检测方法多关注恶意内部人员检测[9].其实,失陷终端造成的内部威胁可能危害性更大,其主要原因在于以量取胜和行为突变.由于电力终端种类和数量众多,攻击者通过广泛撒网方式控制的失陷终端越多,攻击机会就越大,从而达到以量取胜的目的.失陷终端未被入侵控制前,一直从事正常行为.攻击者可以披着"合法身份"的外衣突然干坏事,这种行为突变能充分利用攻击检测的时间滞后性,出奇制胜.

遵循"永不信任,始终认证"的原则,网络中所有设备、用户和流量都应经过认证和授权,零信任已成为对抗内部威胁的一种有效手段[10].然而,现有研究方案多偏向于零信任引擎的中心化部署,难以应对海量终端接入电力物联场景下的认证需求.此外,零信任引擎的部署若距离电力终端过远,容易延迟认证时间,不利于零信任在时延敏感的电力物联场景下的应用推进.

深入分析海量终端接入电力物联场景下的认证需求,零信任应该从中心走向边缘,围绕密集的电力终端部署零信任引擎,对抗其中潜在的失陷终端威胁,从而构建出一种边缘零信任模型.本文的主要创新之处有3方面:

1) 将零信任赋予的网络内部监控和认证职能,下沉到电力物联网边缘,靠近电力终端,分布式多点部署零信任引擎,防止单点失效和拒绝服务攻击.明确了零信任核心组件之间的相互协作运行机制,使用虚拟化方式配置零信任核心组件,减轻了对边缘服务器的消耗.

2) 边缘分离信任评估涉及信任因素收集、存储和计算.充分利用安装在电力终端上的零信任客户端,实时收集信任因素,提交给就近的边缘服务器.引入联盟区块链——信任因素区块链(trust factors chain, TF_chain),由存储型边缘服务器共同维护,实现电力终端在移动中产生的信任因素共享,有助于追踪溯源和防止信息被篡改.零信任引擎只负责认证,调度TF_chain上的数据,就可快速计算出电力终端的信任值,避免了零信任引擎更替过程中容易出现延时的数据迁移工作.从信任因素中提取异常因子和敏感因子,形成边缘动态信任评估方案,迅速反应失陷终端的行为突变,做到及时阻断.

3) 设计了适用于边缘认证信息传递的签密方案,基于椭圆曲线的无证书策略,避免了密钥托管问题.该方案在计算效率上具有较好的轻量性,可以抵抗边缘认证信息的篡改,确保安全传递到云端.之后,位于云端的电力数据中心仅需验证和发放授权凭证,依据资源访问请求类型提供相应的服务,有效缓解了安全认证压力.

1 相关工作

随着网络安全边界的逐渐淡化,零信任越来越受到产业界重视.自从遭遇Google极光事件后,谷歌

开始启动零信任领域的研究计划,其为员工打造的BeyondCorp[11]架构成为第一个真正实现零信任的落地方案,明确了用户、设备与应用之间的安全关系,通过持续鉴权模式建立可信链条,允许合法用户访问受保护的业务.腾讯在《零信任解决方案白皮书》[12]中概括了零信任的核心思想,指出不以网络内外来区分访问主体,未验证的流量都默认为不可信.工业和信息化部在《关于促进网络安全产业发展的指导意见(征求意见稿)》中,首次将零信任安全列入需要"着力突破的网络安全关键技术"[13].

美国国家标准技术研究院(National Institute of Standards and Technology, NIST)发布的《零信任安全架构》标准草案[14]指出,零信任安全架构是一种端到端的网络/数据保护方法,包括身份、凭证、访问管理、运营、终端、主机环境和互联的基础设施等多个方面.作为目前最具权威性的零信任安全架构,NIST 提出的架构主要包括主体、受访资源、辅助系统和零信任引擎等,如图 1 所示:

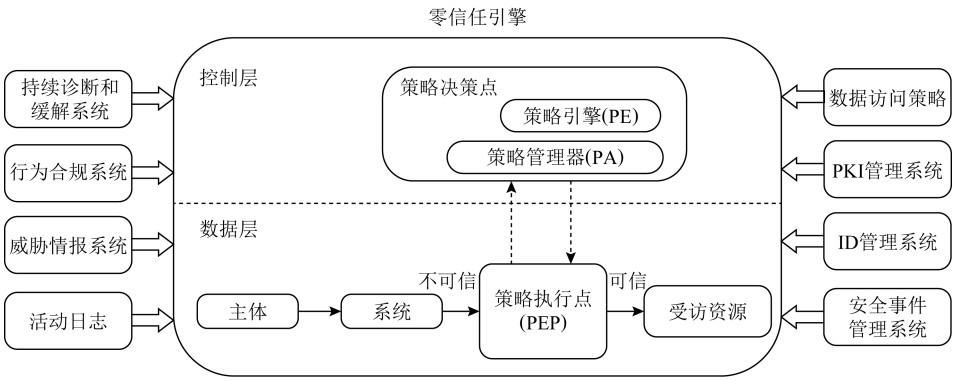

Fig. 1 Zero trust security architecture proposed by NIST[14]

图 1 NIST 提出的零信任安全架构[14]

主体就是网络内部可以访问资源的用户、设备或终端.通常在主体上安装零信任客户端进行风险感知,实时监控设备的安全状态,如出现越权操作、恶意数据注入等可疑行为,会及时被零信任客户端发现,告知零信任网关拦截.如未安装零信任客户端或出现对零信任客户端的操控行径,主体就无法在网络内容进行通信活动和请求访问资源.

鉴于零信任客户端的风险感知机制能及时阻断异常流量方面的可疑行为,策略引擎(policy engine, PE)、策略管理器(policy administrator, PA)、策略执行点(policy enforcement point, PEP)等核心组件构成的零信任引擎,则注重保护网络内部的受访资源,防范敏感信息被窃取的威胁.其中,PE 对主体的可信情况进行分析,形成认证结果;PA 根据认证结果,判决允许或拒绝连接;PEP 负责持续监控和结束主体与受访资源之间的连接,通常被称为零信任网关.

零信任能够有效提高数据中心对系统内恶意节点横向移动以及网络渗透攻击的防御能力[15].因此,零信任也迅速成为学术界的研究热点,研究者主要依托 NIST 提出的零信任安全架构开展相关研究.文献[16]在云架构的软件定义网络框架中针对MAC 欺骗的问题,提出了一种基于零信任网络的访问控制策略.文献[17]提出一种基于零信任的物联网安全架构,采用全面认证和实时监控的策略实现电力物联网的安全.文献[18]提出了一种云环境下的概念性零信任策略,防范数据泄露风险,保障数据的完整性和机密性.文献[19]针对当前电力移动互联面临的安全风险,从身份识别和访问控制 2 个方面设计了基于零信任的安全防护框架.文献[20]提出了一种基于零信任模型的医疗健康数据漏洞的防御系统,经过身份验证的用户和设备才能与网络交互,确保数据传输的安全性.

在零信任安全架构中,对实体的认证大多基于信任评估.目前,已经存在一些相关的信任评估机制.文献[21]设计了一种多维信任评估方案,包括评估节点的综合信任值和相邻节点的推荐信任值.文献[22]在云环境中提出了一种信任管理框架,设置信任反馈模块以增强信任值计算和更新的可信度.文献[23]通过发送无人机感知物联网设备数据来评估移动车辆的信任值,保证数据收集过程中低成本的安全性.文献[24]提出了一种电力终端信任共识方法,基于 Beta 分布建立了多元信任评价主体机制,得出综合信任值.

综合国内外研究现状,零信任引擎的部署多偏向于中心化,在终端数量有限的场景下,可以有效监控

失陷终端,阻断恶意数据注入和防止敏感信息的窃取威胁.对于海量终端接入的电力物联场景,中心化的零信任引擎部署容易出现单点失效故障.此外,契合零信任原则的信任评估方法较为缺乏,现有的信任评估方案多采用静态的信任值计算方法,信任值的更新滞后于主体行为的变化,难以及时应对行为突变的失陷终端威胁.

对此,面向海量终端接入的电力物联场景,本文提出了一种抗失陷终端威胁的边缘零信任模型.表1展示了本文模型相对于最新相关研究工作的优势.

Table 1 Comparison with Related Works

表1 与相关研究工作的对比

相关工作	零信任引入	监控方式	信任评估	突发行为阻断	认证信息传递	信任因素收集
文献[17]	支持	中心化	不支持	不支持	加密	不支持
文献[18]	支持	中心化	动态	不支持	不支持	不支持
文献[19]	支持	中心化	静态	不支持	加密	中心化收集
文献[20]	支持	区块链	不支持	不支持	不支持	不支持
文献[21]	不支持	不支持	静态	不支持	不支持	不支持
文献[22]	不支持	不支持	静态	不支持	不支持	不支持
本文模型	支持	边缘化	动态	及时阻断	签密	边缘实时收集

2 系统架构

边缘计算作为电力物联网的重要技术,其实质是一种分散式运算架构[25].将云计算和存储能力下沉到网络边缘,可以实现应用、服务和内容的本地化、近距离、分布式部署[26].另外,就地化分布式保护[27]已成为保障电力物联网稳定运行的重要思路.

鉴于此,可将零信任赋予的网络内部监控和认证职能,下沉到按照电力系统“发、输、变、配、用”环节划分的每个边缘区域,在电力终端周围进行零信任引擎的分布式部署和相关信任评估.

电力物联场景下的边缘零信任模型,可建立在“端”“边”“云”系统架构上实现.如图2所示,该架构包括终端层、边缘层和云层.

1) 终端层.对每个联网的电力终端安装零信任

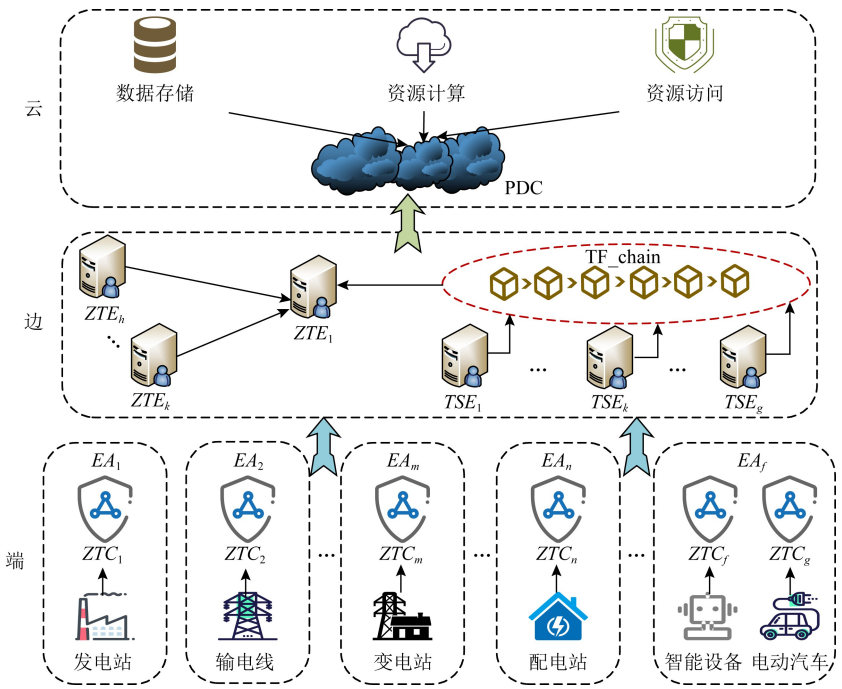

Fig. 2 Network architecture of edge zero-trust model

图2 边缘零信任模型的系统架构

客户端,实时监控其网络活动和资源访问请求.零信任客户端带有的风险感知机制,能对异常流量方面的可疑行为进行及时阻断.对于电力终端的资源访问请求,零信任客户端一般难以确定可疑情况,需要提交给零信任引擎进行认证研判.

2) 边缘层.根据业务范围,电力物联网可以划分为 f 个边缘区域,定义为集合 $\Gamma=\{EA_1,EA_2,\cdots,EA_k,\cdots,EA_f\}$.在每个区域,统一分配边缘服务器集合 $\Lambda=\{\Theta,\Phi\}$.其中,$\Theta=\{TSE_1,TSE_2,\cdots,TSE_k,\cdots,TSE_g\}$为 g 台边缘服务器组成的信任存储引擎集合,共同维护一个 TF_chain 实现可追踪、防篡改的终端信任因素存储;$\Phi=\{ZTE_1,ZTE_2,\cdots,ZTE_k,\cdots,ZTE_h\}$为$h$ 台边缘服务器组成的零信任引擎集合,包含 1 个主引擎和 $h-1$ 个次引擎.当主引擎宕机时,会自动升级一个次引擎为主引擎.对装载零信任引擎的每台 ZTE 边缘服务器,按其硬软件资源进行虚拟化,统一虚拟成执行 PE,PA 和 PEP 等零信任核心组件功能的 3 个虚拟机.

3) 云层.输电、配电、售电等任何一个过程都需要电力数据中心对其进行服务[28].下沉零信任的监控和认证职能到网络边缘后,电力数据中心(power data center, PDC)仅需验证和发放授权凭证,然后依据资源访问请求类型提供相应的服务,在保障电力物联网内部安全的前提下,有效提高了认证效率.

3 边缘零信任模型设计

为适应电力物联场景下海量终端的监控和认证需求,做到失陷终端检测快速而有效,构建出一种边缘零信任模型.

3.1 边缘零信任引擎部署

在每个边缘区域分布式部署零信任引擎,是构建边缘零信任模型的首要环节.采用虚拟化方式,PE,PA 和 PEP 等零信任核心组件可配置在单台边缘服务器的 3 个虚拟机上,而不用花费 3 台边缘服务器分别去配置.

零信任核心组件之间的相互协作构成了零信任模型的运行机制,主要包含 6 个步骤:1)电力终端发出的资源访问请求,会被零信任客户端生成一个认证需求上报给 PEP;2)PEP 首先拦截资源访问请求,而后转发认证需求给 PE;3)PE 调用存储在 TF_chain 上的信任因素,计算终端信任值,对资源访问请求进行认证,并将认证结果分发给 PA 和 PEP;4)对于认证通过的主体,PA 生成授权凭据交给 PEP;5)PEP 将认证结果和授权凭据提交给云层的 PDC;6)验证授权结果有效后,PDC 通知 PEP 释放资源访问请求的拦截.

即使对零信任引擎进行了边缘化部署,某个边缘区域的电力终端发出的访问请求若较为频繁,也可能使零信任引擎宕机.特别地,攻击者可以在未探知零信任引擎具体位置的情况下,控制一些失陷终端制造大量没有注入任何恶意代码的正常流量,经由零信任客户端自动流向零信任引擎,形成拒绝服务攻击.

对此,应该对零信任引擎在每个边缘区域实施分布式多点部署,组成零信任引擎集合 $\Phi=\{ZTE_1,ZTE_2,\cdots,ZTE_k,\cdots,ZTE_h\}$.边缘分布式多点部署规则如下:

规则 1. Φ 集合中的 h 个零信任引擎分散于每个边缘区域的不同位置,避免攻击者的位置探测.主引擎处于工作状态,负责监控整个边缘区域的电力终端.其余的 $h-1$ 个次引擎处于待机状态,并建立轮值次引擎集合 Ξ,依次等待成为主引擎.

规则 2. 假设 ZTE_k 为主引擎,c_k 代表其处理能力.设置处理能力的告警阈值为 δ.一旦出现 $c_k\geqslant\delta$,ZTE_k 就向 Ξ 集合中的 $h-1$ 个次引擎广播离线通知.

规则 3. 主引擎长时间处于高强度工作状态,也可能给边缘服务器造成压力过载.给定 ZTE_k 的轮值时间为 t_k,设置最高轮值时长为 τ.当 $t_k\geqslant\tau$ 时,ZTE_k 向 Ξ 集合中的 $h-1$ 个次引擎广播离线通知.

规则 4. 为避免主引擎因突发宕机而无法发送离线通知,Ξ 集合中排名第一的次引擎(假设为 ZTE_p)需要一直监测主引擎的活动状态.

规则 5. ZTE_p 如果监测到 ZTE_k 突发宕机,就向 Ξ 集合中其后的次引擎广播 ZTE_k 的离线通知及其成为主引擎的上线消息.

规则 6. 宕机的主引擎恢复后,加载到 Ξ 集合中,成为最后一个次引擎.

3.2 边缘动态信任评估

动态信任评估是零信任模型实现电力终端快速认证的核心环节.随着零信任引擎的边缘化部署,适时提出边缘动态信任评估方案,有助于减轻云端计算负载.

如图 3 所示,边缘动态信任评估方案的实现涉及信任因素收集与上链存储,以及为 PE 调用服务的终端信任值计算.

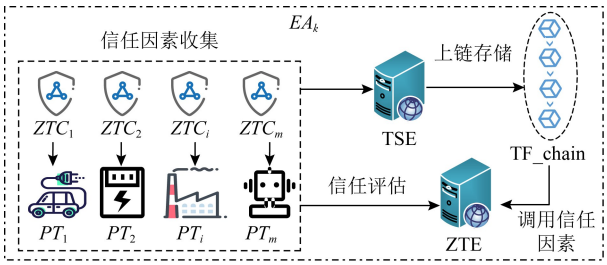

Fig. 3 Edge dynamic trust evaluation scheme

图 3 边缘动态信任评估方案

3.2.1 信任因素收集与上链存储

零信任客户端在监测电力终端网络活动过程中,需要根据终端行为变化情况,实时收集信任因素,提交给就近的 TSE 边缘服务器上链存储.

定义边缘区域 EA_k 中的电力终端集合 $\Delta=\{PT_1,PT_2,\cdots,PT_i,\cdots,PT_m\}$.以 PT_i 为例,ZTC_i 表示安装在其上的零信任客户端.PT_i 的信任因素集合包含 3 种类型,即 BTF,ATF,STF,典型的信任因素如表 2 所示.

BTF 表示基本信任因素,用于计算 PT_i 的基本信任值;ATF 表示异常信任因素,用于衰减 PT_i 的基本信任值;STF 表示敏感信任因素,用于及时阻断 PT_i 可能被失陷控制的情况.

每当 PT_i 的某个信任因素发生变化时,ZTC_i 就实时向就近的 TSE 边缘服务器发送更新信息.

鉴于联盟区块链[29]的预选共识矿工特点,ZTC_i 周围就近的 TSE 边缘服务器担任当前 TF_chain 区块链的共识矿工头.每当一个信任因素发生变化时,就会生成一个新区块.

Table 2 Trust Factors

表 2 信任因素

类型	标识	属性
BTF	btf_{i1}	认证成功
	btf_{i2}	认证失败
ATF	atf_{i1}	口令异常
	atf_{i2}	请求异常
	atf_{i3}	信息探测
	atf_{i4}	数据包异常
STF	stf_{i1}	身份冒用
	stf_{i2}	IP 地址错位
	stf_{i3}	越权请求
	stf_{i4}	信息篡改

对比特币的区块结构[30]进行改进,在继承原有参数{前一区块哈希,区块 ID,时间戳,Merkle 根}的基础上,新增$\{PT_i,sn_i^p,r_i\}$到区块头,打包更新的信任因素到区块体,如图 4 所示:

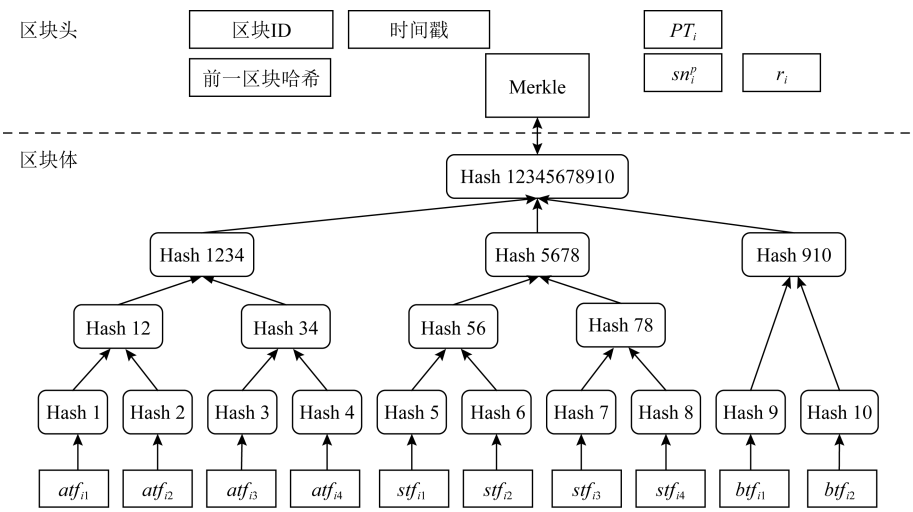

Fig. 4 Block storage structure for trust factors

图 4 信任因素的区块存储结构

在区块头中,sn_i^p 表示在 TF_chain 区块链上关于 PT_i 新生成区块 B_ID_p 的序列号,r_i 为冗余次数.序列号从 1 开始计数,Υ 表示 TF_chain 区块链上所有序列号的集合.区块体中存储着 PT_i 的各个信任因素.

由于边缘区域按照“发、输、变、配、用”环节业务划分,电力终端的移动一般不会超出本区域.但是,ZTC_i 实时向就近的 TSE 边缘服务器发送 PT_i 的信任因素更新信息,每发送一个信任因素更新,就会促使一个新区块生成,可能造成大量的冗余区块,

加重各个 TSE 边缘服务器的存储负载.对此,结合区块链的时序特征和信任因素的区块存储结构,提出算法 1 消除冗余区块.

算法 1 可以嵌入到 TF_chain 区块链的智能合约中定期自动运行,向前消除冗余区块,为 TSE 边缘服务器减轻存储压力.

算法 1. 冗余区块消除.

输入:Δ,Υ,r_i,TF_chain;

输出:TF_chain.

① for $PT_i \in \Delta$ then
② if $r_i \geqslant 1$ then
③ if $sn_i^p == \min(\Upsilon)$ then
④ 消除 TF_chain 的当前冗余区块;
⑤ 删除 Υ 集合中的 sn_i^p;
⑥ end if
⑦ end if
⑧ end for

信任因素存储在 TF_chain 区块链上的最大优势在于防篡改性.区块链是一种链式存储结构,下一区块保存了上一区块的哈希值.如果攻击者对其中一个区块进行篡改,该区块后面的所有区块都必须被修改.假设区块 B_ID_p 后面有 l_p 个区块,则篡改该区块后,还需继续篡改的区块个数 Z_p 为

$$Z_p = g + (g)^2 + \cdots + (g)^{l_p} = \frac{(g)^{l_p+1} - g}{g-1}. \quad (1)$$

例如,当 TSE 边缘服务器个数 $g=5$,$l_p=6$ 时,$Z_p=19\,530$,因此,TF_chain 区块链几乎无法被篡改.

3.2.2 终端信任值计算

Beta 分布能与信任分布很好地拟合,其数学期望可用于节点信任值计算,是最经典、最广泛使用的信任评估模型之一[31].Beta 分布具有计算简单、灵活性好、统计能力强和适用性强等特点[24].因此,采用 Beta 分布作为计算电力终端的基本信任值概率统计模型.Beta 分布大概率密度函数为[32]

$$Beta(\alpha,\beta) = \frac{\psi(\alpha,\beta)}{\psi(\alpha)\psi(\alpha)} \tau^{\alpha-1}(1-\tau)^{\beta-1}, \quad (2)$$

其中,τ 表示电力终端行为的可能性,$0<\tau<1$,$\alpha>0$,$\beta>0$.

在电力物联网中,使用 BTF 信任因素次数计算基本信任值.当 PT_i 认证成功时,$\alpha = btf_{i1}+1$.否则 $\beta = btf_{i2}+1$.因此,PT_i 的基本信任值可以用 Beta 分布函数计算:

$$bt_i = Beta(\alpha+1,\beta+1), \quad (3)$$

显然,α 和 β 都为整数.Beta 分布函数的期望值推导为

$$E[Beta(\alpha,\beta)] = \frac{\alpha}{\alpha+\beta}. \quad (4)$$

进一步计算 bt_i:

$$bt_i = \frac{btf_{i1}+1}{btf_{i1}+btf_{i2}+2}. \quad (5)$$

然而,bt_i 带有的静态信任评估特性,对于电力终端的失陷威胁行为反应具有一定的滞后性.假如 PT_i 失陷,bt_i 由于无法迅速衰减,会给攻击者带来多次实施威胁的机会.信任作为一种主观状态,可随用户交互经验、时间等因素的动态变化而发生变化,利用静态信任进行计算会使推荐结果渐渐偏离现实状态[33].因此,有必要引入异常衰减因子改进基本信任值,开启动态信任评估.

在电力物联网中,使用 ATF 信任因素次数计算异常衰减因子,协助零信任引擎的异常监测认证.PT_i 的异常因子计算如下:

$$af_i = \frac{1}{s \times \max(A_i)} \sqrt{\sum_{q=1}^{s} (atf_{iq})^2}, \quad (6)$$

其中,$A_i = \{atf_{i1}, \cdots, atf_{iq}, \cdots, atf_{is}\}$ 为 PT_i 的 ATF 信任因素次数集合;$\max(A_i)$为集合中的最大值,用于归一化异常因子.

算法 2. 电力终端可信认证.

输入:Ω;

输出:ar_i.

① 计算基本信任值 bt_i;
② if $bt_i<\sigma$ then
③ $ar_i=0$ 认证失败;
④ else
⑤ 计算动态信任值 dt_i;
⑥ if $dt_i<\sigma$ then
⑦ $ar_i=0$ 认证失败;
⑧ else
⑨ 计算终端信任值 t_i;
⑩ end if
⑪ if $t_i<\sigma$ then
⑫ $ar_i=0$ 认证失败;
⑬ else
⑭ $ar_i=1$ 认证成功;
⑮ end if
⑯ end if

引入异常衰减因子 af_i 后,PT_i 的动态信任值可计算为

$$dt_i=\begin{cases}\dfrac{btf_{i1}+1}{btf_{i1}+btf_{i2}+2}-\\ \quad\dfrac{1}{s\times\max(A_i)}\sqrt{\sum_{q=1}^{s}(atf_{iq})^2}, & dt_i>af_i,\\ 0, & dt_i\leqslant af_i.\end{cases}\tag{7}$$

同时,利用零信任客户端的风险感知机制,实时感知和收集 STF 信任因素次数,计算敏感因子 sf_i,及时应对失陷终端的突变行为,即

$$sf_i=\begin{cases}\sigma, \forall(stf_{iu})_{u=1}^{v}\geqslant 1,\\ 0, \text{all}(stf_{iu})_{u=1}^{v}=0.\end{cases}\tag{8}$$

当任意一个 STF 信任因素次数大于或等于 1 时,sf_i 的赋值为信任门限值 σ.待清除失陷终端上的恶意代码或指令,重新夺回控制权,加固安全后,PT_i 的 STF 信任因素次数清零.零信任客户端进入新的实时感知和收集阶段.

敏感因子 sf_i 的作用在于迅速调节 PT_i 的动态信任值低于门限值.因此,最终的终端信任值可计算为

$$t_i=\begin{cases}|dt_i-sf_i|, & \forall(stf_{iu})_{u=1}^{v}\geqslant 1,\\ dt_i, & \text{all}(stf_{iu})_{u=1}^{v}=0.\end{cases}\tag{9}$$

PE 调用存储在 TF_chain 上的信任因素集合 Ω,通过算法 2 得到关于 PT_i 的认证结果 ar_i.

3.3 边缘认证信息签密传递

认证成功后,PA 根据 PE 提交的认证结果 ar_i 生成授权凭据 ac_i 发送给 PEP,形成边缘认证信息 $m_i=(PT_i\parallel ar_i\parallel ac_i\parallel ts_i)$.其中,$ts_i$ 为该认证信息的时间戳.

若向 PDC 传递的边缘认证信息处于明文状态,攻击者可以在传输过程中劫持并篡改.对 m_i 进行签密传递,可以确保边缘认证信息的安全性和完整性.

如图 5 所示,签密传递的参与方有密钥生成中心(key generation center, KGC)、PEP 和 PDC.其中,KGC 负责随机生成密钥;PEP 对 m_i 加密和签名;PDC 负责接收和验证密文的正确性.签密传递方案的实现包括 5 个过程.

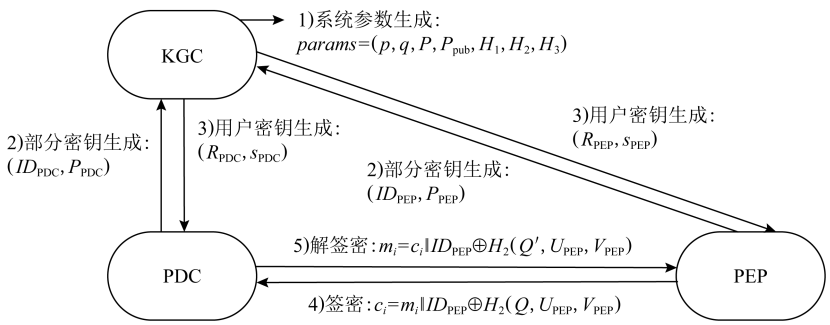

Fig. 5 Signcryption for edge authentication information

图 5 边缘认证信息的签密

1) 系统参数生成

KGC 选择一个安全参数 K,生成 2 个大素数 p 和 q. G 是阶为 q 的加法循环群,P 是 G 的一个生成元.定义哈希函数 $H_1:\{0,1\}^*\times G\times G\rightarrow Z_q^*$, $H_2:G\times G\times G\rightarrow\{0,1\}^*$, $H_3:\{0,1\}^*\times\{0,1\}^*\times G\times G\times G\times G\rightarrow Z_q^*$. KGC 随机选取 $x\in Z_q^*$ 作为主密钥.计算系统公钥 $P_{\text{pub}}=x\times P$. KGC 秘密保存主密钥 x,并公开系统参数 $params=(p,q,P,P_{\text{pub}},H_1,H_2,H_3)$.

2) 部分密钥生成

PEP 随机选取 $x_{\text{PEP}}\in Z_q^*$,计算公钥 $P_{\text{PEP}}=x_{\text{PEP}}\times P$.随后,将 PEP 的身份信息 ID_{PEP} 和公钥 P_{PEP} 通过安全信道传递给 KGC. KGC 随机选取 $r_{\text{PEP}}\in Z_q^*$,计算部分公钥 $R_{\text{PEP}}=r_{\text{PEP}}\times P$,部分私钥 $s_{\text{PEP}}=r_{\text{PEP}}+h_1^{\text{PEP}}\times x$.并将$\langle R_{\text{PEP}},s_{\text{PEP}}\rangle$通过安全信道传递给 PEP.其中,$h_1^{\text{PEP}}=H_1(ID_{\text{PEP}},R_{\text{PEP}},P_{\text{PEP}})$.

3) 用户密钥生成

PEP 通过计算 $s_{\text{PEP}}\times P=R_{\text{PEP}}+h_1^{\text{PEP}}\times P_{\text{pub}}$ 验证部分私钥是否有效.若有效,则 PEP 的公私钥分别为 $PK_{\text{PEP}}=(R_{\text{PEP}},P_{\text{PEP}})$, $SK_{\text{PEP}}=(s_{\text{PEP}},x_{\text{PEP}})$.

4) 签密

同样,可以计算出 PDC 的公私钥分别为 $PK_{\text{PDC}}=(R_{\text{PDC}},P_{\text{PDC}})$, $SK_{\text{PDC}}=(s_{\text{PDC}},x_{\text{PDC}})$.PEP 对边缘认证信息 m_i 的签密过程有 5 步:

① PEP 随机选取 $u_{\text{PEP}}\in Z_q^*$, $v_{\text{PEP}}\in Z_q^*$,计算 $U_{\text{PEP}}=u_{\text{PEP}}\times P$, $V_{\text{PEP}}=v_{\text{PEP}}\times P$.

② 计算 $Q=u_{\text{PEP}}\times(h_1^{\text{PDC}}\times P_{\text{pub}}+R_{\text{PDC}})+v_{\text{PEP}}\times P_{\text{PDC}}$.

③ 计算 $c_i=m_i\parallel ID_{\text{PEP}}\oplus H_2(Q,U_{\text{PEP}},V_{\text{PEP}})$.

④ 计算 $h_2^{PEP}=H_3(c_i,ID_{PEP},U_{PEP},V_{PEP},R_{PEP},P_{PEP})$.

⑤ 计算 $sig_{PEP}=x_{PEP}+h_2^{PEP}(u_{PEP}+s_{PEP})$.

PEP 生成签密后的密文 $\delta_i=(V_{PEP},U_{PEP},c_i,sig_{PEP})$,将其发送给 PDC.

5) 解签密

PDC 接收到密文 δ_i,进行解签密,验证密文的正确性.解签密过程有 4 步:

① $h_2^{PEP}=H_3(c_i,ID_{PEP},U_{PEP},V_{PEP},R_{PEP},P_{PEP})$.

② 计算 $Q'=U_{PEP}\times s_{PDC}+x_{PDC}\times V_{PEP}$.

③ 计算 $m_i=c_i\parallel ID_{PEP}\oplus H_2(Q',U_{PEP},V_{PEP})$.

④ 计算 $sig_{PEP}\times P=X_{PEP}+h_2^{PEP}\times(U_{PEP}+R_{PEP}+h_1^{PEP}\times P_{pub})$.

下面证明签密方案的正确性.

验证消息的真实性.由式(10)可知 $Q'=Q$,据此可以正确解密出明文 $m_i\parallel ID_{PEP}=c_i\oplus H_2(Q',U_{PEP},V_{PEP})$.

$$\begin{aligned}Q'&=s_{PDC}\times U_{PEP}+x_{PDC}\times V_{PEP}=s_{PDC}\times u_{PEP}\times P+\\&x_{PDC}\times v_{PEP}\times P=(r_{PDC}+h_1^{PDC}\times x)\times u_{PEP}\times P+\\&v_{PEP}\times P_{PDC}=u_{PEP}\times R_{PDC}+u_{PEP}\times h_1^{PDC}\times P_{pub}+\\&v_{PEP}\times P_{PDC}=u_{PEP}\times(R_{PDC}+h_1^{PDC}\times P_{pub})+\\&v_{PEP}\times P_{PDC}=Q.\end{aligned}\tag{10}$$

验证签名消息的真实性,验证式为

$$\begin{aligned}sig_{PEP}\times P&=X_{PEP}+h_2^{PEP}\times(U_{PEP}+R_{PEP}+h_1^{PEP}\times\\&P_{pub})=x_{PEP}\times P+h_2^{PEP}\times P\times(u_{PEP}+r_{PEP}+\\&h_1^{PEP}\times x)=(x_{PEP}+h_2^{PEP}\times(u_{PEP}+r_{PEP}+\\&h_1^{PEP}\times x))\times P=(x_{PEP}+h_2^{PEP}\times(u_{PEP}+\\&s_{PEP}))\times P.\end{aligned}\tag{11}$$

在本方案中,PEP 计算 $sig_{PEP}=x_{PEP}+h_2^{PEP}(u_{PEP}+s_{PEP})$进行签名.PEP 的私钥 SK_{PEP} 由 KGC 和 PEP 共同生成.假使攻击者能够获取 PEP 的身份信息,但计算签密者的私钥属于椭圆曲线离散对数困难问题,攻击者难以伪造其签名.因此,本方案可以抵抗边缘认证信息的篡改,确保安全传递到 PDC.

4 仿真分析

4.1 仿真环境设置

本文使用 Matlab 搭建实验平台,对所提方案进行仿真分析,验证抗击失陷终端威胁的抑制效果和边缘零信任安全模型的实施效率.

仿真环境参数设置如表 3 所示:

Table 3 Simulation Parameters Table

表 3 仿真参数表

参数	描述	预设值
N	电力终端数量	2000
E	边缘区域数量	5,10,20
Z	零信任引擎数量	10～30
Ts	仿真轮数	50
m	失陷终端比例	30%
σ	信任门限值	0.5

4.2 抗击失陷终端威胁仿真分析与结果

在零信任安全架构中,信任值是实现电力终端快速认证的有效依据. 通过 50 轮实验仿真,观测 3 种信任评估方案下失陷终端的信任值变化情况.

如图 6 所示,在前 20 轮,电力终端未失陷,3 种方案的信任值都趋于增加;到了第 20 轮,该电力终端突然被失陷控制,观测结果发生变化.

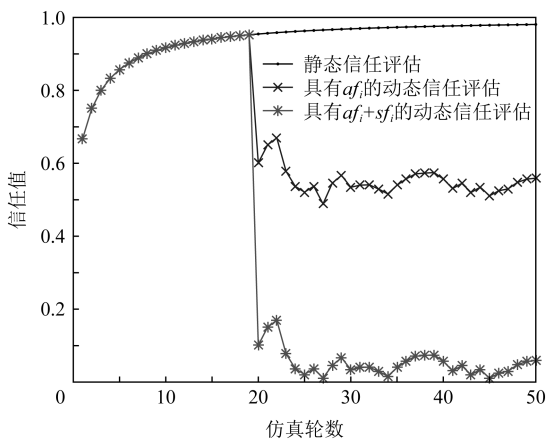

Fig. 6 Variation of trust value for a compromised terminal

图 6 失陷终端的信任值变化情况

对于静态信任评估方案,信任值的反应滞后性使失陷终端总能认证成功,反而造成信任值的持续增长.引入异常因子 af_i 的动态信任评估方案,可以快速反应电力终端的失陷情况,但信任值的衰减幅度有限,在门限值附近缓慢波动.随着轮数的增加,其会衰减到门限值以下,但可能给予失陷终端过多的威胁机会.引入异常因子 af_i 和敏感因子 sf_i 的动态信任评估方案,能及时应对电力终端的突变失陷,迅速将其信任值衰减到门限值以下.

当失陷终端的信任值低于门限值时,则无法认证成功,从而失去了恶意威胁机会.随机选取一个边缘区域为例,其中,电力终端数为 200,失陷终端比例

为 30%.如图 7 所示,静态信任评估方案不能衰减失陷终端的信任值,该边缘区域出现的恶意威胁次数无法被抑制.引入异常因子 af_i 的动态信任评估方案,难以将失陷终端的信任值衰减到门限值以下,也存在着抑制恶意威胁次数的困难.引入异常因子 af_i 和敏感因子 sf_i 的动态信任评估方案,能及时阻断失陷终端,恶意威胁次数在突发时就被迅速清零.

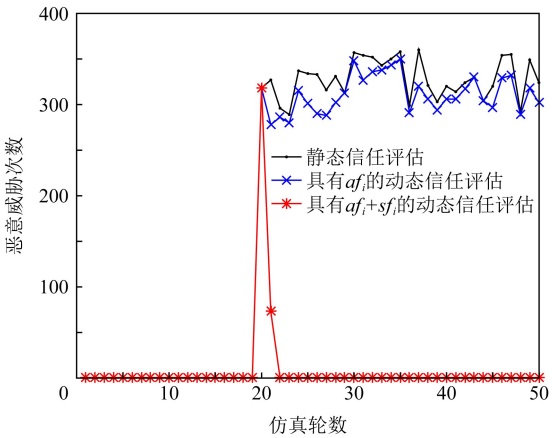

Fig. 7 Suppression of malicious threats

图 7 恶意威胁次数抑制情况

进一步观察在该边缘区域内的失陷终端检测情况.如图 8 所示,引入异常因子 af_i 和敏感因子 sf_i 的动态信任评估方案,表现出较好的失陷终端检测率,在出现失陷苗头时就被及时掐断和检测出来.

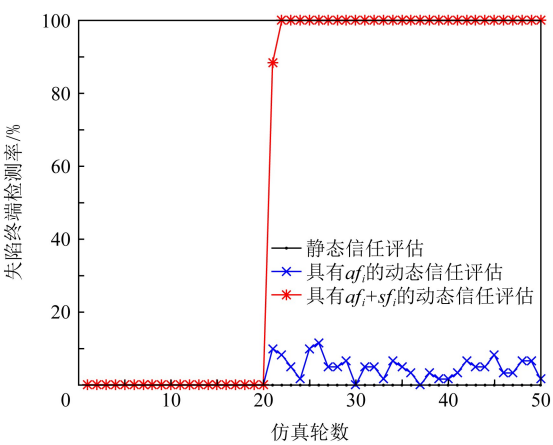

Fig. 8 Detection rate of compromised terminals

图 8 失陷终端检测率

4.3 边缘零信任模型效率仿真结果与分析

采用边缘化部署方案,能极大地减轻云端 PDC 的零信任处理负载.如图 9 所示,随着资源访问请求的增加,中心化部署方案下的零信任处理负载呈线性增长趋势.分散给边缘区域后,划分的边缘区域越多,每个边缘区域承接的零信任处理负载就越少.

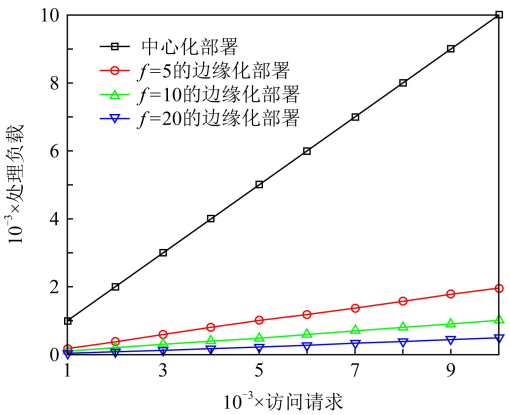

Fig. 9 Comparison of processing overload

图 9 处理负载对比

在每个边缘区域部署零信任引擎时,可以采取实体化配置或虚拟化配置 2 种方案.如图 10 所示,虚拟化配置零信任引擎的 PE,PA 和 PEP 核心组件到一台边缘服务器上,相对于给每个核心组件各实体化配置一台边缘服务器的方案,有效减轻了边缘服务器的消耗数量.

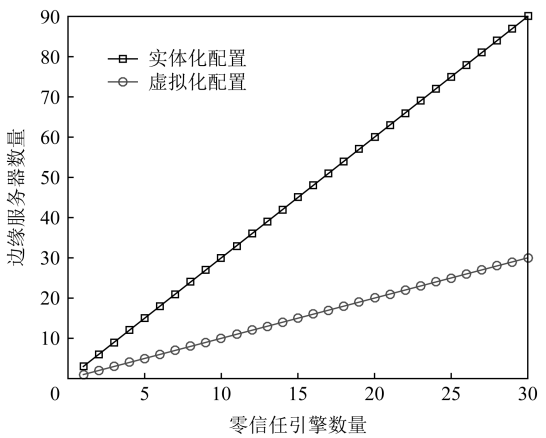

Fig. 10 Edge server consumption

图 10 边缘服务器消耗情况

最后,采用签密方案将生成的边缘认证信息传递给 PDC,可以有效防止篡改.为证明本文签密方案的计算效率轻量性,与最新的典型签密方案进行对比.

签密方案的计算效率,主要取决于椭圆曲线上的点乘 E_m 和点加 E_a 运算.结合具体测量结果(E_m=0.4847 ms,E_a=0.0021 ms)[34],从表 4 可以看出,本文方案在计算效率上优势明显.因此,本文签密方案可在确保边缘认证信息安全传递的同时,具有较好的计算效率轻量性.

Table 4 Comparison of Computation Efficiency

表 4 计算效率对比 ms

方案	签密时间	解签密时间	总时间
文献[35]方案	$4E_m+2E_a\approx1.9430$	$7E_m+4E_a\approx3.4013$	5.3443
文献[36]方案	$5E_m+2E_a\approx2.4277$	$7E_m+2E_a\approx3.3971$	5.8248
文献[37]方案	$6E_m+2E_a\approx2.9124$	$8E_m+6E_a\approx3.8902$	6.8026
本文签密方案	$5E_m+2E_a\approx2.4277$	$5E_m+4E_a\approx2.4319$	4.8596

5 总 结

针对零信任面临海量电力终端接入的中心化部署压力,提出了一种边缘零信任模型.在电力终端周围进行零信任引擎的分布式多点部署,设计信任因素的实时收集与区块链存储方案.引入异常因子和敏感因子,通过动态信任评估,能应对失陷终端的突变行为,迅速衰减其信任值.采用轻量级签密方案,确保及时阻断失陷终端威胁的边缘认证信息到云端传递的安全性.仿真结果表明,本文提出的边缘零信任模型,在抑制失陷终端威胁方面的效果显著,具有较好的失陷终端检测率.未来的研究工作是深入分析东西向流量特征,针对失陷终端在电力物联网内部发出的加密型恶意流量,设计有效的快速检测方法,进一步增强失陷终端威胁的抑制效果.

作者贡献声明:冯景瑜设计论文整体架构、系统模型和实验方案,并完成论文初稿的写作;于婷婷参与了系统模型和实验方案的设计、论文初稿的写作及修改;王梓莹和张文波负责实验仿真和实验结果分析;韩刚和黄文华对系统模型和实验方案提出建设性意见.

参 考 文 献

[1] Zhou Zhenyu, Wu Jun, Liao Haijun. Power Internet of Things Communication and Information Security Technology [M]. Beijing: China Machine Press, 2020 (in Chinese)
(周振宇, 伍军, 廖海君. 电力物联网通信与信息安全技术[M]. 北京: 机械工业出版社, 2020)

[2] Liu Tao, Ma Yue, Jiang Hefang, et al. Research on power grid security protection architecture based on zero trust [J]. Electric Power Information and Communication Technology, 2021, 19(7): 25-32 (in Chinese)
(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] Samaniego M, Deters R. Zero-trust hierarchical management in IoT [C] //Proc of 2018 IEEE Int Congress on Internet of Things (ICIOT). Piscataway, NJ: IEEE, 2018: 88-95

[4] Ying Huan, Liu Songhua, Han Lifang, et al. Overview of power industry control system security technology [J]. Electric Power Information and Communication Technology, 2018, 16(3): 56-63 (in Chinese)
(应欢, 刘松华, 韩丽芳, 等. 电力工业控制系统安全技术综述[J]. 电力信息与通信技术, 2018, 16(3): 56-63)

[5] Ding Weidong, Zhang Liquan, Xu Jianbing, et al. Review of standard system of power grid security and stability control system [J]. Electric Power Engineering Technology, 2021, 40(1): 58-64 (in Chinese)
(丁卫东, 张丽全, 许剑冰, 等. 电网安全稳定控制系统标准体系研究评述[J].电力工程技术, 2021, 40(1): 58-64)

[6] Wang Yu, Li Jun'e, Zhou Liang, et al. A self-healing architecture for power industrial control systems against security threats to embedded terminals [J]. Power System Technology, 2020, 44(9): 417-429 (in Chinese)
(王宇, 李俊娥, 周亮, 等. 针对嵌入式终端安全威胁的电力工控系统自愈体系[J]. 电网技术, 2020, 44(9): 417-429)

[7] Suo Yanfeng, Wang Shaojie, Qin Yu, et al. Summary of security technology and application in industrial control system [J]. Computer Science, 2018, 45(4): 25-33 (in Chinese)
(锁延锋, 王少杰, 秦宇, 等. 工业控制系统的安全技术与应用研究综述[J]. 计算机科学, 2018, 45(4): 25-33)

[8] Ponemon. 2020 cost of insider threats: Global report [EB/OL]. [2020-10-05]. https://www.proofpoint.com/us/resources/webinars/2020-cost-insider-threats-global-report

[9] Feng Yun, Liu Baoxu, Zhang Jinli, et al. An unsupervised method for timely exfiltration attack discovery [J]. Journal of Computer Research and Development, 2021, 58(5): 995-1005 (in Chinese)
(冯云, 刘宝旭, 张金莉, 等. 一种无监督的窃密攻击及时发现方法[J]. 计算机研究与发展, 2021, 58(5): 995-1005)

[10] Gilman E, Barth D. ZeroTrust Network: Building Secure Systems in Untrusted Networks [M]. Beijing: Posts and Telecommunications Press, 2019 (in Chinese)
(埃文·吉尔曼, 道格·巴斯. 零信任网络: 在不可信网络中构建安全系统[M]. 北京: 人民邮电出版社, 2019)

[11] Ward R, Beyer B. BeyondCorp: A new approach to enterprise security [J]. The Magazine of USENIX&Sage, 2014, 39(6): 6-11

[12] Tencent Security. Zero trust solution white paper [R/OL]. [2021-09-28]. https://cloud.tencent.com/developer/article/1636407
(腾讯安全. 零信任解决方案白皮书[R/OL]. [2021-09-28]. https://cloud.tencent.com/developer/article/1636407)

[13] Ministry of Industry and Information Technology of the People's Republic of China. Guidance on Promoting the Development of Cybersecurity Industry (Draft for Comments) [EB/OL]. (2019-09-27) [2021-10-03]. https://www.miit.gov.cn/ (in Chinese)
(中华人民共和国工业和信息化部. 关于促进网络安全产业发展的指导意见(征求意见稿)[EB/OL]. (2019-09-27) [2021-10-03]. https://www.miit.gov.cn/)

[14] NIST Special Publication 800-207. Zero trust architecture [R/OL]. [2021-10-02]. https://doi.org/10.6028/NIST.SP.800-207

[15] Huang Jie, Yu Ruochen, Mao Dong. Distributed database fine-grained access control based on zero trust in the power Internet of things [J]. Information Security Research, 2021, 7(6): 535-542 (in Chinese)
(黄杰, 余若晨, 毛冬. 电力物联网场景下基于零信任的分布式数据库细粒度访问控制[J]. 信息安全研究, 2021, 7(6): 535-542)

[16] Mandal S, Khan D A, Jain S. Cloud-based zero trust access control policy: An approach to support Work-From-Home driven by COVID-19 pandemic [J]. New Generation Computing, 2021, 39(3): 1-24

[17] Gao Peng, Yang Ruxia, Shi Congcong, et al. Research on security protection technology system of power Internet of things [C] //Proc of 2019 IEEE 8th Joint Int Information Technology and Artificial Intelligence Conf (ITAIC). Piscataway, NJ: IEEE, 2019: 1772-1776

[18] Mehraj S, Banday M T. Establishing a zero trust strategy in cloud computing environment [C] //Proc of 2020 Int Conf on Computer Communication and Informatics (ICCCI). Piscataway, NJ: IEEE, 2020: 1-6

[19] Chen Lu, Dai Zaojian, Chen Mu, et al. Research on the security protection framework of power mobile Internet services based on zero trust [C] //Proc of 2021 6th Int Conf on Smart Grid and Electrical Automation (ICSGEA). Piscataway, NJ: IEEE, 2021: 65-68

[20] Sultana M, Hossain A, Laila F, et al. Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology [J]. BMC Medical Informatics and Decision Making, 2020, 20(1): 1-10

[21] Mathapati M, Kumaran T S, Muruganandham A, et al. Secure routing scheme with multi-dimensional trust evaluation for wireless sensor network [J]. Journal of Ambient Intelligence and Humanized Computing, 2021, 12(6): 6047-6055

[22] Latif R, Afzaal S H, Latif S. A novel cloud management framework for trust establishment and evaluation in a federated cloud environment [J]. The Journal of Supercomputing, 2021, 77(4): 1-24

[23] Huang Shaobo, Liu Anfeng, Zhang Shaobo, et al. BD-VTE: A novel baseline data based verifiable trust evaluation scheme for smart network systems [J]. IEEE Transactions on Network Science and Engineering, 2020, 8(3): 2087-2105

[24] Yu Jiexiao, Yu Liying, Yang Ting. Blockchain-based trust consensus method for powerInternet of things terminal [J]. Automation of Electric Power Systems, 2021, 45(17): 1-10 (in Chinese)
(于洁潇, 于丽莹, 杨挺. 基于区块链的电力物联终端信任共识方法[J]. 电力系统自动化, 2021, 45(17): 1-10)

[25] Lü Jiwei. Optimization survey of online monitoring system for converter station based on ubiquitous power IoT [J]. Electric Power Engineering Technology, 2019, 38(6): 9-15 (in Chinese)
(吕继伟. 基于泛在电力物联网的换流站在线监测系统优化综述[J]. 电力工程技术, 2019, 38(6): 9-15)

[26] Abbas N, Zhang Yan, Taherkordi A, et al. Mobile edge computing: A survey [J]. IEEE Internet of Things Journal, 2018, 5(1): 450-465

[27] Qiu Yutao, Xu Yu, Wang Yuantao, et al. Ring network test device development of on-site distributed protection relay [J]. Electric Power Engineering Technology, 2021, 40(1): 72-78 (in Chinese)
(裘愉涛, 徐昱, 王源涛, 等. 就地化分布式保护环网测试装置研制[J]. 电力工程技术, 2021, 40(1): 72-78)

[28] He Yini, Cao Wei, Wei Changfu, et al. Resource allocation method of power grid cloud platform based on membrane computing and ant colony algorithm [J]. Electric Power Engineering Technology, 2020, 39(1): 103-109 (in Chinese)
(何伊妮, 曹伟, 韦昌福, 等. 基于膜计算和蚁群算法的电网云平台虚拟资源配置方法[J]. 电力工程技术, 2020, 39(1): 103-109)

[29] Meng Tianhui, Zhao Yubin, Wolter K, et al. On consortium blockchain consistency: A queueing network model approach [J]. IEEE Transactions on Parallel and Distributed Systems, 2021, 32(6): 1369-1382

[30] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system [EB/OL]. [2021-10-26]. https://bitcoin.org/bitcoin.pdf

[31] Ganeriwal S, Srivastava M B. Reputation-based framework for high integrity sensor networks [J]. ACM Transactions on Sensor Networks, 2004, 4(3): 66-77

[32] Josang A, Ismail R. The Beta reputation system [C] //Proc of the 15th Bled Electronic Commerce Conf. Bled, Slovenia: University of Maribor, 2002: 41-55

[33] Qi Faxin, Tong Xiangrong, Yu Lei. Agent trust boost via reinforcement learning DQN [J]. Journal of Computer Research and Development, 2020, 57(6): 1227-1238 (in Chinese)
(亓法欣, 童向荣, 于雷. 基于强化学习 DQN 的智能体信任增强[J]. 计算机研究与发展, 2020, 57(6): 1227-1238)

[34] Zhang Wenbo, Huang Wenhua, Feng Jingyu. Secure communication mechanism for VSN based on certificateless signcryption [J]. Journal of Communications, 2021, 42(7): 128-136 (in Chinese)
(张文波, 黄文华, 冯景瑜. 基于无证书签密的车联社会网络安全通信机制[J]. 通信学报, 2021, 42(7): 128-136)

[35] Gao Gaimei, Peng Xinguang, Jin Lizhong. Efficient access control scheme with certificateless signcryption for wireless body area networks [J]. International Journal of Network Security, 2019, 21(3): 428-437

[36] Karati A, Fan C I, Huang J J. An efficient pairing-free certificateless signcryption without secure channel communication during secret key issuance [J]. Procedia Computer Science, 2020, 171: 110-119

[37] Mandal S, Bera B, Sutrala A K, et al. Certificateless-signcryption-based three-factor user access control scheme for IoT environment [J]. IEEE Internet of Things Journal, 2020, 7(4): 3184-3197

Feng Jingyu, born in 1984. PhD, associate professor. His main research interests include IoT security, blockchain and zero-trust.

冯景瑜,1984 年生.博士,副教授.主要研究方向为物联网安全、区块链和零信任.

Yu Tingting, born in 1997. Master candidate. Her main research interests include IoT security and zero-trust.

于婷婷,1997 年生.硕士研究生.主要研究方向为物联网安全和零信任.

Wang Ziying, born in 1991. Master, engineer. Her main research interest is network security.

王梓莹,1991 年生.硕士,工程师.主要研究方向为网络安全.

Zhang Wenbo, born in 1983. PhD, lecturer. His main research interest is IoT security.

张文波,1983 年生.博士,讲师.主要研究方向为物联网安全.

Han Gang, born in 1990. PhD, lecturer. His main research interest is IoT security.

韩 刚,1990 年生.博士,讲师.主要研究方向为物联网安全.

Huang Wenhua, born in 1980. Master, associate professor. Her main research interest is IoT security.

黄文华,1980 年生.硕士,副教授.主要研究方向为物联网安全.