文章编号：2095-4980(2025)07-0711-09

一种基于信任值的有源配电台区“边-端”设备信任评估机制

张　磐，吴　磊，庞　超

(国网天津市供电公司 电力科学研究院，天津 300074)

摘　要：随着分布式能源的普及，有源配电台区内大量分布式“边-端”设备的身份认证和行为识别越来越具有挑战性。受损设备可能会危及配电网的安全性，恶意设备则可以通过注入虚假和恶意数据破坏网络的完整性。与高成本的基于密钥的安全方案相比，使用基于信任的安全性检测恶意节点是一种有效且轻量化的对策。本文提出一种高效信任值评估机制，可有效区分恶意设备，并防御开关和拒绝服务(DoS)攻击。使用贝叶斯估计方法收集并计算边端设备的直接和间接信任值，进一步考虑随时间收集的数据的相关性，通过应用两阶段信任评估框架，在动态环境中实现精确的信任评估，进而确保数据传输的安全性。与现有方法相比，提出的方法在恶意节点检测方面延迟更少，网络吞吐量更高。

关键词：分布式能源；身份认证；行为识别；信任评估

中图分类号：TM734；TN711　　**文献标志码：**A　　**DOI：**10.11805/TKYDA2025046

A trust value-based trust evaluation mechanism for "edge-to-end" devices in active distribution substation area

ZHANG Pan，WU Lei，PANG Chao

(Electric Power Research Institute，State Grid Tianjin Electric Power Company，Tianjin 300074，China)

Abstract：With the widespread adoption of distributed energy resources, the authentication of a large number of distributed "edge-to-end" devices and the identification of their behaviors within active distribution substations are becoming increasingly challenging. The damaged devices may jeopardize the security of the distribution network, while the malicious devices can disrupt the integrity of the network by injecting false and malicious data. Compared to high-cost key-based security solutions, employing trust-based security to detect malicious nodes is an effective and lightweight countermeasure. This paper proposes an efficient trust evaluation mechanism that can effectively distinguish malicious devices and defend against switch and Denial-of-Service(DoS) attacks. Using the Bayesian estimation method, the direct and indirect trust values of edge-end devices are collected and calculated, further considering the correlation of data collected over time. By applying a two-stage trust evaluation framework, accurate trust evaluation is achieved in dynamic environments, thereby ensuring the security of data transmission. Compared with existing methods, the proposed method has less delay in detecting malicious nodes and higher network throughput.

Keywords：distributed energy resource；identity authentication；behavior recognition；trust assessment

收稿日期：2025-02-24；**修回日期：**2025-04-05

基金项目：国网天津市电力公司科技资助项目(电科-研发　2023-41)

引用格式：张磐,吴磊,庞超. 一种基于信任值的有源配电台区"边-端"设备信任评估机制[J]. 太赫兹科学与电子信息学报, 2025,23(7):711-719. DOI:10.11805/TKYDA2025046.

Citation format：ZHANG Pan,WU Lei,PANG Chao. A trust value-based trust evaluation mechanism for "edge-to-end" devices in active distribution substation area[J]. Journal of Terahertz Science and Electronic Information Technology, 2025,23(7):711-719. DOI:10.11805/TKYDA2025046.

目前，全球范围内配电系统的转型正在加速推进。电力系统的脱碳进程推动了可再生能源资源的迅速增长，尤其是分布式能源资源(Distributed Energy Resources，DER)，如屋顶太阳能、风力涡轮机、电动汽车和储能设备等。这些技术的普及使传统的电力消费者逐步转型为“产消者”。随着可再生能源中DER的广泛应用，标准化、实时且安全的通信和协调控制需求愈发迫切[1-2]。智能配用电系统信息通信网络安全的核心原则可归结为机密性、完整性和可用性(Confidentiality，Integrity，Availability，CIA)三要素[3]。针对DER的潜在攻击不仅涉及通信协议，还包括对输电线路及其他关键组件的物理攻击，这些组件连接公共事业设施与DER[4]。此外，中间人攻击、数据完整性攻击(如导致电网电压过低或过高的攻击)、通过网络钓鱼邮件进行的数据注入攻击、拒绝服务(DoS)攻击等，都为DER的推广应用带来了巨大的挑战，并对配电网的安全性构成了全新的威胁[5]。

近年来，针对DER的网络攻击事件引起了广泛关注。2015年，乌克兰的3家地区电力配送公司遭遇网络攻击，导致停电数小时，影响了22.5万名客户。攻击者通过鱼叉式网络钓鱼邮件传播Black Energy 3恶意软件，从而劫持了监控与数据采集系统[6]。另一个典型案例是2003年俄亥俄州戴维斯–贝斯核电站遭受的Slammer蠕虫攻击。该蠕虫感染了核电站的两台计算机系统，导致系统瘫痪长达5 h，使控制室的工程师无法监控关键的安全参数与指标。该核电站的T1网络连接绕过了防火墙，给蠕虫攻击提供了路径。尽管安全补丁在攻击发生的六个月前已发布，系统工程师却未能及时安装[7]。此外，2022年印度最大的电力行业“Tata Power”遭受网络攻击，导致公司系统出现故障。为恢复系统的正常运行，公司不得不手动重新安装系统固件以恢复默认设置。这不仅耗费了大量时间和人力，还可能对电力供应的稳定性造成短期的干扰[8]。目前，针对有源配电台区中DER的信息安全问题，业界和学术界已展开了广泛研究。如，为了应对内部攻击，研究者们提出了基于信任和声誉的安全机制，用于评估通信节点的可靠性，并基于评估结果识别恶意节点[9]。在新兴的传感技术领域，由于节点通常部署在开放环境中，网络安全、防御对手以及确保数据的完整性、机密性和身份验证显得尤为重要。这些方法能够在保证较好的吞吐量和最小延迟的前提下提升安全性，但受限于传感器节点的资源限制，通过加密手段实现网络安全较为困难。此外，虽然传统安全方法能够有效应对外部攻击，但由于恶意节点已渗透到网络内部，这些方法对内部攻击的防御效果有限[10]。

通过信任机制，不仅能够解决访问控制和恶意节点检测问题，还提供了安全的端到端可信路由路径。此外，信任评估机制能够识别网络中的异常行为、故障和恶意节点，基于信任的安全方案通常是在节点层级通过与邻近节点的无线电交易构建的。文献[11]中提出了一种轻量级的分布式信任框架，能够抵抗Sybil攻击并保护用户匿名性。该信任机制通过贝叶斯方法和加权平均法进行直接和间接信任计算，同时利用声誉机制传播基于意见的决策。文献[12]提出了一种基于分层区块链架构的信任管理方案模型，用于处理分布式车联网节点。该方法减少全网存储开销与计算资源需求，但该系统高度依赖路侧单元(Road Side Unit，RSU)节点的计算资源和覆盖能力，一旦RSU受限或出现故障，可能影响信誉值更新和共识效率。文献[13]提出了一种基于社区模型的信任管理机制，旨在提升移动Ad hoc网络的安全性和可靠性。但该模型依赖社区内信任值最高的辅助节点进行信任评估，一旦这些辅助节点被恶意利用或遭受攻击，可能对整体信任计算产生较大影响。文献[14]采用指数分布对声誉进行估算，从而获得直接信任值，并利用滑动窗口和遗忘因子机制对直接信任值进行更新。基于熵理论，该方法对直接信任值的不确定性进行量化，并引入间接信任值以弥补直接信任评估中的偏差。通过对直接与间接信任值进行综合评价，从而提高了判断的准确性，并能有效抵抗开关攻击和共谋攻击。文献[15]提出了一种基于证书的安全机制，通过引入证书授权中心对各智能电子设备进行身份认证和公钥绑定，从根本上消除了未经授权的设备接入隐患。该方法不仅弥补了传统无证书方案的不足，还在满足实时性要求的前提下，有效提升了智能变电站通信网络的安全性，为智能电网的网络安全防护提供了一种具有实际应用前景的解决方案。

针对上述问题，本文提出了一种基于信任值的有源配电台区"边–端"设备信任评估机制。该机制不仅能够识别负责虚假报告的恶意边端设备，还能够提升网络的吞吐量和整体性能，并有效检测出各类攻击。

1 边端设备信任模型构建

传统中心化信任模型存在单点失效风险，而现有分布式方案往往缺乏对"边–端"网络动态特征的适应性，难以有效应对数据篡改、恶意节点入侵等复合型安全威胁。本文提出基于模块化架构的"边–端"设备信任模型：首先，通过流量监控模块记录和分析节点间的已发送、已接收和中继转发的数据包信息，记录各个节点的流量数据信息；其次，基于贝叶斯方法，构建直接和间接信任评估机制，为信任评估模块提供数据支持，以识别恶意节点并维护网络的可信性；最后，通过决策模块的信任评估机制通过结合短期动态监测和长期信誉累积，实现对通信节点的精准动态可信评估。3个模块通过协同工作机制形成"监测–评估–响应"的闭环系统，不仅能够有效

抵御恶意节点的攻击，还能在动态网络环境中保持较高的评估精确度和响应速度，对保障网络通信的安全性和稳定性具有重要意义。本文提出的"边-端"设备信任模型由 3 个模块组成，如图 1 所示。

1) 流量监控模块：该模块通过交换请求和响应数据包，对相邻节点的数据包转发行为进行监测，并记录流量配置文件中的关键信息，包括节点的 3 类流量数据：发送数据包、接收数据包和转发数据包。此外，该模块还存储节点间传输的总数据包信息，包括源节点和目标节点。通过实时监控这些数据，流量监控模块能够有效分析相邻节点的转发行为。

2) 信任评估模块：该模块依据节点间的历史交互情况，评估传感器节点的直接信任和间接信任。评估过程中，系统利用发送、接收及转发的流量配置信息作为衡量指标。基于这些数据，信任评估模块计算各节点的信任值，并将其传递至决策模块，以辅助决策过程。

3) 决策模块：该模块利用信任评估结果，将节点的信任值与预设阈值进行比较。若节点的信任值不低于阈值，则将其判定为可信节点；反之，若信任值低于阈值，则该节点被标记为恶意节点，并触发相应的隔离措施，以确保网络安全性。

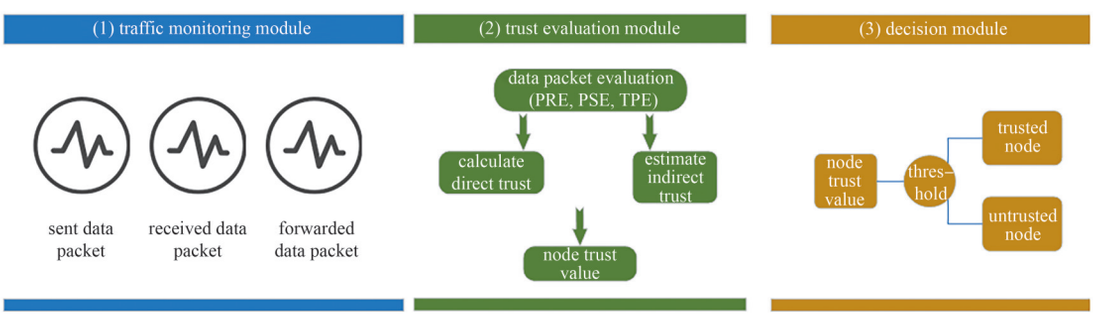

Fig.1 Overall framework of the trust evaluation mechanism

图 1　信任评估机制总体框架图

1.1　流量监控模块

流量监控模块通过交换请求和响应控制数据包观察相邻节点的数据包转发行为。这些控制数据包记录在每个节点的流量配置文件中，包含以下 3 类流量信息：

1) 已发送数据包：设节点 i 发送的数据包集合为 S_i，则节点 i 发送的数据包数量为：

$$|S_i| = \sum_{j=1}^{n} \mathbb{I}(S_{ij}) \tag{1}$$

式中：S_{ij} 为第 j 个发送的数据包，$\mathbb{I}(S_{ij})$ 为指示函数，当节点 i 发送 j 个数据包时，$\mathbb{I}(S_{ij})=1$，否则为 0；n 为节点 i 发送的数据包的总数。

2) 已接收数据包：设节点 i 接收的数据包集合为 R_i，则节点 i 接收的数据包数量为：

$$|R_i| = \sum_{j=1}^{m} \mathbb{I}(R_{ij}) \tag{2}$$

式中：R_{ij} 为第 j 个接收的数据包，$\mathbb{I}(R_{ij})$ 为指示函数，当节点 i 接收 j 个数据包时，$\mathbb{I}(R_{ij})=1$，否则为 0；m 为节点 i 接收的数据包的总数。

3) 传输数据包：设节点 i 转发的数据包集合为 T_i，则节点 i 转发的数据包数量为：

$$|T_i| = \sum_{j=1}^{p} \mathbb{I}(T_{ij}) \tag{3}$$

式中：T_{ij} 为第 j 个转发的数据包，$\mathbb{I}(T_{ij})$ 为指示函数，当节点 i 转发 j 个数据包时，$\mathbb{I}(T_{ij})=1$，否则为 0；p 为节点 i 转发的数据包的总数。

直接使用数据包的集合大小进行求和可能会导致错误计数，故使用指示函数 $\mathbb{I}(\cdot)$ 来判断某个数据包是否存在，并据此进行计数，防止无效数据包被错误计数，从而确保数据包的有效性。

此外，存储的信息还包括在节点之间传输的总数据包数量，涵盖源节点和目标节点。流量监控模块的工作原理如下：假设节点 i、j 和 k 为参与一跳邻居数据包转发的相邻节点，并且它们位于彼此的传输范围内。直接信

任的计算过程通过在时间“t”时刻，节点“i”向节点“j”传输数据包来完成，进而验证节点“j”是否将这些数据包成功转发给节点“k”。节点的可信度级别基于以下 3 个参数评估：

1) 数据包接收评估

$$R_{ij}(t)=\sum_{k=1}^{t} r_{ij}(k) \tag{4}$$

式中 $r_{ij}(k)$ 为时间 k 内节点 j 从节点 i 接收到的数据包数量。

2) 数据包发送评估

$$S_{ij}(t)=\sum_{k=1}^{t} s_{ij}(k) \tag{5}$$

式中 $s_{ij}(k)$ 为时间 k 内节点 i 发送给节点 j 的数据包数量。

3) 中转数据包评估

$$T_{ijk}(t)=\sum_{k=1}^{t} t_{ijk}(k) \tag{6}$$

式中 $t_{ijk}(k)$ 为时间 k 内节点 i 通过中间节点 j 发送给节点 k 的数据包数量。

流量监控模块通过观察节点 j 的数据包转发行为，帮助节点 i 获得节点 j 的真实行为。如果节点 j 的转发率与节点 i 发送的数据包相匹配，则节点 i 认为节点 j 是可信的。此外，节点 i 还可通过间接信任从其他相邻节点验证节点 j 的行为。

随着时间的推移，更多的流量数据会逐步更新信任度概率，而节点间的信任关系也可能因通信通道的不稳定而发生变化。为此，概率贝叶斯估计理论被用于信任度的计算与验证。最终，节点的信任度通过 3 个评估参数(数据包接收评估、数据包发送评估和传输数据包评估)确定。这种信任度计算方法通过持续监控和评估节点之间的交互行为，确保了网络内的信任关系是动态且准确的，并能够应对网络环境的变化。

1.2 信任评估模块的功能定义和工作机制

信任评估模块的主要任务是通过监控通信节点的转发、接收和传输行为，综合评估节点的可信度，并据此推测其是否为恶意节点或可信节点的概率。具体而言，当节点能够准确无误地将数据包转发至预定目标，并且这些转发行为被详细记录在流量配置文件中，且与相邻节点共享相关信息时，该节点会被判定为可信节点；反之，如果节点故意丢失数据包或篡改数据包的转发过程，通过在流量配置文件中伪造接收与转发的统计数据来掩盖其恶意行为，则该节点会被视为恶意节点。此外，为确保评估结果的精确性和可靠性，信任评估模块可分为 3 部分：信任接受者、信任评估者和决策者，三者共同协作，确保最终的信任评估结果符合系统的安全标准。

信任接收方由 3 个模块组成：流量评估指标、直接信任评估机制和间接信任评估机制。流量评估指标的关键组成部分包括：

1) 数据包接收评估：数据包接收评估用于计算在时间段 t 内，节点“k”成功接收到来自发送节点“i”的数据包所占的比例。发送节点与接收节点之间可能存在多个恶意节点，从而导致数据包丢失情况严重。接收节点从发送节点接收到的数据包数量被称为直接接收报告。接收到的数据包所占的比例为：

$$r_{ij}(t)=\frac{1}{N}\sum_{n=0}^{N-1}\frac{Pk_{ij}^{\mathrm{re}}(t-n)-Pk_{ij}^{\mathrm{re}}(t-n+1)}{Pk_{ij}^{\mathrm{re}}(t-n)+Pk_{ij}^{\mathrm{re}}(t-n+1)} \tag{7}$$

式中 $Pk_{ij}^{re}(t-n)$ 表示在指定时间间隔 t 内从发送节点到接收节点成功接收到的数据包总数。其中：i 表示发送节点，数据包的原始发送方(信任评估的发起者)；j 表示中间节点，负责转发数据的节点(被评估的节点)；k 表示接收节点，数据包的最终接收方。为更准确地描述被评估节点的状态，考虑了两个连续的时间间隔进行分析。分母部分则用于对结果进行归一化，以确保评估结果的标准化和可比性。

2) 数据包发送评估：数据包发送评估表示在时间段 t 内，节点 i 监测到从节点 j 发往节点 k 的数据包数量。此外，尽管中间节点成功转发到下一个节点的数据包无法被发送者直接监控，但如果它们位于相同的通信频道并且接收器处于开启状态，通信范围内的任何节点都能接收到这些数据包。因此，发送者依然可监控中间节点转发的数据包数量。数据包发送计算为：

$$a_{ij}(t)=\frac{Ps_{ij}^{\mathrm{re}}(t-n)}{Ps_{ij}^{\mathrm{re}}(t-n)+Prt_{ij}^{\mathrm{re}}(t-n+1)} \tag{8}$$

式中 $Ps_{ij}^{\mathrm{re}}(t-n)$ 为待传输的数据包。由于数据包未能成功接收，部分数据包需要进行重传。数据包未收到或需要重传的原因可能为信道损耗或存在恶意节点。假设网络中存在恶意节点，因此，重传的数据包也应纳入考虑，在式(8)中用 Prt_{ij}^{re} 表示。

3) 中转数据包评估：中转数据包评估表示在时间段 t 内，发送方 i 通过若干中间节点成功转发到接收节点 k 的数据包数量。在多跳环境中，节点很难直接与接收节点通信。当节点 j 更新其流量配置文件并将更新信息传递给节点 i 时，经过验证并确认信息的真实性后，该信息将被判断为可信或不可信。中间节点和接收节点的实际数据包传输量为：

$$Tpe_{jk}^{\mathrm{re}}(t-n)=\frac{Tp_{ij}^{\mathrm{re}}(t-n)-Tp_{ij}^{\mathrm{re}}(t-n+1)}{Tp_{ij}^{\mathrm{re}}(t-n)+Tp_{ij}^{\mathrm{re}}(t-n+1)} \tag{9}$$

式中 $Tpe_{jk}^{\mathrm{re}}(t-n)$ 表示从节点 j 发送到节点 k 的实际数据包传输量，包括中转数据包和中间节点实际接收到的数据包，TP 表示从节点 j 到节点 k 的实际传输数据包总量(包含中转包)。

模型评估频率为周期性评估，即在预设的固定时间间隔内，对网络节点的信任值进行动态调整，以实时反映其行为变化。具体而言，系统会收集最近一个评估周期内的数据包传输相关信息，包括数据包的传输成功率、丢失率，以及是否存在异常行为(如数据篡改或伪造记录)。经过经验验证，周期性评估的时间间隔 T 设为 40 s，在确保信任值实时性的同时，平衡了计算资源的消耗。

1.3 决策模块信任评估机制

两阶段信任评估机制结合短期动态监测与长期信任累积，优化设备节点的信任计算，确保系统在复杂环境下的鲁棒性。首先，短期动态信任评估采用滑动时间窗口和长短时记忆网络(Long Short-Term Memory，LSTM)模型计算短期信任值，并通过动态调整权重增强异常节点检测能力，使攻击行为迅速反映在信任计算中。其次，长期信任累积评估结合历史信任记录计算长期信任值，利用参数控制历史信任保留比例，并结合邻近节点的信任反馈提高评估可靠性，同时对恶意行为节点施加非线性衰减，通过恶意行为次数修正因子进行累积惩罚。最后，信任值通过风险等级调整权重进行自适应融合，计算最终信任值，并采用 Sigmoid 函数动态调整攻击发生时的权重，以缩短高风险响应时间，提高系统适应能力。该机制综合评估节点的短期行为特征与长期可信度，确保准确识别恶意节点并触发隔离措施，从而维护网络安全性。

两阶段信任评估流程通过短期行为动态监测与长期信誉累积反馈的协同优化，实现复杂攻击场景下的精准可信评估。具体流程如下：

1) 短期动态监测阶段：采用滑动时间窗(窗口长度 W_t)实时提取设备在边缘侧的行为特征，构建轻量化 LSTM 模型计算短期信任评分：

$$T_{\mathrm{short}}=f(S_{\mathrm{c}},D_{\mathrm{r}},U_{\mathrm{r}}) \tag{10}$$

式中：S_{c} 为通信成功率；D_{r} 为任务响应时延；U_{r} 为资源占用率。

结合联邦协同验证机制，通过云端加密对比跨区域节点行为特征，识别瞬时异常(如 $D_{\mathrm{r}}>\mu_{\mathrm{d}}+3\sigma_{\mathrm{d}}$ 时触发告警)。D_{r} 为任务响应时延，节点完成任务所需的响应时间；μ_{d} 为历史时延平均值，基于历史数据计算的任务响应时延均值；σ_{d} 为历史时延标准差，历史任务响应时延的波动性度量；$\mu_{\mathrm{d}}+3\sigma_{\mathrm{d}}$ 为异常检测阈值，时延正常范围的统计上界。

2) 长期信誉累积阶段：设计动态衰减因子 $\lambda(t)=\mathrm{e}^{-\tau t}$($\tau$ 为衰减系数)对历史评分进行指数衰减，强化近期行为权重，并通过贝叶斯信誉更新模型，融合多源交互数据：

$$R_{\mathrm{new}}=\alpha R_{\mathrm{history}}+(1-\alpha)\sum_{k=1}^{N}\beta_k R_k^{\mathrm{fed}} \tag{11}$$

式中：$\alpha\in[0,1]$ 为历史信誉保留因子；β_k 为联邦节点 k 的可信度权重(由云端联邦聚合结果动态计算)；R_{history} 为节点在过去累积的历史信任评分；R_k^{fed} 为对恶意节点实施惩罚后的实际信誉值。

对确认为恶意的节点施加非线性惩罚：

$$R_{\mathrm{mal}}=R_{\mathrm{pre}}\log\left(1+\eta C_{\mathrm{mal}}\right) \tag{12}$$

式中：η为惩罚强度；C_{mal}为恶意行为次数；R_{pre}为在施加惩罚前，节点根据历史行为计算的预期信誉值。

3) 两阶段自适应融合：基于环境风险等级L_{risk}动态调整权重，生成最终信任值：

$$T_{\mathrm{final}}=\gamma(L_{\mathrm{risk}})T_{\mathrm{short}}+[1-\gamma(L_{\mathrm{risk}})]R_{\mathrm{new}} \tag{13}$$

式中$\gamma(L_{\mathrm{risk}})$为 Sigmoid 函数。当攻击频率上升时$(L_{\mathrm{risk}}>L_0)$，短期评分权重$\gamma$显著增大，提升对突发威胁的响应速度。

阈值的选择方式为：首先设定基础阈值，基础阈值为预实验中恶意节点信任值的最大值；其次，当网络检测到恶意行为增加(如攻击频率升高、异常节点增多)时，提高信任阈值，减少恶意节点对系统的影响。动态调整的公式如下：

$$T_{\mathrm{new}}=T_{\mathrm{base}}+\alpha\times\frac{R_{\mathrm{a}}}{R_{\mathrm{a}}^{\max}}+\beta\times\frac{N_{\mathrm{e}}}{N_{\mathrm{e}}^{\max}} \tag{14}$$

式中：T_{base}为基础阈值，固定初始值为 0.5；R_a为攻击频率，即单位时间内检测到的攻击事件数；$R_{\mathrm{a}}^{\max}$为攻击频率最大值，即历史统计的最高攻击频率；N_{e}为异常节点比例，表达式为：当前异常节点数量/总节点数量；$N_{\mathrm{e}}^{\max}$为异常节点比例最大值，即历史统计的最高异常节点比例；α、β为调节系数，用于控制阈值调整幅度。

所提方法的算法如下所示，将流量配置文件作为输入，并将其分为发送、接收和传输数据包。

输入：通信概况(通信质量、节点状态、传输包信息)

输出：检测作为受信任/不受信任的节点

1：R_{ij}^{avg}(计算在过去间隔平均收到数据包）

2：S_{ij}^{avg}(计算平均发送数据包）

3：T_{ij}^{avg}(计算在过去间隔平均运输包）

4：$P(\mathrm{MN}|S_{ij}^{\mathrm{avg}})=P(\mathrm{PSE}|\mathrm{MN})\times P(\mathrm{MN})/P(S_{ij}^{\mathrm{avg}})$。MN 表示恶意节点；PSE 表示数据包发送事件。

5：if $P(\mathrm{MN}|S_{ij}^{\mathrm{avg}})>T_{\mathrm{h}}$

6：Then 标记为受信任设备

7：Else

8：标记为不受信任设备

9：更新数据库为先验概率

10：end if

算法的第 1~3 行：基于周期间隔计算所有 3 种类型数据包的平均值。第 4 行为基于贝叶斯估计理论计算节点为恶意或非恶意的概率。算法的第 5 行及以后，根据阈值评估计算出的概率，以将节点标记为可信或不可信。

所提出的基于信任度的信任评估机制(Trust Assessment Mechanism，TAM)可评估接收的数据包、发送的数据包和通过的传输数据包信息，结合直接信任值和间接信任值评估每个节点的信任级别以应对虚假报告并维护可信环境。

2 信任评估机制性能分析

2.1 仿真设定

为确定所提机制的性能，在离散事件模拟器 OMNET++中进行模拟测试。硬件平台选用 Intel Core i7−12700K 处理器，16 GB DDR4 内存，1 TB SSD 存储，操作系统为 Ubuntu 22.04 LTS，使用 Matlab 搭建仿真实验环境。“边−端”设备随机部署在天津市的某个有源配电台区中，节点的传输范围保持在 20 m[16]。传感器节点和接收器节点以相同的初始能量、计算和存储容量静态部署。对于不同的实验，模拟时间在 200~1 000 s 之间。最初，所有节点都表现为值得信赖，但随着时间的推移，一些节点表现得像恶意的。通过 Bad−Mouth(BM)、On/Off 和 DoS 攻击模拟恶意节点，为检测恶意节点，将信任更新周期设置为 40 s[17]。因此，实验中每个节点的信任值平均更新 25 次。为评估介于 0 和 1 之间的节点的可信度，将信任值阈值设为 0.5。除获得信任值外，阈值还用于区分可信节点和恶意节点，避免错误指控。网络上的流量为恒定比特率(Constant Bit Rate，CBR)类型，数据包大小设置为 50 byte[18]。由于反应性和按需性，将按需距离矢量路由协议(Ad hoc On−Demand Distance Vector，AODV)视为基线路由协议[19−20]。该仿真模型的参数设置如下：仿真区域大小为 100 m×100 m，节点布置方式为随机，仿真时间设定为 200~1 000 s 之间，数据流类型为用户数据报协议(User Datagram Protocol，UDP)，数据包大小为 50 byte，物理层标准采用 IEEE 802.15.4，流量负载采用 CBR，节点序号为 10、20、30、40 和 50。

2.2 恶意节点识别能力分析

第 1 个场景：在存在恶意传感器节点的情况下分析信任度，结果如图 2 所示。从图 2 可以看出，与自适应过滤的基于信任的节点选择(Adaptive Filtering Trust-based Node Selection，AF-TNS)[21]和 Trust-Doe[22]相比，所提出的 TAM 机制的信任度在不断提高，随着时间的推移，所提出的方法由于其在分析虚假报告和准确识别恶意节点方面的预测行为而获得了更高的信任度。

第 2 个场景：分析恶意传感器节点在整个场景中的比例从 10% 增加至 50%(每次增加 10%)时的信任度。为确保实验准确性，在 200~1 000 s 的不同模拟时间段进行实验观察，结果如图 3 所示。可以看出当恶意传感器节点增加时，信任度随之降低并在一定范围内维持稳定。

第 3 个场景：模拟恶意节点数量从 5% 增加至 45%。

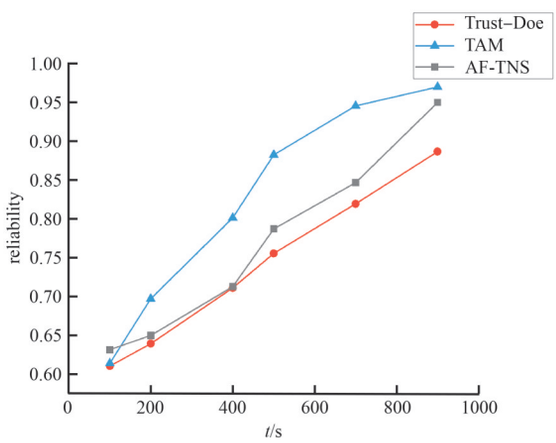

Fig.2 Degree of trust
图 2　信任度

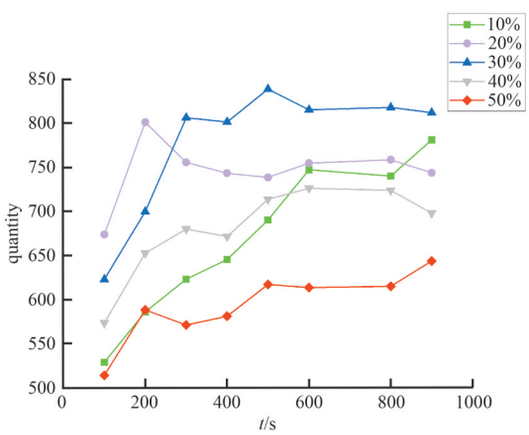

Fig.3 Trustworthiness when the number of malicious sensor nodes increases
图 3　恶意传感器节点增加时的信任度

图 4 为入侵签名检测算法(Intrusion Signature Detection Algorithm，ISDA)、基于信誉的安全协议算法(Reputation-based Security Protocol Algorithm，RSPA)和 TAM[23]对可信度的影响。该图只描述了 200 s 时的观测值。

仿真结果表明，所提出的 TAM 能有效检测节点的变化行为，且在各个比例下的可靠性均显著高于基于信誉的安全协议算法(RSPA)和入侵签名检测算法(ISDA)，表现出更强的抗攻击能力与鲁棒性。对恶意节点的早期检测和隔离可以节省重新传输数据包所需的带宽、传输功率和能量。由于提议的机制能够选择可信节点，并考虑到信任评估的误报率，因此能有效检测到攻击。

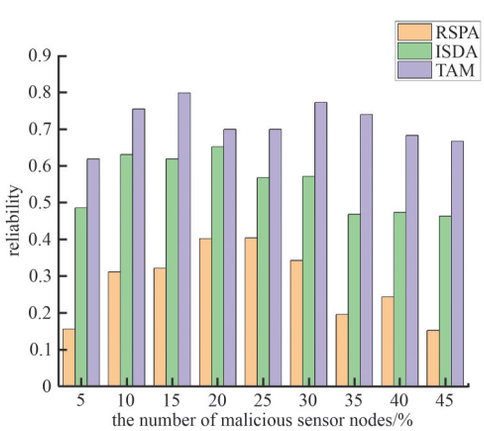

Fig.4 Credibility of malicious sensor nodes for different attacks
图 4　针对不同攻击的恶意传感器节点的可信度比例

3　结论

本文提出了一种基于信任值的有源配电台区“边-端”设备信任评估机制，可抵御恶意节点和内部攻击。在计算有源配电台区“边-端”设备的直接和间接信任值时采用了贝叶斯估计法，进一步考虑了一段时间内收集到的数据的相关性，然后将其进一步用于选择值得信赖的节点进行数据转发。仿真结果表明，与 AF-TNS 和 Trust-Doe 相比，所提出的机制具有更好的抵御 DoS 攻击的能力，不仅在一定程度上成功识别和隔离了恶意节点，还提高了假阳性检测率。在以后的研究中，将进一步改进该机制，抵御包括其他类型的恶意节点攻击，如 Sybil、选择性转发和虫洞攻击。

参考文献：

[1] 杨挺,党兆帅,王旭东,等. 混合交易模式下电力系统全环节碳排放核算方法[J]. 中国电机工程学报, 2025,45(1):38-52. (YANG Ting,DANG Zhaoshuai,WANG Xudong,et al. Carbon emission accounting method for the entire electricity system in the mixed trading model[J]. Proceedings of the CSEE, 2025,45(1):38-52.) DOI:10.13334/j.0258-8013.pcsee.232494.

[2] CHANG V,KUO Y H,RAMACHANDRAN M. Cloud computing adoption framework: a security framework for business clouds[J]. Future Generation Computer Systems, 2016(57):24-41. DOI:10.1016/j.future.2015.09.031.

[3] 张同须,余立. 信息通信技术若干发展趋势[J]. 电信科学, 2024,40(4):151-159. (ZHANG Tongxu,YU Li. Several development trends of information and communication technology[J]. Telecommunications Science, 2024,40(4):151-159.) DOI:10.11959/j.issn.1000-0801.2024075.)

[4] 张晓良. 电力信息网络安全协调控制防御理论及关键技术研究[D]. 北京:华北电力大学, 2023. (ZHANG Xiaoliang. Research on the theory and key technologies of coordinated control and defense for power information network security[D]. Beijing:North China Electric Power University(Beijing), 2023.) DOI:10.27140/d.cnki.ghbbu.2023.000197.

[5] 杨挺,李浩,赵宇明,等. 电力信息物理系统故障通信恢复策略[J]. 电网技术, 2025,49(1):381-389. (YANG Ting,LI Hao,ZHAO Yuming,et al. Fault communication recovery strategy of power cyber-physical system[J]. Power System Technology, 2025,49(1):381-389.) DOI:10.13335/j.1000-3673.pst.2023.0915.

[6] SHAIKH R A,JAMEEL H,D'AURIOL B J,et al. Group-based trust management scheme for clustered wireless sensor networks[J]. IEEE Transactions on Parallel and Distributed Systems, 2009,20(11):1698-1712. DOI:10.1109/TPDS.2008.258.

[7] YAO Zhiying,KIM D,DOH Y. PLUS:parameterised localised trust management based security framework for sensor networks[J]. International Journal of Sensor Networks, 2008,3(4):,224-236. DOI:10.1504/IJSNET.2008.019005.

[8] DEY A K,GUPTA G P,SAHU S P. EMTD: explainable malicious traffic detection model using hybrid deep learning techniques for industrial IoT networks[J]. Arabian Journal for Science and Engineering, 2024:2191-4281. DOI:10.1007/s13369-024-09578-2.

[9] ZHOU Hai, WU Yuanming, FENG Li, et al. A security mechanism for cluster-based WSN against selective forwarding[J]. Sensors, 2016,16(9):1537. DOI:10.3390/s16091537.

[10] MOMANI M,CHALLA S. Survey of trust models in different network domains[DB/OL]. arXiv, 2010:0168. (2010-10-01)[2025-02-24]. https://arxiv.org/abs/1010.0168 DOI: 10.48550/arXiv.1010.0168.

[11] QUERCIA D, HAILES S, CAPRA L. B-trust: Bayesian trust framework for pervasive computing[C]// The 4th International Conference on Trust Management. Pisa,Italy:Springer, 2006:298-312. DOI:10.1007/11755593_22.

[12] 刘代东,金睿,魏松杰. 基于联盟链的分布式车联网节点信誉管理系统[J/OL]. 计算机工程, 2024:1-13. (2024-08-08)[2025-02-24]. https://doi.org/10.19678/j.issn.1000-3428.0069457. (LIU Daidong,JIN Rui,WEI Songjie. Distributed vehicular network node reputation management system based on consortium blockchain[J/OL]. Computer Engineering, 2024:1-13. (2024-08-08)[2025-02-24]. https://doi.org/10.19678/j.issn.1000-3428.0069457.) DOI:10.19678/j.issn.1000-3428.0069457.

[13] 汪张生. 社区模型的移动 Ad hoc 网络信任管理方案[J]. 重庆大学学报, 2011,34(8):134-138. (WANG Zhangsheng. Trust management scheme for mobile Ad hoc networks based on community model[J]. Journal of Chongqing University, 2011,34(8):134-138.)

[14] KONG L,ZHAI F,ZHAO Y,et al. Evaluation method of trust degree of distribution IoT terminal equipment based on information entropy[J]. Journal of Physics Conference Series, 2021,1754(1):012108. DOI:10.1088/1742-6596/1754/1/012108.

[15] USTUN T S, HUSSAIN S M S. An improved security scheme for IEC 61850 MMS messages in intelligent substation communication networks[J]. Journal of Modern Power Systems and Clean Energy, 2020,8(3):591-595. DOI:10.35833/MPCE.2019.000104.

[16] FENG Renjian, XU Xiaofeng, ZHOU Xiang, et al. A trust evaluation algorithm for wireless sensor networks based on node behaviors and ds evidence theory[J]. Sensors, 2011,11(2):1345-1360. DOI:10.3390/s110201345.

[17] JIANG Jinfang, HAN Guangjie, WANG Feng, et al. An efficient distributed trust model for wireless sensor networks[J]. IEEE Transactions on Parallel and Distributed Systems, 2015,26(5):1228-1237. DOI:10.1109/TPDS.2014.2320505.

[18] BAO F Y,CHEN I R. Dynamic trust management for mobile networks and its applications[M]. Blacksburg,VA,United States: Virginia Polytechnic Institute & State University, 2013.

[19] SIMAREMARE H, ABOUAISSA A, SARI R F, et al. Security and performance enhancement of AODV routing protocol[J]. International Journal of Communication Systems, 2015,28(14):2003-2019. DOI:10.1002/dac.2837.

[20] SHAHABI Sina,GHAZVINI M,BAKHTIARIAN M. A modified algorithm to improve security and performance of AODV protocol against black hole attack[J]. Wireless Networks, 2016,22(5):1505-1511. DOI:10.1007/s11276-015-1032-y.

[21] ALFARRAJ O, ALZUBI A,TOLBA A. Trust-based neighbor selection using activation function for secure routing in wireless sensor networks[J]. Journal of Ambient Intelligence and Humanized Computing, 2018(15):1-11. DOI:10.1007/s12652-018-0885-1.

[22] NIE S. A novel trust model of dynamic optimization based on entropy method in wireless sensor networks[J]. Cluster Computing,

2017,22(l5):11153-11162. DOI:10.1007/s10586-017-1337-y.

[23] 张森强,唐朝京,张权,等. 基于攻击效能的网络攻击法分类与形式化描述[J]. 太赫兹科学与电子信息学报, 2004,2(3):161-166,175. (ZHANG Senqiang,TANG Zhaojing,ZHANG Quan,et al. Network attack classification on results and formal description[J]. Journal of Terahertz Science and Electronic Information Technology, 2004,2(3):161-166,175.) DOI:10.3969/j.issn.1672-2892.2004.03.001.

作者简介：

张　磐(1983-)，男，硕士，正高级工程师，主要研究方向为配电自动化、智能配用电技术.email:ator66w@163.com.

吴　磊(1985-)，男，硕士，高级工程师，主要研究方向为智能配电网和继电保护技术.

庞　超(1995-)，男，硕士，工程师，主要研究方向为智能配用电技术研究.

（上接第710页）

作者简介：

梁　铃(1988-)，女，学士，高级工程师，主要研究方向为电网调度自动化技术.email:lianglingaa@163.com.

姬　源(1979-)，男，学士，高级工程师，主要研究方向为电力调度自动化研究及应用.

黄育松(1978-)，男，硕士，高级工程师，主要研究方向为电网调度自动化技术.

覃　海(1988-)，女，学士，高级工程师，主要研究方向为电网调度自动化控制与运行管理.

代　江(1985-)，男，学士，高级工程师，主要研究方向为电网调度运行与管理.

张云菊(1973-)，女，学士，高级工程师，主要研究方向为主网自动化专业管理技术.

郭　明(1984-)，男，学士，高级工程师，主要研究方向为电网调度自动化技术.

石启宏(1994-)，男，学士，工程师，主要研究方向为电网调度自动化技术.

陈　飞(1987-)，男，博士，助理研究员，主要研究方向为数字孪生、信息物理融合、调度自动化.