doi:10.11835/j.issn.1000.582X.2024.08.008

面向电网安全的零信任动态访问控制

陈 岑[1],屈志昊[2],汪 明[3],魏兴慎[4],钱珂翔[5]
(1. 国网河南省电力公司电力科学研究院,郑州 450052; 2. 河海大学 计算机与软件学院,南京 210089;
3. 国家电网有限公司 北京 100031; 4. 国网电力科学研究院有限公司 南京 211102;
5. 国网智能电网研究院有限公司 北京 102209)

摘要:随着信息通信技术在电力信息系统中的不断发展和应用,电网的防护边界逐渐模糊,外部攻击和内部威胁日益严重,急需对电力系统信息资源的访问进行有效控制,确保数据安全。本文在电网二次系统安全防护总体框架的基础上,结合零信任安全机制,提出面向电网信息安全的零信任动态访问控制模型。该模型通过分析电网系统的访问主体属性与行为信息的特点,综合考虑威胁行为、滑动窗口、惩罚机制等因素对访问控制的影响,实现对访问主体信任值的持续评估和动态控制。仿真实验结果表明,增加推荐信任能合理兼顾主观和客观2种信任评价,使电网访问主体的信任值评估更准确。此外,针对外部威胁行为,信任评估引擎会迅速更新访问者的综合信任值,使非法主体无法获得系统的访问权限,具有更好的控制细粒度。

关键词:零信任;电网信息安全;动态访问控制;安全防护架构;信任值
中图分类号:TP309 **文献标志码:**A **文章编号:**1000-582X(2024)08-081-09

Zero trust dynamic access control for power grid security

CHEN Cen[1], *QU Zhihao*[2], *WANG Ming*[3], *WEI Xingshen*[4], *QIAN Kexiang*[5]
(1. State Grid Henan Electric Power Research Institute, Zhengzhou 450052, P. R. China; 2. College of Computer Science and Software Engineering, Hohai University, Nanjing 210089, P. R. China; 3. State Grid Corporation of China, Beijing 100031, P. R. China; 4. State Grid Electric Power Research Institute Co., Ltd., Nanjing 211102, P. R. China; 5. State Grid Smart Grid Research Institute Co., Ltd., Beijing 102209, P. R. China)

Abstract: With the continuous development and application of information and communication technology in power information system, the protection boundary of power grid is gradually blurred, and external attacks and internal threats are increasingly serious. It is urgent to carry out effective access control to the information resources of power system to ensure its data security. Based on the general security protection framework of power grid secondary system and zero-trust security mechanism, this paper proposes a zero-trust dynamic access control model for power grid information security. By analyzing the attributes of the access subject and the characteristics of the behavior information of the power grid system, the model comprehensively considers the influence of threatening behavior, sliding window, punishment mechanism and other factors on the access control, and realizes the continuous evaluation and dynamic control of the access subject trust value. The results of

收稿日期:2023-10-11
基金项目:国家电网科技项目(5108-202224046A-1-1-ZN)。
Supported by Technology Project of State Grid Co.,Ltd.(5108-202224046A-1-1-ZN).
作者简介:陈岑(1990—),女,硕士,主要从事通信与网络安全方向研究,(E-mail)1020065011@qq.com。

simulation experiments show that increasing the recommended trust can reasonably take into account both subjective and objective trust evaluations, which makes the assessment of the trust value of the access subject of the power grid more accurate. In addition, in response to external threat behaviors, the trust evaluation engine will rapidly update the comprehensive trust value of the visitor, making it impossible for illegal subjects to gain access to the system, with better fine-grained control.

Keywords: zero trust; power grid information security; dynamic access control; security protection framework; trust values

随着国家电网提出“三型两网,世界一流”的战略目标,工业智能电网的安全格局发生了质的变化,暴露在外的电网终端成为攻击者目标,电网安全威胁也随之出现。目前,中国电力系统的网络安全防护主要以边界隔离为主,总体遵循“安全分区、网络专用、横向隔离、纵向认证”的原则。但大规模终端设备和用户在电力物联网环境中的广泛接入增加了网络暴露,这对以边界隔离为特征的保护系统提出严重挑战。此外,电网终端设备和用户的认证、访问控制大多采用“一次认证、一次授权、长效”的方式,难以应对来自内部和外部设备以及拥有合法权利的用户威胁,用户的安全认证与信任度评估存在严重不足[1-4]。

为保护电网中的信息资源,研究人员积极开展融合零信任的系统安全防护研究。零信任网络以保护服务数据安全为目标,强调网络的一切实体均不可信,为电网终端的安全保护提供颠覆性的解决方案[5-8]。此外,零信任要求在每次访问或通信时都进行身份验证,而不仅仅是在用户登录时。对于电网中潜在的攻击行为,零信任框架强调实时检测和快速响应,及时检测潜在威胁并采取适当措施。文献[9]提出基于角色的访问控制(role-based access control,RBAC)和基于属性的访问控制(attribute-based access control,ABAC),前者根据各个角色的工作职能分配相应的权限并完成授权,但缺少环境上下文及对权限分配是静态、粗粒度的访问控制。后者以实体属性为基础进行授权决策,依据实体属性的变化动态更新访问控制决策,但其与RBAC相比,无法进行事前审计,一旦属性及规则过多,整个系统响应会很慢。文献[10]针对电网数据安全问题,提出分布式数据库细粒度访问控制,结合ABAC和RBAC的优势,但没考虑外部威胁行为对访问主体信任的影响。

综上,本文针对目前电力信息系统外部攻击与内部潜在威胁层出不穷的问题,在现有电力二次系统安全防护总体框架基础上,提出面向电网信息安全的零信任动态访问控制模型。该模型对用户、设备、环境和访问主体信任值进行持续评估和动态访问控制。此外,综合考虑威胁行为、滑动窗口、惩罚机制对访问主体信任值的影响,实时更新访问主体的信任阈值,降低数据安全风险隐患,提高电力系统的数据安全与业务安全。

1 面向电网安全的零信任安全防护架构

1.1 电网系统安全防护总体框架

电网二次系统安全防护总体框架如图1所示。其电力安全保护总体策略主要基于以下4个步骤[11]:1)安全分区:根据业务重要性和对主系统的影响,将电网安全保护平台划分为4个安全区域,通过加密和身份验证加强对实时控制系统等关键区域的保护;2)横向隔离:使用不同强度的安全隔离设备,对实时控制系统与各级电网管理信息系统之间进行有效的安全隔离,隔离强度应接近或达到物理隔离;3)网络专业化:调度数据网络内置于专用通道中,实现与其他数据网络的物理隔离,通过MPLS-VPN或IPsec-VPN技术,在专用网络中形成相互隔离的VPN,避免安全区域之间的垂直交叉;4)纵向认证:采用经过认证的加密和访问控制技术,实现生产控制数据的远程安全传输和垂直边界的安全保护。

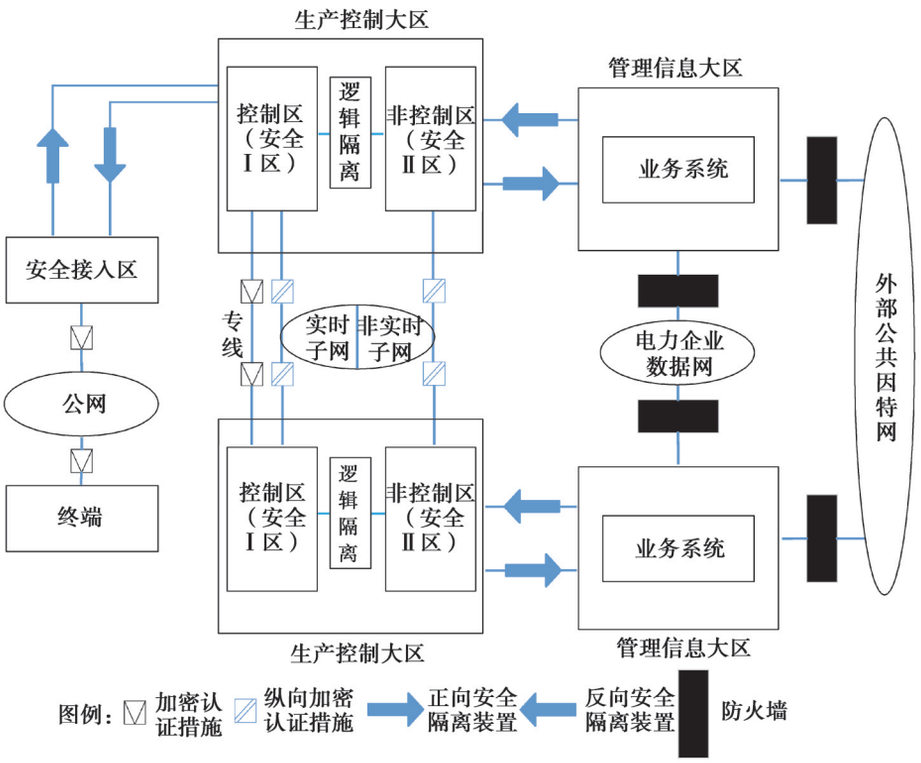

图 1　电网二次系统安全防护总体框架

Fig. 1　Overall framework of security protection for secondary system of power grid

1.2　零信任安全架构及安全机制

零信任安全架构[12-15]如图 2 所示,遵循“以身份为基础、以资源为核心、持续信任评估、动态访问控制”的构建原则,将整个零信任模型分为身份管理基础设施、数据平面、控制平面 3 层架构,实现访问主体到目标客体的端到端安全控制。

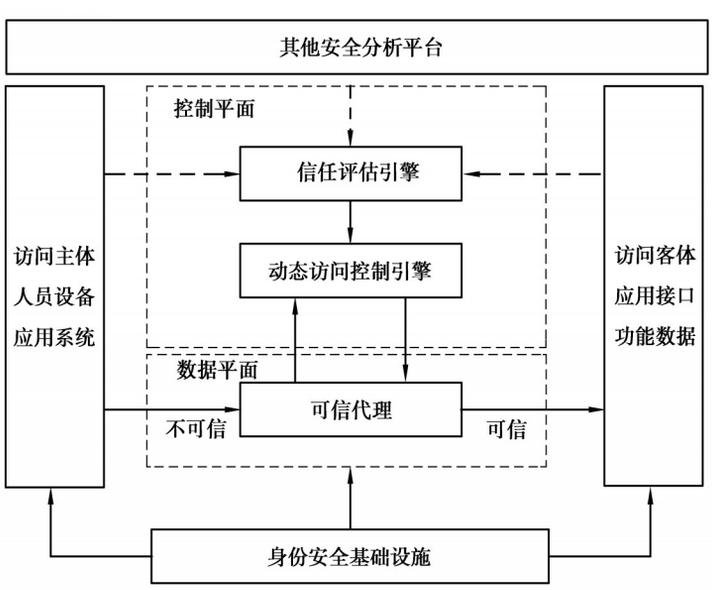

图 2　零信任安全架构

Fig. 2　Zero-trust security architecture

零信任的安全机制是以保护服务数据安全为目标,旨在解决“基于网络边界建立信任”这种固有问题。此外,它将网络防御的边界缩小到单个或更小的资源组,不再根据网络区域授予预设信任权限,使防护措施从传统网络层面扩展到应用层面。通常来说,零信任网络建立在以下 5 个基本假定之上:

1)网络无时无刻不处于危险环境中;

2)网络自始至终存在外部或内部威胁;

3)网络位置不能决定网络的可信度;

4)所有设备、用户和网络流量都应经过认证和授权;

5)安全策略必须是动态的,基于尽可能多的数据源进行计算。

相比传统的网络边界防护对象,零信任网络将威胁源从网络外部延伸至网络内部,将网络中一切行为实体视为不可信,将边界模型中的“信任但验证”转换到“从不信任,始终验证”模式。

1.3 融合零信任的电网信息安全防御框架

为了保障电网信息安全,本文在电网二次系统安全防护总体框架基础上,结合零信任安全机制,构建了面向电网信息安全的零信任安全防御框架[16-18]。如图3所示,该架构主要包括典型终端场景、电力信息系统、安全访问控制平台及可信访问代理等。安全访问控制区域的多源数据汇总平台主要由电力终端感知系统、用户设备终端和外部应用组成,主要对系统、终端设备等进行数据收集、过滤、提取、汇总和标准化处理,为信任评估模块提供可信评价的原始数据。智能信任评估平台和动态访问控制平台相结合,基于多元数据汇总平台和可信访问代理上报的感知信息和访问日志信息,对访问主体和访问请求的信任级别和风险程度进行评价。可信访问代理是1个策略执行的发起者,通过接收典型终端场景发来的业务进行安全访问,将可靠的访问日志信息上报给智能信任评估平台进行评估。

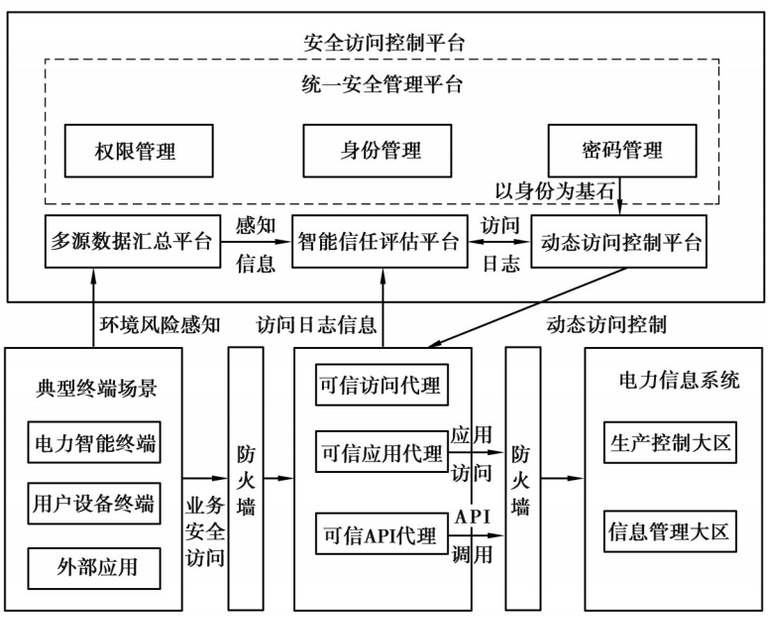

图3 基于零信任的电网信息安全防御框架

Fig. 3 Grid information security defense framework based on zero trust

2 面向电网安全的零信任动态访问控制模型

在面向电网信息安全的零信任防御框架基础上,针对电力信息系统的边界模糊、难以进行持续信任评估等问题,提出面向电网安全的零信任动态访问控制模型,实现对访问主体信任值的持续评估和信任阈值的动态调整,提高电网系统的安全性。

2.1 访问主体的信任控制模型

根据图3可知,一些外部的典型终端场景如电力智能终端、外部应用等,这些应用要访问电力信息系统里面的资源,满足可信访问代理、可信API代理等一些信任需求,而这些外部应用的信任值计算主要依靠信任控制平台和访问控制平台等信任评估设备,给可信访问代理提供信任值判断依据,判断是否满足信任需求。在此过程中,信任控制平台等设备是关乎外部应用能否访问电力资源的直接因素,提出访问主体的信任控制模型,如图4所示。系统通过给定权限阈值来限制访问主体的权限范围,而权限阈值也会随着系统运行

自动调整范围。综合信任值依据用户、设备、环境的基础信任值以及推荐信任值4个维度进行计算,每次发起访问前需要对访问主体重新进行信任评估。在此基础上,每次会话中访问主体以及各维度的权限仅在当前会话中有效,而权限获取的依据是访问主体的综合信任值以及各维度的独立信任值。此外,在该控制模型中,访问主体(Access_sub)不是一直不变,访问主体的权限 W 也不是一直有效。在1次会话中,访问主体依据当前信任值 $G(S)$ 获取相应的权限 W_1,当访问结束后,访问主体的信任值 $G(S)$ 便不再可用,随之访问主体也不再拥有之前的权限 W_1,只有重新经过信任引擎评估,才可以获取对应权限 W_1。当访问主体的环境、设备等发生变化时,信任值降低,如果执行相同请求将会被拒绝,实现细粒度的访问控制。

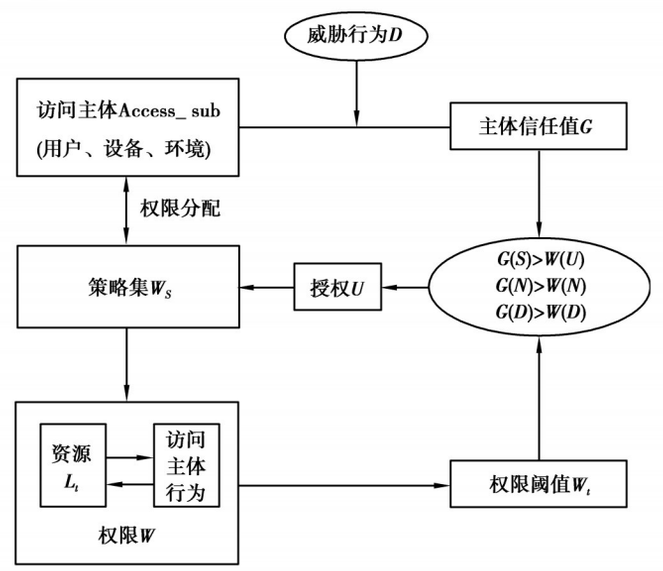

图4　访问主体的信任控制模型

Fig. 4　Trust control model of access subject

2.2　访问主体的信任度量指标

访问主体的信任度量指标如图5所示,主要包含用户、设备、环境等3种不同的信任评估指标。其中,用户信任评估指标包括身份信息和认证信息2种不同的信任依据;设备信任评估指标包括标识信息和设备信息2种不同的信任依据;环境信任评估指标包括网络状态、资源状态和访问次数3种不同的信任依据。此外,为保证系统内部安全,兼顾可能存在的威胁行为,使系统可以给出准确的信任值,迅速拒绝危险请求。

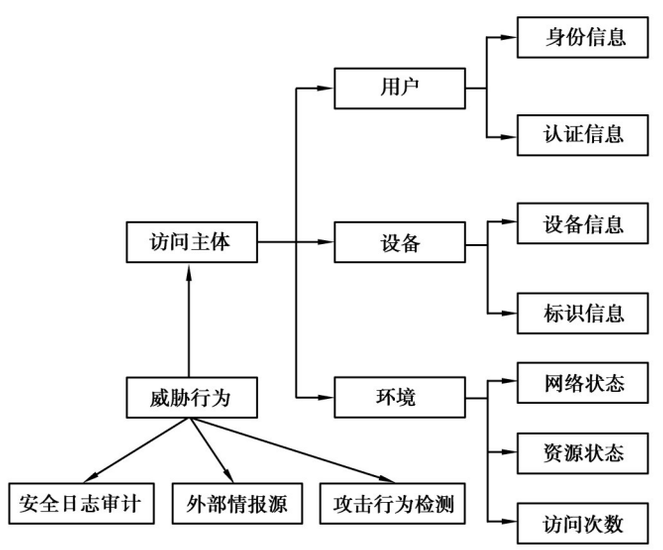

图5　访问主体度量指标

Fig. 5　Access subject metrics

2.3 访问主体的信任值计算

在提出的访问主体信任控制模型和信任度量指标基础上，设计基于访问主体信任值和权限阈值的信任算法，只有当综合信任值满足权限阈值要求时，访问主体才能获得系统给予的访问权限。此外，为了保证数据的实时性和防止恶意节点非法访问，引入滑动窗口机制和惩罚机制。

2.3.1 滑动窗口机制

零信任的安全机制要求对网络中一切行为实体视为不可信，每当访问主体发起访问请求时都要重新计算当前的信任值，故引入滑动窗口机制来保证信任值计算的实时性。

图6为滑动窗口模型，将1个大小为n的窗口分为若干单位窗口，每交互1次，窗口移动1个单位，窗口内数据的权重也发生变化，直到离开这个窗口，失去信任评估价值。窗口内数据权重变化的衰减函数为

$$A(z)=\begin{cases}1-\beta, & z=n,\\ A(z-1)+1/n, & z<n,\end{cases} \tag{1}$$

式中：β是衰减范围因子，取值为任意小的正数；z为访问主体历史记录和当前访问记录的距离；n为滑动窗口大小。

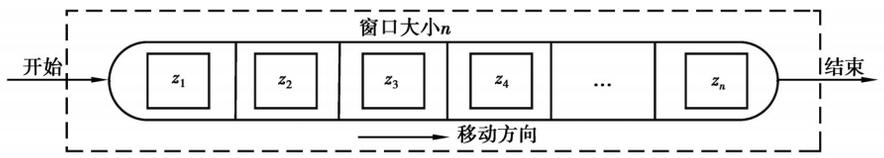

图6 滑动窗口模型

Fig. 6 Model of a sliding window

2.3.2 惩罚机制

为防止恶意节点对电网中的数据信息进行非法获取，本节给出惩罚机制。当电网中的检测系统检测到非法操作后，将对访问主体中的用户、设备及环境3个度量指标增加1个信任值上限，限制恶意节点后续非法获取访问权限的行为，信任值上限由式(2)给出

$$X=F\cdot\sin\left(\frac{k}{2K}\cdot\pi\right)\cdot X', \tag{2}$$

式中：X'为访问主体的信任上限；F为惩罚系数，系数越小，惩罚力度越大；$k\in\{1,2,3,4,5\}$为当前非法访问对应的等级；K为非法操作等级的数量。当恶意节点进行非法操作时，访问主体的信任值会有影响，多次发生同样的非法行为后对相应的信任阈值进行不断更新。

2.3.3 访问主体综合信任值计算

基于访问控制模型和度量指标计算用户信任值时，一般有2种方法：1)根据以往交互记录得到的信任值进行直接判断，也叫直接信任值或基础信任值；2)在直接判断的基础上，参考其他节点的推荐信任。而1个完整的信任机制应该兼顾主观和客观2种信任机制。

访问主体基础信任值计算流程如下：将访问主体的用户、设备和环境3个不同的基础信任指标用集合v表示，将3者各自的信任度量指标转化为对应的信任等级值，用集合l_v表示3者不同基础信任等级值，访问主体3个不同基础信任值的计算公式如下

$$P_v(z)=\frac{1}{1+\mathrm{e}^{-\sum_{l\in l_v}a_l\times z_l\times A(z)}}, \tag{3}$$

式中：z_l为各个度量指标所含的信任值；a_l为各个度量指标的影响因子，即所占权重；$A(z)$为衰减因子。

访问主体推荐信任值的计算流程如下：将访问主体的用户、设备和环境3个不同的推荐信任指标用集合t表示，并将3者各自的信任度量指标转化为对应的信任等级值，用集合R_t表示3者不同推荐信任等级值，则访问主体3个推荐信任值的计算公式如下

$$V_t(z)=\frac{\sum_{R\in R_t} b_R\times c_R\times h_R}{\sum_{R\in R_t} b_R\times c_R}, \tag{4}$$

式中:b_R为各个度量指标所推荐的信任度;c_R为推荐的可信度的等级,$c_R\in(1,2,3,4,5)$;h_R为推荐者的推荐能力,$R\in R_t$。故用户、设备和环境3者各自的综合信任值如下

$$g_n(z)=\lambda\times P_v(z)+(1-\lambda)\times V_t(z), \tag{5}$$

式中:λ为基础信任值所占比例,$(1-\lambda)$为推荐信任值所占比例。对$g_n(z)$进行加权求和后,得到访问主体的综合信任值

$$G(z)=\sum_{n=1}^{3} t_n\times g_n(z), \tag{6}$$

式中,t_n为访问主体中用户、设备和环境3者所占比例,其和为1。此外,考虑威胁行为对访问主体信任值的影响,可进一步得到访问主体的综合信任值

$$G'(z)=\prod k_n\times\sum_{n=1}^{3} t_n\times g_n(z), \tag{7}$$

式中,k_n表示威胁行为的影响因子。

当访问主体对电网中的数据进行请求时,电网中的信任评估引擎将根据各个信任评估度量指标计算出访问主体的综合信任值,只有信任值大于系统给定的权限阈值时,访问主体才能对目标资源进行正常的操作获取。

3　仿真及参数设定

为了验证所提零信任动态访问控制模型的有效性,本节对访问主体在访问过程中的信任值变化进行仿真,验证所提模型能否实现动态细粒度控制,仿真主要依据提出的访问主体的信任值计算方法。选取访问主体中各个信任度量指标作为信任计算的依据,确定各个度量指标的基础信任值范围、推荐信任值范围、权重和影响因子,实验参数如表1所示。

表1　访问主体的参数设置

Table 1　Parameter settings for access subject

度量主体	信任评估指标	基础信任值范围z_l	推荐信任值范围b_R	权重t_n	影响因子a_l
用户	身份信息	[0,1]	[0.7,1]	0.5	1
	认证信息	[0,0.5]	[0.7,1]		
设备	设备信息	[0,1]	[0.5,0.7)	0.3	1
	标识信息	[0,0.5]	[0.5,0.7)		
环境	网络状态	[0,1]	[0,0.5)	0.2	1
	资源状态	[0,0.6]	[0,0.5)		
	访问次数	[0,0.5]	[0,0.5)		

图7给出了用户、设备、环境和访问主体度量指标的个数和综合信任值关系。随着度量指标个数的增多,不同度量主体的信任值增长趋势不同,这种差异主要是由不同权重造成的。其中,设备和环境的综合信任值上升得较为平缓且信任上限较低,这是因为2者在访问主体中所占比重较小。此外,在度量指标个数达到10个后,用户、设备、环境和访问主体的综合信任值基本稳定,这反映了任何访问者在获取更高信任权限时的困难程度会加剧,系统不是无条件地开放所有访问入口,访问者的信任值总会是有限定的阈值。

图8给出了威胁行为对访问主体信任值的影响。当系统在度量指标个数为10时检测到相应的威胁行为后,信任评估引擎会迅速做出反应,评判各威胁行为的影响因子k_n,修改访问者的综合信任值。当系统后续持续检测到该威胁行为的存在,会不断要求信任评估引擎更新访问者的综合信任值,直至信任值为0,使非法

主体无法获得系统的访问权限。

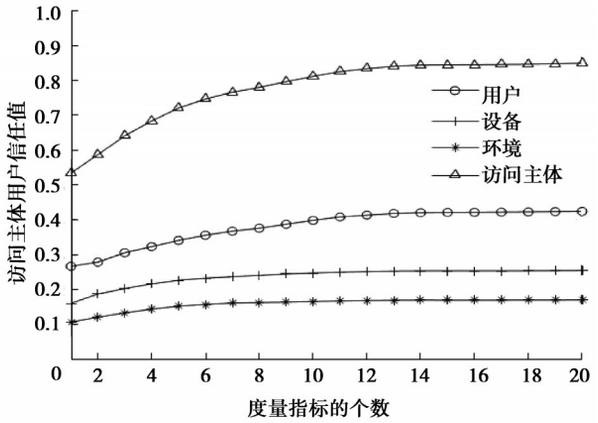

图7 度量指标对访问信任值的影响

Fig. 7 The impact of metrics on access trust values

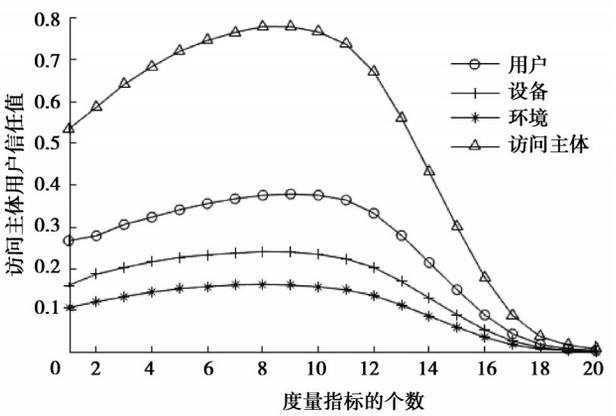

图8 威胁行为对访问信任值的影响

Fig. 8 The impact of threat behavior on access trust values

图9为增加推荐信任对访问主体信任的影响。随着度量指标个数增多,2者的曲线增长趋势有明显不同。单一的基础信任缺乏推荐信任,系统评判访问者信任值大小时,根据以往交互记录得到的信任值进行直接判断,故访问主体的信任值增加较快,且信任上限会随着度量指标个数的增多逐渐接近1。若在直接判断的基础上参考其他节点的推荐信任,则系统每次对访问者进行信任值评判时,会兼顾以往交互记录和其他节点的推荐信任,故增长速度较缓且信任上限达不到临界点1。综上,增加推荐信任能合理兼顾主观和客观2种信任评价,使电网访问主体的信任值评估更加准确。

图10给出了惩罚机制对信任阈值的影响。假定访问主体的初始信任阈值为0.8,惩罚衰减系数为1,当访问主体连续发生恶意非法访问时,获得的信任阈值将急速下降,超过6次非法访问时,它能获得的信任阈值几乎为0,任何访问者都无法获得访问权限,防止恶意非法用户无限制地获取系统信任权限,有效保护系统的安全性能。

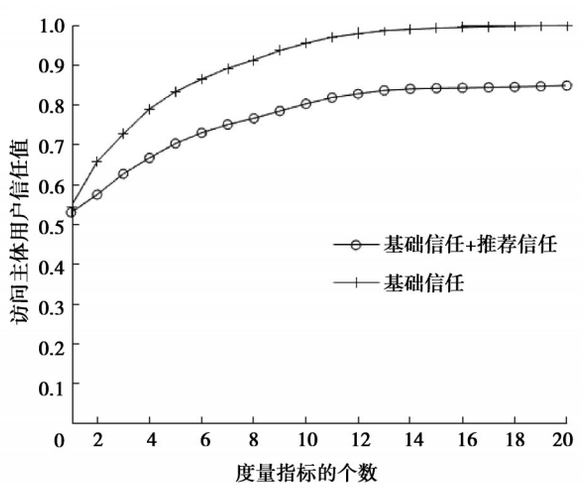

图9 推荐信任对主体信任的影响

Fig. 9 The impact of recommendation trust on the subject trust

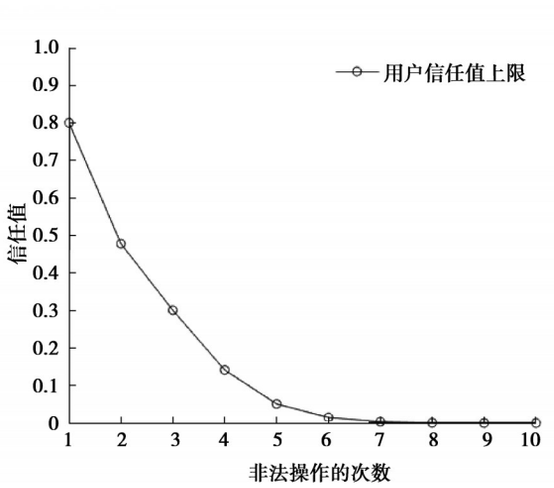

图10 惩罚机制对信任阈值的影响

Fig. 10 The impact of punishment mechanism on trust threshold values

4 总 结

针对目前电力信息系统终端开放互动、电网防护边界模糊、传统边界安全防护体系难以保证电力信息系统终端安全接入的问题,本文在融合零信任的电网信息安全防御框架基础上,提出动态访问控制模型。每当

访问者获取任意设备权限时,需要经过可靠的信任评估,且只有当获取的信任值大于当前设备的信任阈值时,才能进行访问。此外,为保证数据的实时性和防止恶意节点的非法访问,引入滑动窗口机制惩罚机制以实现对访问主体信任值的持续评估和动态控制,仿真结果验证了所提访问控制模型的可行性和有效性。

参考文献

[1] Gao P, Yang R X, Shi C C, et al. Research on security protection technology system of power internet of things[C]//2019 IEEE 8th Joint International Information Technology and Artificial Intelligence Conference (ITAIC). Chongqing, China: IEEE, 2019: 1772-1776.

[2] Khurana H, Hadley M, Lu N, et al. Smart-grid security issues[J]. IEEE Security and Privacy, 2010, 8(1): 81-85.

[3] Xie M. Smart Grid borderless access control technology based on network security situational awareness[J]. Energy Reports, 2022, 8: 415-423.

[4] Salmeron J, Wood K, Baldick R. Analysis of electric grid security under terrorist threat[J]. IEEE Transactions on Power Systems, 2004, 19(2): 905-912.

[5] Annamalai A, Kumar V S, Baptist A L J. Augmenting zero trust network architecture to enhance security in virtual power plants [J]. Energy Reports, 2022, 8: 1309-1320.

[6] Bertino E. Zero trust architecture: does it help?[J]. IEEE Security & Privacy, 2021, 19(5): 95-96.

[7] Shi C C, Fei J X, Zhang X J, et al. Continuous trust evaluation of power equipment and users based on risk measurement[J]. Scientific Programming, 2020: 8895804.

[8] Yang T, Zhu L, Peng R X. Fine-grained big data security method based on zero trust model[C]//2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS). Singapore：IEEE, 2018: 1040-1045.

[9] 诸葛程晨, 王群, 刘家银, 等. 零信任网络综述[J]. 计算机工程与应用, 2022, 58(22): 12-29.
Zhuge C C, Wang Q, Liu J Y, et al. Survey of zero trust network[J]. Computer Engineering and Applications, 2022, 58(22): 12-29.(in Chinese)

[10] 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.
Huang J, Yu R C, Mao D. Distributed database fine-grained access control based on zero trust in the power internet of things[J]. Journal of Information Security Research, 2021, 7(6): 535-542.(in Chinese)

[11] Li X M, Huang R, Liu J, et al. System construction of protection solutions of secondary power system in power plant based on information security[C]//2009 Asia-Pacific Power and Energy Engineering Conference. Wuhan, China: IEEE, 2009: 1-4.

[12] Adahman Z, Malik A W, Anwar Z. An analysis of zero-trust architecture and its cost-effectiveness for organizational security [J]. Computers & Security, 2022, 122: 102911.

[13] Syed N F, Shah S W, Shaghaghi A, et al. Zero trust architecture: a comprehensive survey[J]. IEEE Access, 2022, 10: 57143-57179.

[14] YU S B, LI C Y, Ji Z. Application of zero trust architecture in network trust system[J]. Communications Technology, 2020, 10: 2533.

[15] Phiayura P, Teerakanok S. A comprehensive framework for migrating to zero trust architecture[J]. IEEE Access, 2023, 11: 19487-19511.

[16] Zeng R, Li N G, Zhou X M, et al. Building a zero-trust security protection system in the environment of the power Internet of Things[C]//2021 2nd International Seminar on Artificial Intelligence, Networking and Information Technology. Shanghai, China: IEEE, 2021: 557-560.

[17] Gao P, Yan L C, Chen Z Y, et al. Research on zero-trust based network security protection for power Internet of Things[C]// 2021 IEEE 4th International Conference on Automation, Electronics and Electrical Engineering. Shenyang, China: IEEE, 2021: 458-461.

[18] Wu K H, Shi J, Guo Z M, et al. Research on security strategy of power Internet of Things devices based on zero-trust[C]//2021 International Conference on Computer Engineering and Application (ICCEA). Kunming, China: IEEE, 2021: 79-83.

（编辑　侯　湘）