DOI:10.11784/tdxbz202310009

虚拟电厂异构接入终端轻量级信任评价方法

盆海波[1]，蔡绍堂[2]，吴维农[2]，胡　骏[3]，董　峰[1]，杨　挺[1]
（1. 天津大学电气自动化与信息工程学院，天津 300072；2. 国网重庆市电力公司信息通信分公司，重庆 401121；
3. 湖南医药学院医学人文与信息管理学院，怀化 418000）

摘　要：针对多类型异构终端广泛接入造成虚拟电厂（VPP）网络攻击接口激增致使传统安全防护方法难以抵御网络内部攻击的能力，无法实现终端持续高可靠接入的问题，本文提出一种基于私有链的 VPP 异构接入终端轻量级信任评价方法，实现 VPP 异构终端安全、准确和高效的信任评价. 首先，通过研究各类异构接入终端交互特性，建立面向 VPP 各类异构终端的虚拟映射机制，提出基于信息熵的 VPP 异构终端多因素信任评价方法，综合考虑终端通信行为、数据质量和传输速率 3 种信任因素，采用信息熵对各类信任值进行融合加权计算，避免信任权重的主观分配，提升 VPP 异构终端信任评价精度；其次，提出一种基于私有链的海量异构终端信任参数共识方法，设计全节点共识验证机制实现对上链信任参数进行可靠性筛选，有效验证信任参数上链的合法性与真实性，并采用 Merkle 山脉逐层构建信任参数根哈希值，改进传统私有链区块结构，降低信任参数存储和计算复杂度，实现信任参数的轻量化存储与计算. 最后，构建了包含风电场、光伏、储能以及各类异构终端的 10 kV 虚拟电厂接入终端信任评价仿真算例. 仿真结果表明，较现有信任评估方法，本文所提方法可有效抵御诽谤、ON-OFF 等网络内部攻击，实现了异构终端安全、精准和轻量的信任评价.

关键词：虚拟电厂；异构终端；轻量级；私有链；信任评价
中图分类号：TM732　　**文献标志码**：A　　**文章编号**：0493-2137（2025）03-0260-14

Lightweight Trust Evaluation Method for Virtual Power Plant Heterogeneous Access Terminals

Pen Haibo[1]，Cai Shaotang[2]，Wu Weinong[2]，Hu Jun[3]，Dong Feng[1]，Yang Ting[1]
（1. School of Electrical and Information Engineering，Tianjin University，Tianjin 300072，China；
2. Information and Communication Branch，State Grid Chongqing Electric Power Company，Chongqing 401121，China；
3. School of Medical Humanities and Information Management，Hunan University of Medicine，Huaihua 418000，China）

Abstract：In response to the widespread access of various types of heterogeneous terminals causing a sharp increase in attack interfaces in virtual power plant（VPP），traditional security methods struggle to defend against internal network attacks，leading to unreliable and discontinuous terminal access. To address this issue，this paper proposes a lightweight trust evaluation method for VPP heterogeneous access terminals based on private blockchain technology，aiming to achieve secure，accurate，and efficient trust evaluation of these terminals. First，by analyzing the interaction characteristics of various heterogeneous access terminals，a virtual mapping mechanism is established for various types of heterogeneous terminals in the VPP. Then，a multi-factor trust evaluation method based on information entropy is proposed. This method considers three trust factors：terminal communication behavior，data quality，and transmission rate. Information entropy is used to fuse and weigh the various trust values，thereby avoiding subjective allocation of trust weights and improving the accuracy of trust evaluation for heterogeneous terminals. Second，a trust

收稿日期：2023-10-09；**修回日期**：2024-07-01.
作者简介：盆海波（1989—　），男，博士，讲师，penhaibo@tju.edu.cn.
通信作者：蔡绍堂，caishaotang1992@tju.edu.cn.
基金项目：国家重点研发计划资助项目（2022YFB2403800）；中国博士后科学基金资助项目（2019M651037）；天津市自然科学基金资助项目（19JCQNJC06000）.
Supported by the National Key Research and Development Program of China（No. 2022YFB2403800），the China Postdoctoral Science Foundation（No. 2019M651037），the Natural Science Foundation of Tianjin，China（No. 19JCQNJC06000）.

parameter consensus method based on private block-chain is introduced for managing massive heterogeneous terminals. This method achieves reliable screening of on-chain trust parameters by designing a full-node consensus verification mechanism, effectively verifying the legitimacy and authenticity of trust parameters. The Merkle mountain is used to construct root Hash for trust parameters layer by layer, improving the traditional private block-chain block structure. This approach reduces the complexity of trust parameter storage and calculation, achieving lightweight storage and calculation of trust parameters. Finally, the trust evaluation performance under various types of terminal access is analyzed through simulations in a 10 kV VPP environment consisting of a wind farm, a photo-voltaic device, an energy storage system, and various heterogeneous terminals. The simulation results show that the proposed method outperforms existing trust evaluation methods, effectively resisting defamation and ON-OFF internal network attacks while achieving secure, accurate, and lightweight trust evaluation of heterogeneous terminals.

Keywords: virtual power plant (VPP); heterogeneous terminal; lightweight; private blockchain; trust evaluation

虚拟电厂(virtual power plant, VPP)是一个通过云计算、人工智能、区块链等智能化技术将多个分布式能源(distributed energy resources, DERs)和用户侧负荷进行聚合,形成的统一虚拟能源发电和管理平台[1-3]. 作为一种新型的电力供应模式,规模化 VPP 中电力终端、智能电子设备和网络外设等终端,实现了对分散的、多样化的分布式能源资源进行集成和协调. 然而,海量终端接入使得 VPP 网络攻击接口激增,攻击者常利用暴露于外网和处于网络底层的攻击接口实施身份仿冒、密钥捕获、虚假数据注入等网络攻击,破坏 VPP 的可用性和完整性,给 VPP 系统带来巨大破坏[4-6]. 因此,实现各类分布终端的安全接入与管理对 VPP 的安全稳定运行十分重要. 目前,VPP 终端安全接入与管理方法主要包括身份认证、可信接入与零信任机制.

身份认证作为 VPP 终端安全接入的第 1 道屏障,只有通过认证的设备才能接入 VPP. 文献[7]提出基于属性加密(attribute-based encryption, ABE)的终端身份认证方案,通过结合云边协同计算架构,采用 ABE 实现终端细粒度访问控制和安全身份认证,适用于资源受限环境下的终端身份认证. 文献[8]提出基于隐私保护计算的终端身份认证方案,实现电力终端在隐私敏感场景下电力终端身份认证. 文献[9]提出了基于多因素认证的电力终端身份认证方法,采用密码、生物特征和物理证明等多种因素进行身份认证,提高了可信度和安全性. 虽然双重认证或者多因素认证方式相比单因素方法更为安全,但是其认证方法较为复杂,增加了认证的计算开销. 上述研究仅针对终端首次接入系统的安全认证. 在 VPP 终端层运营管理中,传统的身份认证方法虽然可确保外接终端的安全可信,但是一旦终端接入系统后无法对其进行持续认证管理.

为了弥补身份认证的局限性,可信接入技术的引入有效地提高终端持续安全接入水平,逐渐被应用于电力终端安全管理[10-12]. 面向 VPP 的可信接入是指综合利用身份认证、密钥管理和访问控制等技术,确保只有经过授权的用户和设备才能访问 VPP 系统,构建平台和终端之间的安全连接,防止恶意攻击和数据泄露等安全问题. 可信接入的关键在于建立起完整的认证和授权机制,包括网络访问层设计、完整性评估层设计和完整性度量层设计. 针对电力终端的可信接入研究方面,文献[13]提出了分层信任管理方案. 该方案包括终端层、用户层和应用层的 3 级信任管理模型,并通过构建信任评估算法来评估设备和用户的可信度,从而可以有效地防止未经授权的访问. 文献[14]提出了基于属性证书和区块链技术的可信接入控制方案. 该方案使用属性证书来验证用户的身份,并使用区块链技术来确保终端接入控制信息的完整性和真实性,可以有效地防止各种类型的攻击. 但是,可信接入技术需要在终端侧嵌入可信模块以支撑可信计算,这增加了终端接入的成本与复杂度.

零信任机制作为一种新型的安全管理理念,对接入终端采取“持续验证,永不信任”的接入管理. 与身份认证和可信接入终端接入与管理方法相比,零信任机制框架中接入终端对象的信任与其是否接入系统无关,默认所有对象都是不可信的,并通过动态持续身份验证及信任评估环节有效解决系统内部安全威胁. 文献[15]提出基于安全断言标记语言和开放授权协议的电网终端设备零信任安全架构及模型,该架构使用零信任方法对联网设备的访问请求进行身份验证和授权. 文献[16-17]聚焦面向电网设备的安全问题,提出了基于零信任机制的安全管理方案,用于保护智能电网免受网络攻击,融合身份验证、授权和加密技术,确保智能电网基础设施的安全,并采用软件定义网络(software defined network, SDN)技术和 OpenFlow 协议实现了应用验证. 零信任机制为智能电网提供了高效且安全的防御措施,可有效应对系统内外多种网络攻击. 但是,目前零信任机制框架中各

类终端接入控制与智能化管理技术仍处于初步研究阶段，在多因素身份认证、持续信任评估、动态访问控制、智能风险分析等方法研究以及工程应用亟需开展技术攻关[18-20].

然而，上述成果仅针对 VPP 终端层特定场景的研究中仍然存在一些问题和挑战，如异构终端网络的持续高可靠接入问题仍无法解决，针对网络内部发起的网络攻击无法有效抵御等，需要建立 VPP 异构终端信任评估网络，研究更加安全、精准和轻量的终端信任评价方法，有效抵御 VPP 场景的高级持续性威胁. 因此，本文提出一种基于私有链的 VPP 异构接入终端轻量信任评价方法，实现了异构终端安全、准确和高效的信任评价. 首先，建立 VPP 终端虚拟映射模型，提出基于信息熵的 VPP 异构终端多因素信任评价方法，采用各类信任值的熵权对终端完整信任进行融合，提升信任评价精度；其次，提出一种基于私有链的异构终端信任参数共识方法，设计 VPP 终端信任参数共识验证机制，对上链信任参数进行可靠性筛选，采用 Merkle 山脉逐层构建信任参数根哈希值，改进传统私有链区块结构，解决了各终端信任参数的轻量化存储和计算，实现了各类终端的持续高可靠接入.

1 虚拟电厂各类型接入终端的虚拟映射

VPP 各类终端由多个厂商制造，存在不同的协议和接口，这不仅增加了设备之间互联互通的复杂度，还增加了的网络内部安全风险. VPP 中智能电表、IED、网络外设等终端易遭受诽谤攻击、选择转发攻击、共谋攻击等网络内部攻击手段的入侵[21]. 为实现 VPP 各类终端信任的精准评价，本文通过对 VPP 中各类型终端的交互特性进行分析，并根据 VPP 通信网络建立各类接入终端的虚拟映射模型，如图 1 所示.

VPP 通过已有电力通信网络资源对聚合资源进行高频数据采集和传输，网络中有线和无线传输方式并存，通信方式多样. 本文应用文献[22]所提方法对 VPP 通信网络进行分层分区，具体包括直接服务用户的本地通信，以及服务 VPP 管控平台和本地终端信息上传的远程通信. 可以看出，本地网络主从终端配比高，终端间连接度低，且多采用半双工直连传输方式，这为终端推荐信任和间接信任评价带来了考验. 远程通信具备组网方式灵活、多采用全双工互联通信传输和终端覆盖范围广等特点，有利于 VPP 终端的信任评价. 但远程通信支持电力专网和电信运营商公网的混合组网模式也使得该网络终端遭受网络攻击的风险增加，这对终端信任评价的准确性提出了更高的要求. 本文通过 VPP 各类接入终端的虚拟映射，将本地通信和远程通信功能从硬件中抽象出来，实现各类 VPP 业务终端的统一映射管理和虚拟融合，即使应用不同的通信协议或者媒介也可以无缝对接，这为后续 VPP 终端信任建模奠定了基础.

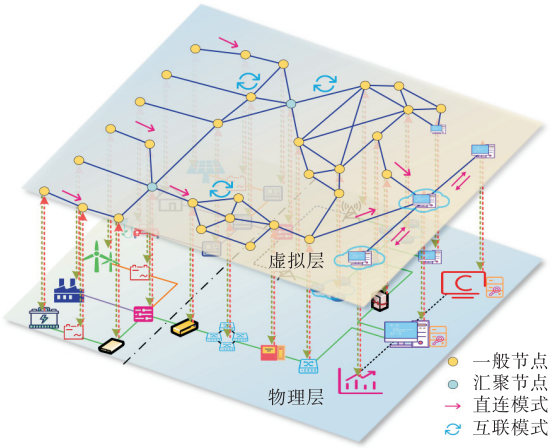

图 1 虚拟电厂各类接入终端的虚拟映射

Fig.1 Virtual mapping of various access terminals of the VPP

2 基于信息熵的 VPP 异构终端多因素信任评价方法

2.1 多因素信任评价模型

基于终端虚拟映射机制，虚拟电厂具有层次结构复杂、节点类型多、通信方式多样、数据传输量大、安全可靠性要求高等特点都为终端信任评价加大难度. 结合传统信任评价工作机制和 VPP 终端交互特性，同时考虑到信任评价模型具有安全性、准确性及轻量性的本质需求特征，进而基于各终端实体发生数据交互行为和对数据的处理行为，使用基于行为的信任参数进行采集、拟合、计算等操作，求取终端在各种评价方式的信任表现. 本文结合 VPP 终端交互过程中通信行为数据、数据质量信息以及传输速率信息建立了直接信任评价模型. 在此基础上，考虑直接信任无法完全实现 VPP 网络异构通信模式的终端信任评价，本文定义直接信任评价、推荐信任评价和间接信任评价并综合进行多维信任计算，通过信息熵实现多维信任评价值的自适应聚合，对终端进行客观的信任评价. 基于信息熵的 VPP 异构终端信任评价方法如图 2 所示.

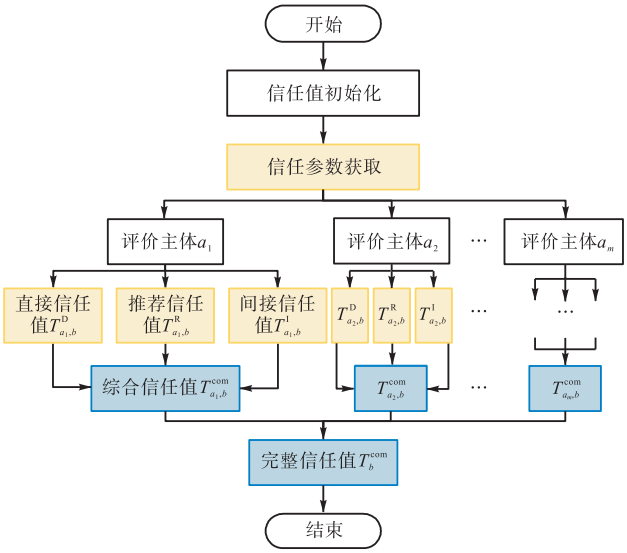

图 2　基于信息熵的 VPP 异构终端信任评价方法

Fig.2　Heterogeneous terminal trust evaluation method for the VPP based on information entropy

2.1.1　VPP 终端信任值定义

定义 1　信任评价过程中参与终端评价的终端被称为评价主体，被评价的终端为评价客体，且评价主体 a 对评价客体 b 的综合信任值 $T_{a,b}^{\mathrm{com}}$ 属于 0 ~ 1 间的连续实数.

$$T_{a,b}^{\mathrm{com}} \in \left\{ T_{a,b}^{\mathrm{com}} \in \mathbb{R} \middle| 0 \leqslant T_{a,b}^{\mathrm{com}} \leqslant 1 \right\} \tag{1}$$

式中 $T_{a,b}^{\mathrm{com}}$ 为终端综合信任值，当信任值 $T_{a,b}^{\mathrm{com}}$ 为 1 时该终端被完全信任，当信任值为 0 时，该终端为完全不可信终端.

2.1.2　直接信任评价

考虑 VPP 主从终端配比高，终端的直连通信场景广泛，该场景涉及到两终端间信息的直接交互，无法满足推荐信任和间接信任的评价条件. 为完善终端间的直接信任评价方法，对终端直接信任评价的 3 种信任影响因素进行建模，量化终端的直接信任值. 其中，参与直接信任评价的各类信任参数均从私有区块链中获取.

定义 2　对于建立直接通信链路的两交互终端，评价主体 a 基于终端间交互过程中的通信行为、数据质量和传输速率 3 种直接交互信息对评价客体 b 进行信任估计作为直接信任评价，记为 $T_{a,b}^{\mathrm{D}}$.

(1) 基于通信行为的直接信任值：该信任值为评价主体 s 对评价客体 o 行为的主观期望，本文中通过两个终端之间信誉的概率分布的统计期望来获得. 信誉分布是一个抽象概念，无法用物理量进行描述，本文考虑 VPP 终端数据类型包括负荷、电量等连续实数值，采用 Beta 分布对终端信誉分布进行拟合[23]. 假设终端的信誉为 b^{T}，终端间是否交互成功的行为的观测值为 o^{T}，则基于贝叶斯(Bayes)方程给定观测的信誉概率为

$$P^{\mathrm{B}}(b^{\mathrm{T}} \mid o^{\mathrm{T}}) = \frac{P(b^{\mathrm{T}} \mid o^{\mathrm{T}}) P(b^{\mathrm{T}})}{N^{\mathrm{C}}} \tag{2}$$

式中 N^{C} 为归一化常数.

进而，基于看门狗机制的输出 $D_{a,b}^{\mathrm{WG}}$ 对终端信誉值进行更新. 评价主体 a 对评价客体 b 更新后的信誉 $R_{a,b}^{\mathrm{new}}$ 表示为

$$R_{a,b}^{\mathrm{new}} = \frac{P^{\mathrm{B}}\left(D_{a,b}^{\mathrm{WG}} \mid R_{a,b}^{\mathrm{new}}\right) R_{a,b}^{\mathrm{new}}}{\sum P^{\mathrm{B}}\left(D_{a,b}^{\mathrm{WG}} \mid R_{a,b}^{\mathrm{new}}\right) R_{a,b}^{\mathrm{new}}} \tag{3}$$

然后，采用 Beta 分布对信誉分布进行拟合，其概率密度函数表示为

$$P^{\mathrm{Beta}}(x^{\mathrm{C}}) = \frac{\Gamma(\alpha^{\mathrm{B}} + \beta^{\mathrm{B}})}{\Gamma(\alpha^{\mathrm{B}}) + \Gamma(\beta^{\mathrm{B}})} (x^{\mathrm{C}})^{\alpha^{\mathrm{B}}-1} (1 - x^{\mathrm{C}})^{\beta^{\mathrm{B}}-1} \tag{4}$$

式中：$P^{\mathrm{Beta}}(\cdot)$ 为概率密度函数；α^{B} 和 β^{B} 为 Beta 分布参数，$\alpha^{\mathrm{B}} \geqslant 0$，$\beta^{\mathrm{B}} \geqslant 0$；$x^{\mathrm{C}}$ 为关于通信的随机变量，$0 \leqslant x^{\mathrm{C}} \leqslant 1$；$\Gamma(\cdot)$ 为伽马函数.

$$T_{a,b}^{\mathrm{DC}} = E^{\mathrm{Exp}}\left(R_{a,b}^{\mathrm{new}}\right) = E^{\mathrm{Exp}}\left[P^{\mathrm{Beta}}(\alpha_{a,b}^{\mathrm{S}} + 1, \beta_{a,b}^{\mathrm{F}} + 1)\right] = \frac{\alpha_{a,b}^{\mathrm{S}} + 1}{\alpha_{a,b}^{\mathrm{S}} + \beta_{a,b}^{\mathrm{F}} + 2} \tag{5}$$

式中：$T_{a,b}^{\mathrm{DC}}$ 为评价主体 a 对评价客体 b 基于通信行为的直接信任值；$E^{\mathrm{Exp}}(\cdot)$ 为期望函数；$\alpha_{a,b}^{\mathrm{S}}$ 和 $\beta_{a,b}^{\mathrm{F}}$ 分别为评价主体 a 和评价客体 b 历史交互的成功和失败次数.

(2) 基于数据质量的直接信任值：该信任值是指终端接收或转发的数据是否可信，本文中通过评价主体 a 对评价客体 b 传输的数据包相似度进行计算. 数据包具有空间相关性，即相邻终端之间发送的数据包在同一区域总是相似的，且这些数据包的特征值服从正态分布. 对于一组服从正态分布的数据，其概率密度函数为

$$P^{\mathrm{nomal}}(x^{\mathrm{D}}) = \frac{1}{\sigma^{\mathrm{D}}\sqrt{2\pi}} \exp\left[-\frac{(x^{\mathrm{D}} - \mu^{\mathrm{D}})^2}{2(\sigma^{\mathrm{D}})^2} \right] \tag{6}$$

式中：x^{D} 为数据包的特征值，具体包括数据大小、时间戳、格式等；μ^{D} 和 σ^{D} 分别为数据的平均值和方差.

若终端通信数据包属性的平均值越接近一组数据的平均值，则评价客体的信任值相对较高，反之，则相对较低. 因此，基于数据质量的直接信任值 $T_{a,b}^{\mathrm{DD}}$ 的计算式为

$$T_{a,b}^{\mathrm{DD}} = 1 - 2\int_{\mu^{\mathrm{D}}}^{\sigma^{\mathrm{D}}} P^{\mathrm{nomal}} x^{\mathrm{D}} \mathrm{d}x^{\mathrm{D}} \tag{7}$$

(3)基于传输速率的直接信任值:该信任值是指当评价主体 a 向评价客体 b 传输数据时,传输速率不在传输阈值内时,终端的信任将受到影响;本文中设定传输速率越接近期望值,终端信任值越高. 基于传输速率的信任值 $T_{a,b}^{\mathrm{DT}}$ 计算式为

$$T_{a,b}^{\mathrm{DT}}=\begin{cases}\dfrac{S_{a,b}^{\mathrm{Q}}-T_{a,b}^{\mathrm{ML}}}{E_{a,b}^{\mathrm{Q}}-T_{a,b}^{\mathrm{ML}}} & S_{a,b}^{\mathrm{Q}}\leqslant E_{a,b}^{\mathrm{Q}}\\ \dfrac{T_{a,b}^{\mathrm{MH}}-S_{a,b}^{\mathrm{Q}}}{T_{a,b}^{\mathrm{MH}}-E_{a,b}^{\mathrm{Q}}} & S_{a,b}^{\mathrm{Q}}>E_{a,b}^{\mathrm{Q}}\end{cases} \tag{8}$$

式中:$S_{a,b}^{\mathrm{Q}}$ 表示某时段内主体 a 到客体 b 的实际数据传输量;$T_{a,b}^{\mathrm{ML}}$ 和 $T_{a,b}^{\mathrm{MH}}$ 分别表示某时段内主体 a 到客体 b 的允许的最小和最大数据传输量;$E_{a,b}^{\mathrm{Q}}$ 表示某时段内主体 a 到客体 b 期望的数据传输量.

在得到基于通信行为、数据质量和传输速率的直接信任值之后,需要得到一个综合的直接信任值来度量终端的信任度. 本文中基于信息熵确定各因素直接信任值的不确定度,进而计算各因素直接信任值的权重. 将各直接信任值离散化为二项式分布随机变量后,综合直接信任值的计算过程为

$$H^{\mathrm{E}}\left(T_{a,b}^{\mathrm{DC}}\right)=-T_{a,b}^{\mathrm{DC}}\mathrm{lb}\,T_{a,b}^{\mathrm{DC}}-\left(1-T_{a,b}^{\mathrm{DC}}\right)\mathrm{lb}\left(1-T_{a,b}^{\mathrm{DC}}\right) \tag{9}$$

$$w_{a,b}^{\mathrm{DC}}=\left[1-\frac{H^{\mathrm{E}}\left(T_{a,b}^{\mathrm{DC}}\right)}{\mathrm{lb}\,T_{a,b}^{\mathrm{DC}}}\right]\Bigg/\left\{\left[1-\frac{H^{\mathrm{E}}\left(T_{a,b}^{\mathrm{DC}}\right)}{\mathrm{lb}\,T_{a,b}^{\mathrm{DC}}}\right]+\left[1-\frac{H^{\mathrm{E}}(T_{a,b}^{\mathrm{DD}})}{\mathrm{lb}\,T_{a,b}^{\mathrm{DD}}}\right]+\left[1-\frac{H^{\mathrm{E}}(T_{a,b}^{\mathrm{DT}})}{\mathrm{lb}\,T_{a,b}^{\mathrm{DT}}}\right]\right\} \tag{10}$$

$$T_{a,b}^{\mathrm{D}}=w_{a,b}^{\mathrm{DC}}T_{a,b}^{\mathrm{DC}}+w_{a,b}^{\mathrm{DD}}T_{a,b}^{\mathrm{DD}}+w_{a,b}^{\mathrm{DT}}T_{a,b}^{\mathrm{DT}} \tag{11}$$

式中:$H^{\mathrm{E}}\left(T_{a,b}^{\mathrm{DC}}\right)$、$H^{\mathrm{E}}\left(T_{a,b}^{\mathrm{DD}}\right)$、$H^{\mathrm{E}}\left(T_{a,b}^{\mathrm{DT}}\right)$ 分别表示评价主体 a 对评价客体 b 基于通信行为、数据质量和传输速率的直接信任值的信息熵,$H^{\mathrm{E}}\left(T_{a,b}^{\mathrm{DD}}\right)$ 和 $H^{\mathrm{E}}\left(T_{a,b}^{\mathrm{DT}}\right)$ 可根据式(9)同理求得;$w_{a,b}^{\mathrm{DC}}$、$w_{a,b}^{\mathrm{DD}}$、$w_{a,b}^{\mathrm{DT}}$ 分别表示基于通信行为、数据质量和传输速率的直接信任值熵权,$w_{a,b}^{\mathrm{DD}}$ 和 $w_{a,b}^{\mathrm{DT}}$ 可根据式(10)同理求得.

2.1.3 推荐信任评价

虚拟电厂内终端的互联互通作为终端网络的主要特征之一. 对于该类型终端网络,终端的信任评价不仅受到直接信任的影响,还受到推荐信任的影响,本文引入推荐信任增强对终端的信任评价.

定义 3 对于建立互联通信链路的终端,评价主体 a 通过推荐终端 x 提供的关于评价客体 b 的信任值来判断客体的信任度,该类信任评价被称为推荐信任,评价主体 a 对评价客体 b 推荐信任 $T_{a,b}^{\mathrm{R}}$ 的详细计算过程如下.

$$T_{a,b,x}^{\mathrm{R}}=\frac{\alpha_{a,b}^{\mathrm{S}}\alpha_{x,b}^{\mathrm{S}}+0.5(\beta_{a,x}^{\mathrm{F}}+2)(\alpha_{x,b}^{\mathrm{S}}+\beta_{x,b}^{\mathrm{F}}+2)+\alpha_{a,x}^{\mathrm{S}}}{\alpha_{a,b}^{\mathrm{S}}\alpha_{x,b}^{\mathrm{S}}+\alpha_{a,x}^{\mathrm{S}}\beta_{x,b}^{\mathrm{F}}+(\beta_{x,b}^{\mathrm{F}}+2)(\alpha_{x,b}^{\mathrm{S}}+\beta_{x,b}^{\mathrm{F}}+2)+2\alpha_{a,x}^{\mathrm{S}}} \tag{12}$$

$$H^{\mathrm{E}}\left(T_{a,b,x}^{\mathrm{R}}\right)=-T_{a,b,x}^{\mathrm{R}}\mathrm{lb}\,T_{a,b,x}^{\mathrm{R}}-\left(1-T_{a,b,x}^{\mathrm{R}}\right)\mathrm{lb}\left(1-T_{a,b,x}^{\mathrm{R}}\right) \tag{13}$$

$$w_x^{\mathrm{R}}=\frac{1-\dfrac{H^{\mathrm{E}}(T_{a,b,x}^{\mathrm{R}})}{\mathrm{lb}\,T_{a,b,x}^{\mathrm{R}}}}{\sum\limits_{x=1}^{N^{\mathrm{X}}}\left[1-\dfrac{H^{\mathrm{E}}(T_{a,b,x}^{\mathrm{R}})}{\mathrm{lb}\,T_{a,b,x}^{\mathrm{R}}}\right]} \tag{14}$$

$$T_{a,b}^{\mathrm{R}}=\sum_{x=1}^{N^{\mathrm{X}}}w_x^{\mathrm{R}}T_{a,b,x}^{\mathrm{R}} \tag{15}$$

式中:$T_{a,b,x}^{\mathrm{R}}$ 表示推荐终端 x 发送给评价主体 a 关于评价客体 b 的推荐信任值,x 表示推荐终端编号;$\alpha_{x,b}^{\mathrm{S}}$ 和 $\beta_{x,b}^{\mathrm{F}}$ 分别表示推荐终端 x 与评价客体 b 历史交互的成功和失败次数;$\alpha_{a,x}^{\mathrm{S}}$ 和 $\beta_{a,x}^{\mathrm{F}}$ 分别表示评价主体 a 和推荐终端 x 历史交互的成功和失败次数;$H^{\mathrm{E}}\left(T_{a,b,x}^{\mathrm{R}}\right)$ 为推荐终端 x 产生的推荐信任值的信息熵;w_x^{R} 为终端 x 提供的推荐信任值的熵权;N^{X} 为推荐终端数.

2.1.4 间接信任评价

在虚拟电厂中,由于存在多个终端和多个参与者,直接信任和推荐信任对网络拓扑具有一定的要求,仅使用这两种信任评价方式不足以描述整个信任关系. 因此,本文中进一步引入间接信任. 通过间接信任评价,可以将所有终端之间的信任关系都纳入到信任评价中,从而得到更全面、更准确的信任评价结果.

定义 4 针对 VPP 网络中无法建立直接通信链路的终端,基于信任的传递特性通过推荐终端 x 建立评价主体 a 与评价客体 b 的信任关系,该类信任评价为间接信任评价 $T_{a,b}^{\mathrm{I}}$,间接信任值计算方式为

$$T_{a,b}^{\mathrm{I}}=T_{a,1}^{\mathrm{D}}\times T_{1,2}^{\mathrm{D}}\times\cdots\times T_{x-1,x}^{\mathrm{D}}\times T_{x,b}^{\mathrm{D}} \tag{16}$$

式中:$T_{x-1,x}^{\mathrm{I}}$ 表示推荐终端 $x-1$ 对推荐终端 x 的直接信任值;$T_{x,b}^{\mathrm{I}}$ 表示推荐终端 x 对评价客体 b 的直接信任值.

2.2 信任的聚合与更新

基于本文中提出并给出定义量化的直接信任、推荐信任和间接信任 3 种信任评价,以得到更准确的信任估计结果. 在信任值聚合过程中,权重分配是非常重要的. 为了避免平均分配和主观分配带来的问题,本文采用信息熵作为自适应权重分配的依据. 具体来说,针对每个评价客体,分别计算 3 种信任值的熵权,然后将其作为权重分配系数,将 3 种信任值融合为一个综合信任值. 在 VPP 网络中,一个评价客体

可能会被多个评价主体评价，因此需要考虑多个评价主体的评价结果来反映评价客体在网络中的总体信誉度. 最终，本文提出综合信任值 $T_{a,b}^{\mathrm{com}}$ 成为网络对评价客体的最终信任评价指标. 图 3 为 VPP 异构终端信任评价过程.

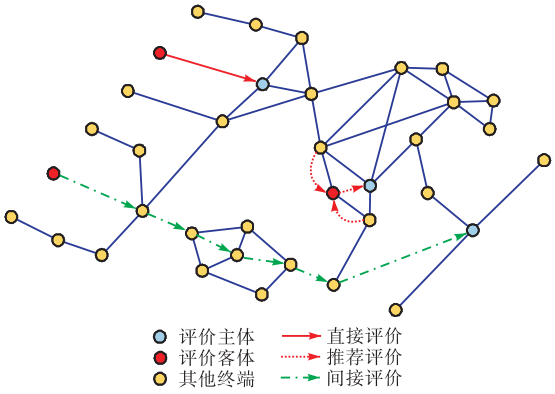

图 3　VPP 异构终端信任评价过程

Fig.3　Heterogeneous terminal trust evaluation process for the VPP

$$T_{a,b}^{\mathrm{com}} = w_{a,b}^{\mathrm{D}} T_{a,b}^{\mathrm{D}} + w_{a,b}^{\mathrm{R}} T_{a,b}^{\mathrm{R}} + w_{a,b}^{\mathrm{I}} T_{a,b}^{\mathrm{I}} \tag{17}$$

式中 $w_{a,b}^{\mathrm{D}}$、$w_{a,b}^{\mathrm{R}}$、$w_{a,b}^{\mathrm{I}}$ 分别为直接信任、推荐信任和间接信任的熵权.

本文中同时考虑到信任关系在 VPP 网络中是动态变化的，终端的行为可能会因为环境变化、被俘获、故障、移除或更新等异常情况而快速或不可预测地改变. 为了维护网络的信任环境，当终端处于异常状态时，其信任值需要及时更新. 本文采用私有链对完整信任进行更新.

3　基于私有链的 VPP 异构终端信任参数共识方法

区块链是一种全新的去中心化分布式记账方式，其分布式存储、公开透明的信息记账方式能避免恶意节点对信息的篡改[24]. 私有链相较于公有链和联盟链，对系统权限的控制程度更高，其写入权限可由某一中心节点完全控制，读取权限通常是选择性公布，更适用于 VPP 内部终端信任管理场景. 因此，采用私有链对 VPP 终端信任参数进行存储，以保障 VPP 终端信任参数的可靠与安全.

3.1　信任参数共识架构

本文中考虑到 VPP 中存在大量的敏感数据和异构终端设备需要更高的隐私保护. 一方面，私有链可以控制参与者的身份，从而有效保护数据隐私，保证 VPP 内部数据的安全性；另一方面，这些设备的种类和性能差异很大，私有链可以自定义信任管理机制，并支持可插拔共识机制，可以快速适应 VPP 内部终端设备的变化，保证信任管理的稳定性和可靠性. 私有链系统通常采用 6 层架构，从底层数据层向上依次为数据、网络、共识、激励、合约和应用层，每层分别承担不同的职责和功能，相互支持，构成了经典的区块链架构[25]. 本文将私有链通用架构与 VPP 终端信任管理场景相结合，设计基于私有链的 VPP 信任参数共识方案. 图 4 所示为基于私有链的 VPP 信任参数共识方案.

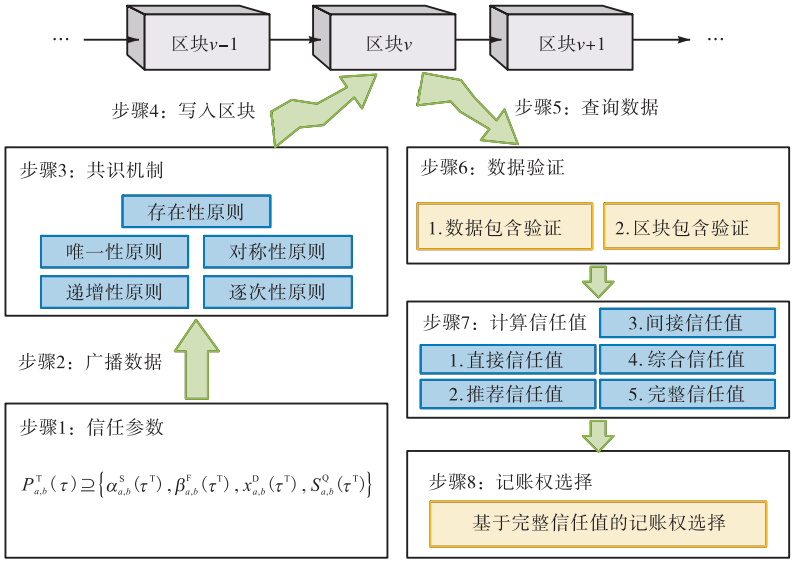

图 4　基于私有链的 VPP 信任参数共识方案

Fig.4　Trust parameter consensus project for the VPP based on a private blockchain

基于私有链的虚拟电厂终端信任共识方案如下：　首先，VPP 终端根据其通信行为、数据质量以及传输

速率信任参数生成信任参数包,并通过通信网络广播发送至其他终端;其次,其他终端按照提出的共识机制对所有信任参数进行合法性和真实性验证,通过验证的信任参数由本周期记账终端写入区块链. 当需要评价其他设备信任水平时,将从私有链上查询并提取所需数据. 此时,对于部分终端无法直接参与共识的终端,首先,设计了基于 Merkle 山脉(Merkle mountain range, MMR)的信任参数验证方法,对私有链的数据进行辅助验证;然后,采用基于查询的信任参数,结合基于信息熵的 VPP 终端多因素信任评价模型,对评价客体的完整信任值进行计算;最后,为满足 VPP 终端对安全性的差异化需求,选取完整信任值最高的终端参与下一周期记账,生成下一个区块并添加在私有链最末端.

3.2 终端信任参数共识方法

对 VPP 终端的实体和虚拟映射进行分析,可发现 VPP 中的终端可分为计算能力和存储能力相对有限的终端(一般节点),以及计算能力强、带宽资源充足、具有汇聚传输能力的终端(汇聚节点). 因此,在私有链中,将 VPP 接入的终端设备按照其本身的特性划分为全节点和轻节点. 全节点能够完整存储私有链中所有区块,具备独立记账、信任参数验证、节点权限管理等功能,例如 IED、集中控制器、核心路由. 轻节点只存储部分区块数据,可以从其他全节点中获取所需的数据并验证信任,不需要存储完整的区块链数据,不享有记账权,例如逆变器、智能电表、一般交换机.

基于全节点和轻节点的特性,对 VPP 中各类终端信任参数共识方案的信任参数的生成、全节点共识机制、轻量化存储和计算 3 个关键环节进行具体的设计.

3.2.1 信任参数的生成

基于多因素信任评价模型,可知节点信任参数包括:节点间通信成功和失败累计次数 $\alpha_{a,b}^{\mathrm{S}}$ 和 $\beta_{a,b}^{\mathrm{F}}$,节点间传输的数据 x^{D},数据传输的速率 $S_{a,b}^{\mathrm{Q}}$. 因此,对于设定的信任更新周期 T^{Ren},评价客体 b 在周期内第 τ^{T} 个时隙生成的信任参数数据包可表示为

$$P_{a,b}^{\mathrm{T}}(\tau^{\mathrm{T}}) \supseteq \left\{\alpha_{a,b}^{\mathrm{S}}(\tau^{\mathrm{T}}), \beta_{a,b}^{\mathrm{F}}(\tau^{\mathrm{T}}), x_{a,b}^{\mathrm{D}}(\tau^{\mathrm{T}}), S_{a,b}^{\mathrm{Q}}(\tau^{\mathrm{T}})\right\} \tag{18}$$

式中 $P_{a,b}^{\mathrm{T}}(\tau^{\mathrm{T}})$ 是在第 τ^{T} 个时隙评价主体 a 中关于评价客体 b 的信任参数包.

各终端将生成的信任参数包广播分发,并且其他节点会对这些信任参数包进行合法性验证.

3.2.2 全节点共识机制

本方法共识机制包括 5 条全节点信任参数的验证准则,用于验证上链信任数据的合法性和真实性,验证准则表示如下.

(1) 存在性:如果评价客体 b 在第 τ^{T} 个时隙不与任意节点发生交互,则该时隙其他节点不存在与评价客体 b 的交互记录.

$$P_{a,b}^{\mathrm{T}}(\tau^{\mathrm{T}}) = \varnothing \quad \alpha_{a,b}^{\mathrm{S}}(\tau^{\mathrm{T}}) + \beta_{a,b}^{\mathrm{F}}(\tau^{\mathrm{T}}) = 0, \forall a \neq b \tag{19}$$

(2) 对称性:同一交互行为在交互双方记录的信任参数包中,交互成功和失败累计的次数、数据特征、数据传输速率应当一致.

$$\begin{cases} \alpha_{a,b}^{\mathrm{S}}(\tau^{\mathrm{T}}) = \alpha_{b,a}^{\mathrm{S}}(\tau^{\mathrm{T}}) \\ \beta_{a,b}^{\mathrm{F}}(\tau^{\mathrm{T}}) = \beta_{b,a}^{\mathrm{F}}(\tau^{\mathrm{T}}) \\ x_{a,b}^{\mathrm{D}}(\tau^{\mathrm{T}}) = x_{b,a}^{\mathrm{D}}(\tau^{\mathrm{T}}) \\ S_{a,b}^{\mathrm{Q}}(\tau^{\mathrm{T}}) = S_{b,a}^{\mathrm{Q}}(\tau^{\mathrm{T}}) \end{cases} \quad \alpha_{a,b}^{\mathrm{S}}(\tau^{\mathrm{T}}) + \beta_{a,b}^{\mathrm{F}}(\tau^{\mathrm{T}}) \neq 0 \tag{20}$$

(3) 唯一性:在第 τ^{T} 个时隙评价主体 a 至多选择一个评价客体信任参数上链.

$$P_{a,b}^{\mathrm{T}}(\tau^{\mathrm{T}}) \cdot P_{x,b}^{\mathrm{T}}(\tau^{\mathrm{T}}) = 0 \qquad \forall x \neq b \neq a \tag{21}$$

(4) 递增性:随着时隙数增加,交互成功与失败累计数只能增加,不可减少.

$$\begin{cases} \alpha_{a,b}^{\mathrm{S}}(\tau^{\mathrm{T}}) \geqslant \alpha_{a,b}^{\mathrm{S}}(\tau^{\mathrm{T}} - 1) \\ \beta_{a,b}^{\mathrm{F}}(\tau^{\mathrm{T}}) \geqslant \beta_{a,b}^{\mathrm{F}}(\tau^{\mathrm{T}} - 1) \end{cases} \tag{22}$$

(5) 逐次性:随着时隙数增加,信任评价主体与评价客体交互成功与失败的累计数只能逐次递增,不能跳变.

$$\begin{cases} \alpha_{a,b}^{\mathrm{S}}(\tau^{\mathrm{T}}) = \alpha_{a,b}^{\mathrm{S}}(\tau^{\mathrm{T}} - 1) + 1 \\ \beta_{a,b}^{\mathrm{F}}(\tau^{\mathrm{T}}) = \beta_{a,b}^{\mathrm{F}}(\tau^{\mathrm{T}} - 1) + 1 \end{cases} \tag{23}$$

为了适应 VPP 的规模,本文新增定义两个参数:节点共识最少参与数 C^{Node} 和最小连续共识次数 C^{Data}. 当参与共识验证的节点数不少于 C^{Node} 时,才可以将信任参数写入区块链. 另外,当某一节点的信任参数在连续的 C^{Data} 次共识验证中均未通过时,该节点会被判定为恶意节点. 该共识机制能够对信任参数进行可靠性筛选,提早发现网络内部的安全隐患. 它能够识别并阻止恶意节点攻击行为,例如发送恶意信任数据诋毁其他良好节点的信誉、篡改不良行为数据来隐藏攻击行为. 基于私有链的不可篡改性,该机制可以确保链上数据的可靠与安全.

3.2.3 轻量化存储和计算

由于 VPP 内各类型终端的计算、储能、通信等能力存在较大的差异,对信任参数的上链带来了计算开销和存储限制等挑战. 传统私有链区块的 root 字段为所有数据的 Merkle 树根哈希值,pre_hash 为父区块的 Hash 值,这样的设计使得每当一个叶子节点的

数据发生变化时，所有在该叶子节点上的节点都需要重新计算哈希值，这会带来较大的计算负担. 因此，基于 Merkle 山脉，本文对私有链区块的区块头和区块体进行改进，如图 5 所示，以适应轻量化存储和计算.

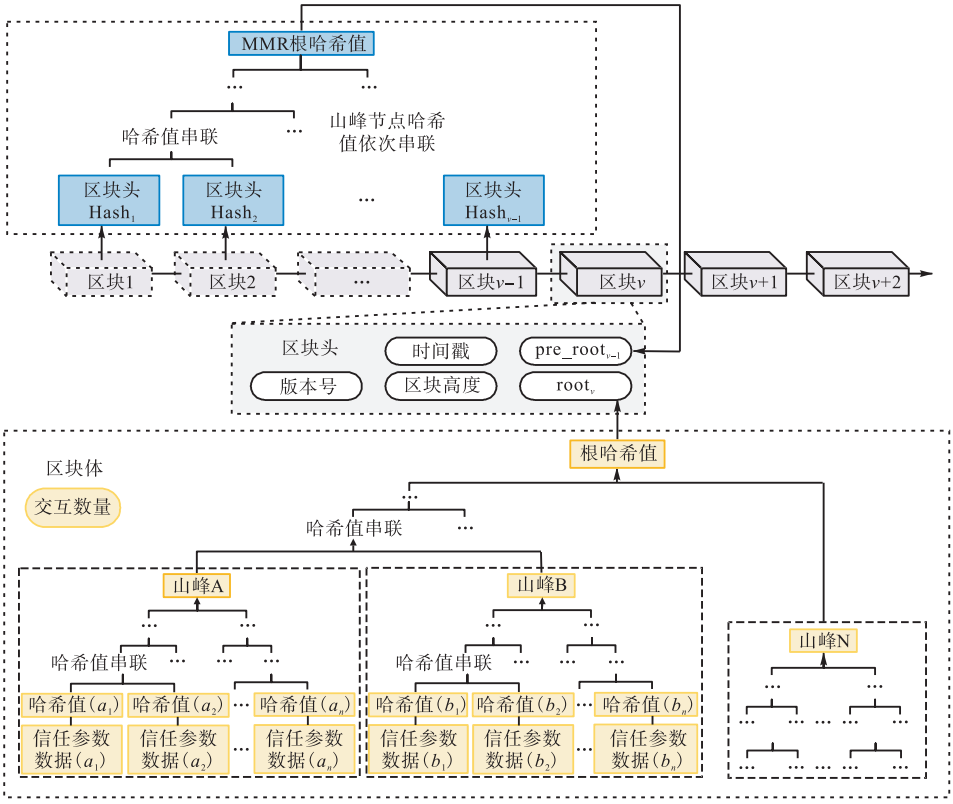

图 5　基于 MMR 的 VPP 接入终端信任管理私有链区块结构

Fig.5　Structure of the private blockchain for VPP access terminal trust management based on MMR

如图 5 所示，本文中所提出的基于 MMR 的 VPP 信任管理私有链区块结构. 该结构使用 pre_root_{v-1} 和 root_v 替换了传统区块的 root 和 pre_hash 字段，pre_root_{v-1} 记录了第 1 个至第 $v-1$ 个区块的区块头哈希值，root_v 为当前区块的区块体 MMR 根哈希值. 区块体包括交互数量和信任参数，多种信任参数以 MMR 的方式逐层构造. 在 MMR 中，每个叶子节点只有一个父节点，即使有一个叶子节点的数据发生了变化，也只需要重新计算它所在的链路上的哈希值，而不必重新计算其他不相关的哈希值. 这使得 Merkle 山脉的哈希计算更加高效，并且可以更快地支持私有链的增量更新.

本文中面向信任参数的私有链区块由两种 MMR 构造，由所有区块头哈希值作为叶节点的 MMR_Head，由本周期内所有信任参数哈希值作为叶子节点的 MMR_Body. 这样更便于链上信任参数的存储，同时也可以快速生成证明以验证数据的可信性. MMR_Head 和 MMR_Body 除叶节点的内容不一致，其他构造方式均相同. 以 MMR_Body 构造为例，首先对待写入区块的 $P_{a,b}^{\mathrm{T}}(\tau^{\mathrm{T}})$ 参数包数据进行统一编码 d_1^{T}，d_2^{T}，…，d_λ^{T}，每个数据的哈希值为 d_1^{TH}，d_2^{TH}，…，d_λ^{TH}，两数据串联的哈希值为 $H^{\mathrm{a}}(d_\lambda^{\mathrm{TH}}, d_{\lambda'}^{\mathrm{TH}})$. 以两终端最少交互两次，逐层构建 8 个叶节点的 MMR_ Body. Merkle 山脉构造过程如图 6 所示.

(1) 初始阶段：将 d_1^{TH} 和 d_2^{TH} 写入 0 和 1 叶节点，并计算 $H^{\mathrm{a}}(d_1^{\mathrm{TH}}, d_2^{\mathrm{TH}})$，串联的写入中间节点，并编号为 2；然后，将 d_3^{TH} 写入第 3 个叶节点，并编号为 3. 此时，Merkle 山脉峰节点编号为 2 与 3.

(2) 叶节点追加阶段：当 d_4^{TH} 写入第 4 个叶节点时，各哈希值进行触发串联合并操作，串联规则可表述为：$H^{\mathrm{a}}(d_3^{\mathrm{TH}}, d_4^{\mathrm{TH}}) \rightarrow H^{\mathrm{a}}[H^{\mathrm{a}}(d_1^{\mathrm{TH}}, d_2^{\mathrm{TH}}), H^{\mathrm{a}}(d_3^{\mathrm{TH}}, d_4^{\mathrm{TH}})]$. 此时，MMR_Body 仅存在一座山峰节点，编号为 6.

(3) 合并循环阶段：当数据哈希值不断写入叶节点时，按叶节点追加方式循环进行，在山峰高度相等时触发串联合并操作，直至 MMR_Body 中所有山峰高度不同时，完成 MMR_Body 的构造.

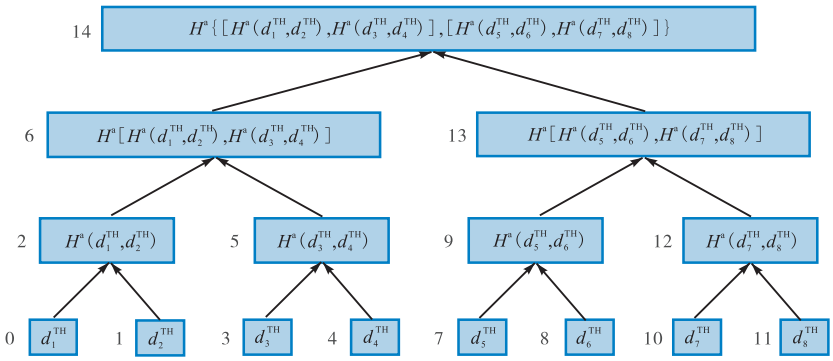

图 6　Merkle 山脉构造过程

Fig.6　Merkle mountain construction process

4　算例验证

4.1　仿真场景设置

为验证终端轻量信任评价方法，基于文献[26]虚拟电厂算例，构建本文 VPP 仿真算例. 基于光纤的 VPP 算例通信网络如图 7 所示. VPP 包括 1 个 34 MW 风电场、1 个 3 MW 光伏装置和 1 个 8 MW/32 MW · h 的电池储能系统，DERs 接口电压等级 10 kV. 并网系统由 1 条母线、3 条进线、1 条出线和 1 个 10 kV 变电站组成. 通信网络划分为 4 个单元：单元 1 为变电单元，包括 1 个合并单元(merging unit，MU)、2 个断路器 IED、1 个保护装置 IED 与 1 个测控 IED；单元 2 为光伏单元；单元 3 为风电单元；单元 4 为储能单元. 单元 2、3、4 各自均包含 1 个 MU、1 个断路器 IED、1 个逆变器 IED、1 个保护装置 IED 和 1 个测控 IED. 各单元内 IED 通过内部交换机与其他设备通信. 汇集交换机和安全接入网关与控制层核心交换机连接. 上层控制中心由监控主机、服务器和密码机等组成. 负荷侧由居民负荷、工业负荷、电动汽车负荷组成，终端类型有智能电表、集中器控制器、交换机、路由器、射频拉远单元(remote radio unit，RRU)、基带处理单元(building base band unit，BBU)等，各类终端总数 1 000.

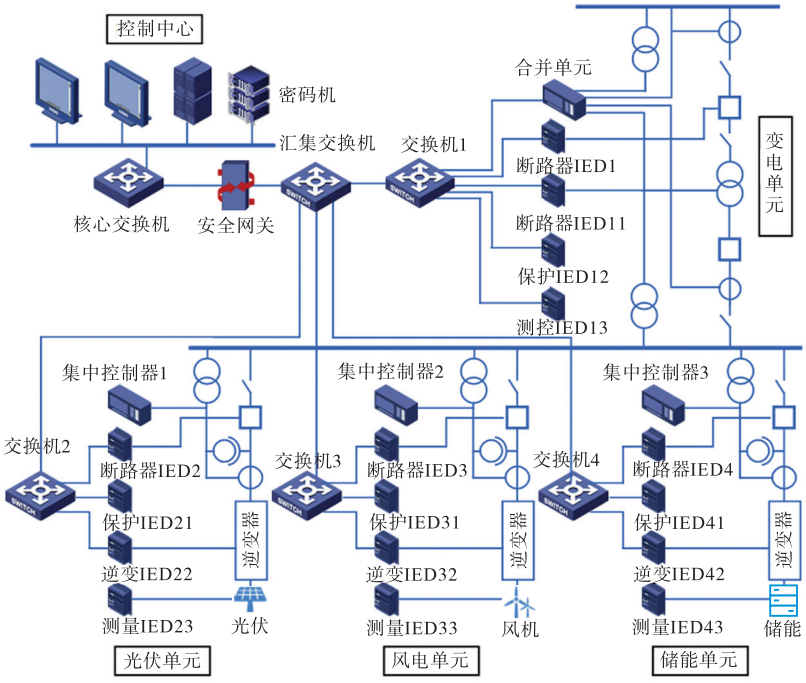

图 7　VPP 算例通信网络

Fig.7　Communication network of VPP example

为模拟信任评价网络，仿真不同终端密度的评价结果，直连模式的终端逻辑连接邻居数设定为 2，互联模式的终端邻居数设定为 4 和 8. 本文结合构建的 VPP 算例，基于 GoLand 2020.2.4 开发环境测试基

于 Go 语言实现的私有链应用程序，对所提信任评价方法的准确性、安全性以及轻量性进行仿真验证. 同时，为充分评估本文所提方法的有效性，选取信任管理研究领域中广泛应用的基于 Beta 分布的信任和信誉评估系统(Beta based trust and reputation evaluation system，BTRES)[27]、基于时间窗口的弹性信任管理方案(time window based resilient trust management scheme，TRTMS)[28]和基于区块链的信任共识(blockchain based trust consensus，BTCM)[29] 3 种信任评价算法进行准确性、安全性和轻量性对比分析. 仿真算例场景的信任评价参数设置如表 1 所示.

表 1　信任评价仿真算例参数

Tab.1　System parameters for trust evaluation simulation

参数	取值	含义
T_b^{IFull}	0.5	初始信任值
T^{Ren}/h	24	信任更新周期
N^{UT}	100	评价客体 b 周期内交互次数
C^{Node}	600	节点共识最少参与数
C^{Data}	3	最小连续共识次数
T^{TFA}	0.7 ~ 1.0	信任域
T^{MFA}	0 ~ 0.3	恶意域
θ^{Suc}	0.95	正常交互成功率
$\varepsilon^{\mathrm{Mal}}$	0.2	恶意交互失败率
o^{Mal}	100 ~ 300	恶意节点数
S^{Head}/Bytes	508	区块头
H^{PB}/Bytes	32	哈希输出

4.2　性能分析

4.2.1　准确性分析

对于一个信任更新周期，设置可信终端信任评价值 $T^{\mathrm{Full}}<0.3$ 时，评价结果为假恶意终端；当恶意终端信任评价值 $T^{\mathrm{Full}}>0.7$ 时，评价结果为假可信终端. 本文中应用信任评价算法的准确率 δ^{ACC}、查准率 δ^{PRE} 和查全率 δ^{REC}[30]来评估信任评价方法的准确性.

如图 8 所示，随着终端网络数量增加，4 种信任评价算法的准确率、查准率和查全率均表现越来越低. 对于 3 种指标，终端数的增加对准确率的变化影响最大，对召回率的影响最小. 对于每一种评价指标的 4 种算法，本文算法受到终端数量的影响最小. 以算法评价准确率为例，当网络终端数为 200 时，TRTMS、BTRES、BTCM 和本文算法中的评价准确率分别为 87.0%、90.5%、90.0%和 91.1%. 各评价方法的评价准确度均较高且相差不大. 但当网络终端数达到 1 000 时，本文算法的对正常终端的评价准确率为 78.6%，3 种对比算法的评价准确率分别为 65.4%、69.4%、70.7%. 本文算法较 3 种对比算法评价准确率分别高出了 13.2%、9.2%、7.9%. 这是由于网络终端规模增加，不可靠的信任参数逐渐增加，TRTMS 和 BTRES 缺乏对信任参数进行辨识，直接导致可信终端评价正确率降低. BTCM 虽然可以对信任参数进行辨识，保障了信任参数可靠性，但 BTCM 信任评价因素只考虑了终端的通信行为，容易对可信终端造成误判. 通过实验结果对比可知，本文所提出的算法在准确率、查准率和查全率各项评价指标均具有明显优势，且受到终端数量的影响最小.

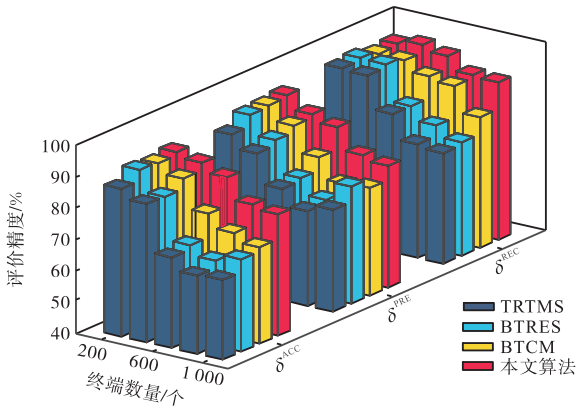

图 8　VPP 终端信任评价准确性

Fig.8　Accuracy of VPP terminal trust evaluation

4.2.2　安全性分析

作为抵御网络内部攻击的有效手段，信任评价方法需要具备必要的安全性. 为对所提算法的安全性进行验证，本文模拟了终端在遭受开关攻击、诽谤攻击两种不同类型的网络内部攻击时，其信任值的变化情况. 在 VPP 网络中，假设评价主体 a 与评价客体 b 初始交互次数 $\alpha_{a,b}^{\mathrm{S}}=\beta_{a,b}^{\mathrm{F}}=0$，$S_{a,b}^{\mathrm{Q}}=0$，即初始状态终端没有交互行为.

1）开关攻击

开关攻击通过多次使用相同的密钥加密不同的明文来分析加密过程中的密钥生成过程. 在开关攻击中，攻击者会试图通过网络内部的某个节点进入系统，在目标系统中插入特定的代码 a^{SF} 修改数据中的二进制位；并利用权限控制从目标系统中窃取信息或者破坏其正常的操作. 攻击事件可以描述为：加密算法 $E^{\mathrm{EA}}(\cdot)$对明文 m^{Ori} 使用密钥 k^{mk} 加密后，其信息被转换成的任意比特串 a^{SF} 异或得到被攻击的密文 m^{Cip}，$m^{\mathrm{Cip}}=E^{\mathrm{EA}}(m^{\mathrm{Ori}},k^{\mathrm{mk}})\oplus a^{\mathrm{SF}}$. 为模拟开关攻击的行为，设定前 40 次正常交互，41 ~ 60 次交互时遭受开关攻击，数据篡改成功的比例设定为 60%，61 次交互时去除开关攻击对终端的影响.

如图 9 所示，在前 40 次正常交互时，终端信任值随着交互次数的增加信任值逐渐增加，基于本文算

法的终端信任值最高可达 0.94. 在第 41 次交互开始,对终端实施开关攻击,4 种信任评价方法的信任值均逐渐降低. 在 60% 数据被篡改开关攻击行为下,本文算法信任值整体水平低于 BTCM 算法,这是由于所提算法的多因素评价不仅考虑了交互行为,还考虑了数据质量和传输速率对信任的影响,对受攻击终端的信任评价值更低. 而对于 BTRES 和 TRTMS 算法,信任参数的微小变化便令信任值骤变,评价系统不稳定,这不利于对攻击行为的判断. 在攻击结束后,随着交互次数增加,终端的信任值随之恢复,但是 BTRES 和 TRTMS 算法信任值恢复较快,且与初始最高信任水平相当. 本文算法的信任恢复速度较慢,且恢复后的最高值为 0.78,是正常交互时最高信任值的 82.98%. 这是由于本文算法中正确信任参数需要得到更多节点的共识才能参与信任计算,信任值的变化趋势可以体现由历史不良行为对终端信任值造成的影响. 可以发现,当数据篡改比例增加时,被攻击的数据更多被篡改为可信的数据,信任值均得到上升. 本文方法与 BTCM 算法的信任值波动均较小,评价系统更稳定,具备抵御开关攻击的能力. 这是由于两种方法均对参与评价的信任参数进行了共识验证,保证了参与评价的信任参数的可靠性和真实性.

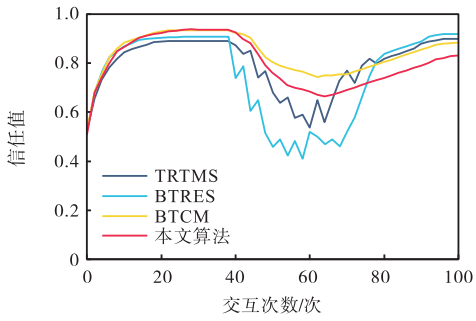

图 9　开关攻击下终端信任值评价结果

Fig.9　Evaluation results of terminal trust values under ON-OFF attacks

2) 诽谤攻击

诽谤攻击是攻击者通过虚假信息、不实行为等手段来污名化目标对象,影响其声誉和信任度的行为. BTRES 算法为抵御诽谤攻击,设定当直接信任与推荐信任和间接信任差值的绝对值大于设定的攻击阈值 θ^{Att} 时,攻击成立;当小于攻击阈值 θ^{Att} 时,可忽略诽谤攻击的影响. 诽谤攻击判定条件为

$$\left|w_{a,b}^{\mathrm{D}}T_{a,b}^{\mathrm{D}}-w_{a,b}^{\mathrm{R}}T_{a,b}^{\mathrm{R}}-w_{a,b}^{\mathrm{I}}T_{a,b}^{\mathrm{I}}\right|>\theta^{\mathrm{Att}} \tag{24}$$

诽谤攻击开始与截止的设置与开关攻击一致,评价客体 b 为可信终端,BTRES 算法 θ^{Att} 值设置为 0.25,本文方法和 BTCM 终端共识比例设定为 60% 与 100%. 随即,在诽谤攻击下,对各信任评价方法的信任评价结果进行对比分析.

如图 10 所示,当诽谤攻击发生时,除本文算法 100% 节点参与共识的情况,其余信任值都明显降低. 这是由于全节点参与共识可以排除不可靠的信任参数参与信任计算,能够准确对评价客体的真实情况进行判断. TRTMS 算法的信任值最低,说明可信终端受到诽谤攻击的影响最大,不具备抵御诽谤攻击的能力. BTRES 算法的信任值计算存在一个恢复的趋势,具有一定抵御诽谤攻击的能力. 这是由于信任值和攻击阈值在满足式(24)时,间接信任参数将被舍弃,不参与信任评价. 但是该方法最终得到的信任评价值为 0.89,不符合对评价客体 b 完全可信的设定. 在 60% 节点参与共识的情况下,本文算法得到的最终信任值较 BTCM 高出 0.11. 这是由于本文算法参与信任评价的信任参数更丰富,节点共识将排除更多影响终端信任的评价因子,因此终端的信任值更高. 可以发现,随着参与共识验证的终端数量增加,本文算法抵御诽谤攻击的能力越强,当网络中所有终端都参与共识时,评价客体的信任评价将不受诽谤攻击的影响.

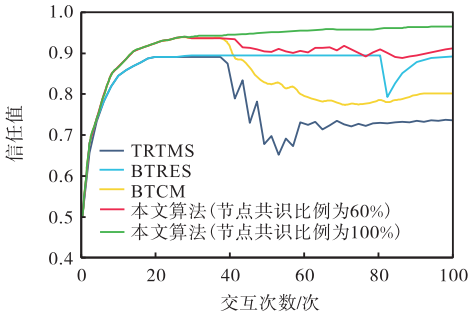

图 10　诽谤攻击下终端信任值评价结果

Fig.10　Evaluation results of terminal trust values under defamation attacks

考虑到 BTRES 算法性能对参数 θ^{Att} 值变化具有相关性,本文进一步分析所提算法(节点共识比例设为 60%、80%、100%)与 BTRES 算法(θ^{Att} 设为 0.25、0.30)的性能对比及各自灵敏度分析,如图 11 所示. 可以看出,当诽谤攻击发生时,本文算法和 BTRES 算法的信任值都发生了明显降低. 相较于 θ^{Att} 值等于 0.25 时,θ^{Att} 值等于 0.30 时 BTRES 算法的信任值会在诽谤攻击开始后会出现突变下降态势,这是因为 BTRES 通过设置攻击阈值参数能够抵御一定的诽谤攻击,但是信任值对该阈值波动的灵敏度较高,从而影响抵御攻击能力. 而在诽谤攻击结束后,BTRES

算法也同样发生突变下降行为，这也是由该阈值变化引起的，并且可以看出，攻击阈值设置越大，突变越提前发生且突变越显著，说明了 BTRES 算法在抵御诽谤攻击方面具有局限性. 通过参数灵敏度分析，可以看出所提方法随着共识比例增加，终端信任值下降程度逐渐降低，即受到诽谤攻击的影响逐渐变小. 在理想情况下，共识比例为 100% 时，诽谤攻击对正常节点的信任值将没有影响. 从而体现了所提出方法中共识机制的有效性.

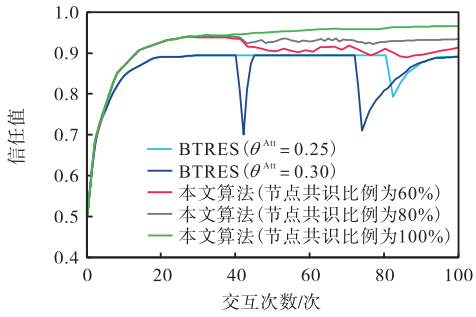

图 11　诽谤攻击中不同算法参数下终端信任值评价结果

Fig.11　Evaluation results of terminal trust values under different algorithm parameters under defamation attacks

4.2.3　轻量性分析

在终端信任评价轻量级存储和计算性能评估方面，设定 TRTMS 与 BTRES 算法的信任参数均保存在评价客体中，存储资源开销取决于信任参数本身大小，在相同的仿真场景下，信任参数量相同. 与上述两种算法对比，本文所提算法和 BTCM 算法信任参数存储能力由区块的构造方式确定. BTCM 采用的是 Merkle 树构造区块，区块储存空间计算评估公式为

$$S^{\mathrm{MT}}=N^{\mathrm{PB}}B^{\mathrm{PB}} \tag{25}$$

本文算法采用的是 MMR 区块构造方法，区块储存空间计算评估公式为

$$S^{\mathrm{MMR}}=B^{\mathrm{PB}}\left(H^{\mathrm{PB}}+\mathrm{lb}\,N^{\mathrm{PB}}\right) \tag{26}$$

式中：S^{MT} 和 S^{MMR} 分别表示 Merkle 树和 MMR 区块构造的私有链存储空间；B^{PB} 表示每个区块的平均大小；H^{PB} 表示哈希值的长度；N^{PB} 表示私有链的区块数量.

由此，在设定固定的区块头和哈希输出大小条件下，对比相同数据量所需的存储资源情况.

如表 2 所示，本文算法与 BTCM 的信任参数存储开销为 kB 量级，TRTMS 与 BTRES 算法存储开销为 MB 量级. 这是由于本文算法与 BTCM 算法采用区块链的方式存储信任参数，存储资源是由区块链的区块头大小与区块高度确定的. 这与传统的信任评价方式有着本质不同. 本文算法存储开销较 BTCM 更优，这是因为本文算法采用 MMR 对私有链区块进行了改进. 在信任参数验证时，轻节点只需要存储一个最近更新的区块头以及全节点发来的 MMR_Head 证明. 由计算方式也可知存储开销与区块数量成对数关系. BTCM 的轻节点验证则需要存储全部区块头，存储开销与区块数量成线性关系.

表 2　不同终端规模信任评价的存储开销

Tab.2　Storage capacity for trust evaluation across different terminal scales

终端规模/个	TRTMS/MB	BTRES/MB	BTCM/kB	本文算法/kB
200	2.8	2.8	99	19.6
400	5.6	5.6	198	20.1
600	8.4	8.4	298	20.4
800	11.6	11.6	397	20.6
1 000	14.8	14.8	496	20.8

5　结　论

本文聚焦 VPP 异构接入终端复杂交互特性对终端管理造成的网络安全威胁问题，建立 VPP 多类终端的虚拟映射模型，充分利用终端交互的通信行为、数据质量和传输速率信息，提出一种私有链的 VPP 异构接入终端轻量信任评价方法，实现异构终端直连和互联交互模式的安全、精准、轻量信任评价，得出如下结论.

（1）本文提出的基于信息熵的 VPP 异构终端多因素信任评价方法可实现直接信任、推荐信任、间接信任、综合信任、完整信任评价结果的融合，信任评价准确率较 TRTMS、BTRES 和 BTCM 方法分别提升了 13.2%、9.2%、7.9%，可实现异构终端精准评价.

（2）所提出的基于私有链的异构终端信任参数共识方法有效提升了信任评价的安全性能，在抵御诽谤攻击、开关攻击等网络攻击能力有显著提升.

（3）本文提出的基于 Merkle 山脉的私有链区块改进方法能够实现信任参数的轻量化存储和计算，所提算法存储开销仅为 kB 级.

参考文献：

[1] Wang Q，Wu W C，Wang B，et al. Asynchronous decomposition method for the coordinated operation of virtual power plants[J]. IEEE Transactions on Power Systems，2023，1(1)：767-782.

[2] Zhang Y，Yuan F M，Zhai H P，et al. Optimizing the planning of distributed generation resources and storages in the virtual power plant，considering load uncertainty

[J]. Journal of Cleaner Production, 2023, 387(1): 36-51.

[3] 杨 挺, 张 剑, 蔡绍堂, 等. 计及隐私数据保护的多虚拟电厂协同调度方法[J]. 天津大学学报(自然科学与工程技术版), 2024, 57(8): 836-846.
Yang Ting, Zhang Jian, Cai Shaotang, et al. Collaborative scheduling method for multivirtual power plants considering privacy data protection[J]. Journal of Tianjin University(Science and Technology), 2024, 57(8): 836-846(in Chinese).

[4] 苏 盛, 汪 干, 刘 亮, 等. 电力物联网终端安全防护研究综述[J]. 高电压技术, 2022, 48(2): 513-525.
Su Sheng, Wang Gan, Liu Liang, et al. Review on security of power internet of things terminals[J]. High Voltage Engineering, 2022, 48(2): 513-525(in Chinese).

[5] Buchta R, Heine F, Kleiner C. Challenges and peculiarities of attack detection in virtual power plants: Towards an advanced persistent threat detection system [C]//2022 IEEE 29th Annual Software Technology Conference. Gaithersburg, USA, 2022: 69-81.

[6] 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.

[7] Feng C S, Yu K P, Aloqaily M, et al. Attribute-based encryption with parallel outsourced decryption for edge intelligent IoV[J]. IEEE Transactions on Vehicular Technology, 2020, 69(11): 13784-13795.

[8] Wei F S, Vijayakumar P, Kumar N, et al. Privacy-preserving implicit authentication protocol using cosine similarity for internet of things[J]. IEEE Internet of Things Journal, 2020, 8(7): 5599-5606.

[9] Kim S, Mun H-J, Hong S. Multi-factor authentication with randomly selected authentication methods with DID on a random terminal[J]. Applied Sciences, 2022, 12(5): 2301.

[10] 陈 璐, 陈华智, 邓 松, 等. 电力内网终端的安全接入控制方法研究[J]. 电力信息与通信技术, 2014, 12(6): 1-5.
Chen Lu, Chen Huazhi, Deng Song, et al. Research on security access control method of power intranet terminal[J]. Electric Power ICT, 2014, 12(6): 1-5(in Chinese).

[11] Zhang X J, Chen L D, Fan J, et al. Power IoT security protection architecture based on zero trust framework [C]//2021 IEEE 5th International Conference on Cryptography, Security and Privacy. Zhuhai, China, 2021: 166-170.

[12] Chen Z Y, Yan L C, Lü Z T, et al. Research on zero-trust security protection technology of power IoT based on blockchain[C]//5th International Conference on Computer Science and Information Engineering(ICCSIE 2020). Dalian, China, 2021: 012039.

[13] Guo S Y, Hu X, Zhou Z Q, et al. Trust access authentication in vehicular network based on blockchain [J]. China Communications, 2019, 16(6): 18-30.

[14] Wang Y F, Wu L, Yang Y. Security authentication method of terminal trusted access in smart grid[J]. International Journal of Security and Its Applications, 2015, 9(7): 337-346.

[15] 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.

[16] Chen Y, Zhou X C, Zhu J, et al. Zero trust security of energy resource control system[C]//2022 IEEE 5th International Electrical and Energy Conference. Nangjing, China, 2022: 5052-5055.

[17] Lü Pang, Sun Xin, Huang Hui, et al. Dynamic trust continuous evaluation-based zero-trust access control for power grid cloud service[C]//2022 4th International Symposium on Robotics & Intelligent Manufacturing Technology(ISRIMT 2022). Changzhou, China, 2022: 012008.

[18] He Y H, Huang D C, Chen L, et al. A survey on zero trust architecture: Challenges and future trends[J]. Wireless Communications and Mobile Computing, 2022, 2022: 1-13.

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

[20] Fernandez E B, Brazhuk A. A critical analysis of zero trust architecture(ZTA)[J]. Computer Standards & Interfaces, 2024, 89: 103832.

[21] Zhao J, Huang J F, Xiong N X. An effective exponential-based trust and reputation evaluation system in wireless sensor networks[J]. IEEE Access, 2019, 7: 33859-33869.

[22] 康重庆, 陈启鑫, 苏 剑, 等. 新型电力系统规模化灵活资源虚拟电厂科学问题与研究框架[J]. 电力系统

自动化，2022，46(18)：3-14.
Kang Chongqing，Chen Qixin，Su Jian，et al. Scientific problems and research framework of virtual power plant with enormous flexible distributed energy resources in new power system[J]. Automation of Electric Power System，2022，46(18)：3-14(in Chinese).

[23] Che S Y，Feng R J，Liang X，et al. A lightweight trust management based on Bayesian and Entropy for wireless sensor networks[J]. Security and Communication Networks，2015，8(2)：168-175.

[24] 史慧洋，刘　鹏，王　鹤. 基于区块链和神经网络的威胁情报评估[J]. 天津大学学报(自然科学与工程技术版)，2022，55(5)：527-534.
Shi Huiyang，Liu Peng，Wang He. Threat intelligence evaluation based on blockchain and a neural network [J]. Journal of Tianjin University(Science and Technology)，2022，55(5)：527-534(in Chinese).

[25] Yang R，Wakefield R，Lyu S，et al. Public and private blockchain in construction business process and information integration[J]. Automation in Construction，2020，118：103-122.

[26] Etherden N，Vyatkin V，Bollen M H J. Virtual power plant for grid services using IEC-61850[J]. IEEE Transactions on Industrial Informatics，2015，12(1)：437-447.

[27] Fang W D，Zhang C L，Shi Z D，et al. BTRES：Beta-based trust and reputation evaluation system for wireless sensor networks[J]. Journal of Network and Computer Applications，2016，59：88-94.

[28] Fang W D，Zhang W X，Yang Y，et al. A resilient trust management scheme for defending against reputation time-varying attacks based on BETA distribution[J]. Science China Information Sciences，2017，60：1-11.

[29] 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.
Yu Jiexiao，Yu Liying，Yang Ting. Blockchain-based trust consensus method for power internet of things terminal[J]. Automation of Electric Power System，2021，45(17)：1-10(in Chinese).

[30] Powers D M W. Evaluation：From precision，recall and F-measure to ROC，informedness，markedness and correlation[EB/OL]. https://doi.org/10.48550/arXiv.2010.16061，2020-10-11.

(责任编辑：孙立华)