Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.047767

ARTICLE

Enhancing Energy Efficiency with a Dynamic Trust Measurement Scheme in Power Distribution Network

Yilei Wang[1], Xin Sun[1], Guiping Zheng[2,3], Ahmar Rashid[4], Sami Ullah[5], Hisham Alasmary[6] and Muhammad Waqas[7,8,*]

[1]Zhejiang Electric-Power Corporation Research Institute, Zhejiang, 310014, China

[2]Faculty of Information Technology, Beijing University of Technology, Beijing, 100124, China

[3]Beijing Trusty Cloud Technology Co., Ltd., Beijing, 100022, China

[4]Department of Computer Science and Engineering, Ghulam Ishaq Khan Institute of Engineering Sciences and Engineering, Topi, 23640, Pakistan

[5]Department of Computer Science, Shaheed Benazir Bhutto University, Sheringal, Upper Dir, 18050, Pakistan

[6]Department of Computer Science, College of Computer Science, King Khalid University, Abha, 61421, Saudi Arabia

[7]School of Computing and Mathematical Science, Faculty of Engineering and Science, University of Greenwich, London, SE10 9LS, UK

[8]School of Engineering, Edith Cowan University, Perth, 6027, Australia

*Corresponding Author: Muhammad Waqas. Email: engr.waqas2079@gmail.com

Received: 16 November 2023 Accepted: 24 January 2024 Published: 26 March 2024

ABSTRACT

The application of Intelligent Internet of Things (IIoT) in constructing distribution station areas strongly supports platform transformation, upgrade, and intelligent integration. The sensing layer of IIoT comprises the edge convergence layer and the end sensing layer, with the former using intelligent fusion terminals for real-time data collection and processing. However, the influx of multiple low-voltage in the smart grid raises higher demands for the performance, energy efficiency, and response speed of the substation fusion terminals. Simultaneously, it brings significant security risks to the entire distribution substation, posing a major challenge to the smart grid. In response to these challenges, a proposed dynamic and energy-efficient trust measurement scheme for smart grids aims to address these issues. The scheme begins by establishing a hierarchical trust measurement model, elucidating the trust relationships among smart IoT terminals. It then incorporates multidimensional measurement factors, encompassing static environmental factors, dynamic behaviors, and energy states. This comprehensive approach reduces the impact of subjective factors on trust measurements. Additionally, the scheme incorporates a detection process designed for identifying malicious low-voltage end sensing units, ensuring the prompt identification and elimination of any malicious terminals. This, in turn, enhances the security and reliability of the smart grid environment. The effectiveness of the proposed scheme in pinpointing malicious nodes has been demonstrated through simulation experiments. Notably, the scheme outperforms established trust metric models in terms of energy efficiency, showcasing its significant contribution to the field.

KEYWORDS

IIoT; trusted measure; energy efficient

1 Introduction

The emergence of Intelligent Internet of Things (IIoT) has resulted in the overlap of many conventional engineering domains with information technology [1], the smart grid being one of them [2,3]. The application of IIoT in the construction of power distribution network has elevated the intelligence and automation of distribution operations and inspections, which, in turn, has provided a strong upgrade and intelligent integration support for the distribution network.

The sensing layer of IIoT in the power distribution network comprises of two components, namely the edge convergence layer and the end sensing layer [4]. The edge convergence layer is, in turn, mainly composed of intelligent fusion terminals, energy controllers and other devices (referred to as "station area fusion terminals"). This layer aggregates the data collected by sensors from across the power distribution network and makes use of the edge computing framework of the station area fusion terminal for data aggregation, processing, and local analysis. The objective is to ensure real-time data collection, instant processing, and regional autonomy to meet operational demands. The second layer, which is the end sensing layer, mainly consists of monitoring devices such as micro-powered wireless sensors, conventional wireless sensors, and wired sensors (collectively referred to as "low-voltage end-sensing units"). These sensors collect the information pertaining to operational status, environmental conditions, visualization information, and operation information of power grid equipment. The thorough approach leads to extensive equipment status sensing as well as a rapid response to operational demands.

Comprising two fragments, namely the remote communication network and the local power distribution network [5,6]. The primary focus of the remote power distribution network is to meet communication needs between the management platform and the station's fusion terminal, characterized by exceptional reliability, minimal latency, and the imperative to distinguish. The local power distribution network, on the other hand, satisfies the communication demand between the station area convergence terminal and the low-voltage end-sensing units (abbreviated as LVESU). In the context of the power distribution network, the specific demands on local distribution networks vary concerning bandwidth, capacity, real-time capabilities, reliability, and security [7–9].

The smart grid, with its growing number of LVESUs, places greater emphasis on the performance, energy efficiency and response speed of station fusion terminals, while also posing security risks to the power distribution network as well as the smart grid as a whole [10,11]. In recent years, a growing number of researchers have directed their focus towards examining security concerns intricately linked with the smart grid. These concerns encompass the trustworthiness of devices, user privacy, key management, trusted data transmission, as well as the confidentiality and integrity of messages. However, the large variations in computational capabilities and storage capacities among various terminals in the smart grid complicate the application of conventional verification and encryption mechanisms.

Trust measurement technology serves an approach to access the reliability of components in a system or network [12]. It leverages diverse metrics and algorithms to precisely gauge the trustworthiness of specific entities, whether they are devices, users, nodes, or other system components [13]. The use of trusted metrics technology can measure and analyze a large number of terminals in the perception layer of the smart IoT system in an all-round way, ensuring the reliability of end perception units and establishing the groundwork for the holistic security in the smart grid [14,15]. Consequently, it becomes imperative to thoroughly explore the trustworthy relationship of terminals in the local power distribution network and adeptly identify malicious terminals to uphold the security and service quality of the smart grid.

Addressing the aforementioned challenges, numerous researchers have put forth diverse solutions. Nevertheless, two primary deficiencies persist. Firstly, the existing solutions fall short in effectively tackling the resource constraints specific to LVESU devices, as they lack comprehensive measurements of both the hardware and software conditions of LVESUs. Secondly, prevailing metric models fail to establish a clear trust relationship between integrated terminals and LVESUs, introducing subjectivity into the evaluation process. This subjectivity poses challenges in accurately identifying malicious nodes within the system. In light of these gaps, we introduce a novel dynamic and energy-efficient trust measurement scheme tailored for distribution networks. The proposed scheme makes significant contributions in optimizing the trust evaluation process.

1. Establishing a network communication model within smart grids, we introduce a three-layer trust measurement framework. This model spans from the IoT management platform to substation integrated terminals and further to LVESUs. The implementation of hierarchical management facilitates precise measurements between devices, elucidating trust relationships among smart IoT terminals in distribution substations.
2. Employing multidimensional measurement factors, we conduct a comprehensive assessment of smart IoT terminals in distribution substations. This involves the integration of static environmental factors, dynamic behaviors, and energy states. By adopting this approach, we mitigate the impact of subjective elements on measurement results, ensuring a more robust evaluation.
3. Designing a detection process for malicious LVESUs, we incorporate threshold and deviation threshold determinations for trustworthiness. This process effectively identifies and eliminates any malicious terminal sensing units, thereby upholding the security and dependability of the smart grid environment.
4. We comprehensively consider the three measurement factors of static environment, dynamic behavior and energy state, which more truly reflects the state of LVESU. Compared with the existing schemes, it is verified that the proposed scheme is also superior to the existing schemes in malicious LVESU detection and energy consumption.

The subsequent sections are organized as outlined below: Section 2 furnishes the existing related work; Section 3 elaborates on the proposed trustworthy operation scheme for local communication networks in distribution substations; Section 4 validates the scheme through experiments, and lastly, Section 5 concludes the presented work in the manuscript.

2 Related Work

Currently, numerous researchers have made significant contributions to enhancing the security and privacy of IoT-related applications. Zong et al. [16] introduced a lightweight access control scheme to address the security concerns associated with consumer-level smart devices. This scheme utilizes blockchain technology to achieve deduplication and dynamic user revocation for smart consumer devices. To tackle the resource constraints of UAV terminals, Wang et al. [17] proposed a practical and lightweight mutual authentication protocol. This protocol is composed of bitwise XOR operations and a one-way hash function, leveraging blockchain technology to mitigate the challenges posed by a centralized trusted center. In a related development, Wang et al. [18] presented a framework oriented towards metaverse modeling for timely and secure data collection. This framework is based on crowd sensing and has been applied in healthcare scenarios to facilitate a bidirectional mapping of patient data between physical and virtual spaces.

There has also been considerable research exploring different trust assessment mechanisms to facilitate secure communication in IoT systems. For example, in Wireless AD Hoc Networks [19],

Wu et al. [20] have proposed a network trustworthiness metric model, namely BLTM, utilizing Beta and Link Quality Indicator (LQI) to combat insider attacks. In this work, the direct and recommended trustworthiness metric are calculated based on the LQI analysis mechanism. This method ensures greater accuracy and stability of low-quality link trustworthiness metrics. Competent in discerning sostile entities and malfunctioning nodes, this fuzzy Ad-hoc trustworthiness metric model by Soleymani et al. [21] effectively addresses the uncertainty and imprecision stemming from non-intrusive factors that impact network data download. The schemes mentioned above involve complex trust metric evaluations to compute the trustworthiness metric values of nodes, which results in higher accuracy; however, at the cost of higher system energy consumption. In addition, there are some schemes, such as [22–26], which can resist certain internal security attacks, but also have some other problems, such as higher energy consumption, high computational complexity, while considering notable network communication overhead.

The challenge of utilizing recommendation credibility metrics from other network nodes lies in the potential risk of dishonest recommendations. To enhance the trustworthiness metric of recommended third-party nodes, Shabut et al. [27] introduced a model and defense scheme based on recommendation trustworthiness metrics. This approach employs clustering techniques to dynamically filter attacks associated with dishonest recommendations, considering factors such as the frequency of interactions between nodes, information compatibility, and temporal closeness. Khanna et al. [28] proposed a novel Subjective Logic (SL) trustworthiness metric model designed for evaluating recommendations among adjacent nodes in ad hoc networks. Meanwhile, Xu et al. [29] presented an algorithm based on recommendation trustworthiness metrics, specifically a collaborative computation model, to determine data forwarding policies. While this algorithm notably improves nodes' ability to identify deceitful or harmful activities, it is crucial to emphasize that the trustworthiness metric model does not address the security of information transmitted by routing nodes, despite its effective enhancement of recommendation precision from external nodes. In a separate domain, Boakye-Boateng et al. [30] conducted trust research, where trust calculations were grounded in the familiarity of interaction among devices and the consequences of devices acknowledging requests. It is noteworthy that, in certain scenarios, engineers might consider queries as component of troubleshooting actions, potentially influencing the sequence of transmitted queries. Additionally, it is crucial to emphasize that there is currently no trust model establishing the correlation among trust levels and the comprehensive trustworthiness and the substation's risk status [31,32].

The Lightweight and Dependable Trust System (LDTS) proposed by Li et al. [33] divides the trustworthy metric decision scheme into two levels, i.e., trustworthy metric decisions at both cluster member and cluster head levels. The trustworthiness metric values based on cluster members are calculated using both direct and indirect trustworthiness metrics. LDTS utilizes feedback reports from cluster heads to specific nodes to build an indirect feedback database. This approach effectively reduces the feedback from malicious nodes and reduces the network risk in open or harsh environments. Alnumay et al. [34] proposed a wireless self-organized quantitative trustworthiness metric model based on ARMA/GARCH theory to calculate the recommended trustworthiness metric using β probability distribution combined with direct trustworthiness metric. Dhelim et al. [35] proposed a large scale IoT trustworthiness metric system by software-defined network approach to manage the trusted state among IoT entity devices, which can effectively detect large-scale attacks. Dang et al. [36] proposed a trusted metric model for smart grids, featuring large deviations in trusted dynamic threshold calculations, which effectively improves the efficiency and accuracy of these calculations. Even though, the above design scheme can effectively resist malicious fraud at the nodes, the use of multiple trust metrics in an integrated calculation process, making use of a static weighted sum, results in subjective prediction outcomes.

3 Trustworthy Operation Mechanism of Local Power Distribution Network in Power Distribution Network

This section provides an overview of the network mechanism within the distribution station network and formulates a detailed trusted operational mechanism based on the local power distribution network in distribution station area.

3.1 Overview

The standard power distribution network designed to facilitate the implementation of IIoT in power distribution comprises two primary segments: the remote power distribution network and local power distribution network. The primary focus of the remote power distribution network is to meet communication needs between the management platform and the station's fusion terminal, characterized by exceptional reliability, minimal latency, and the imperative to distinguish. It is characterized by significant data volumes, extensive coverage, and a reliable two-way communication. For low-voltage distribution, it mainly relies on 4G technology, and can be flexibly switched based on the availability of fiber optic and wireless network coverage in the distribution network.

On the other hand, the local power distribution network primarily serves communication needs between the fusion terminal in the power distribution network and the LVESU. With various service types, equipment variations, and deployment methods, the local network has specific requirements for bandwidth, capacity, real-time capabilities, reliability, and security. In low-voltage distribution power networks, the local network relies predominantly on RS485 wired connections and HPLC. Other communication methods are selectively employed based on specific operational needs within the power distribution network.

At the heart of ensuring the secure operation of a trusted network within the power distribution network lies the measurement of the trust relationship between the end sensing devices. The trustworthiness of a terminal can be defined as a belief in the terminal's ability to perform with reliability and safety within a specific contextual environment. The trustworthiness metric serves as a quantitative representation of a terminal's trustworthiness, and its magnitude signifies the trustworthiness of a power distribution network smart IoT terminal.

The trust metric model for IoT terminals in a distribution power network contains three types of physical devices: the IoT management platform, the power distribution network fusion terminal, and the low-voltage end sensing unit. The trust assessment is carried out through a hierarchical management approach among these devices.

The power distribution network fusion terminal plays a central role in aggregating data, performing edge computing, and integrating applications within the smart IoT systems of the power distribution network. It acts as a link between the information and physical nodes. To reduce the workload on the power distribution network fusion terminal, the IoT management platform divides its responsibilities to use the power distribution network fusion terminal only for collecting the data from LVESUs within a certain range. Finally, the IoT management platform aggregates and evaluates the data coming from the power distribution network fusion terminal, as collected from the LVESUs.

The architecture of this hierarchical trust measurement scheme is illustrated in Fig. 1. The trust measurement process occurs at two levels: The IoT management platform measures the power distribution network fusion terminal which, in turn, measures the LVESU.

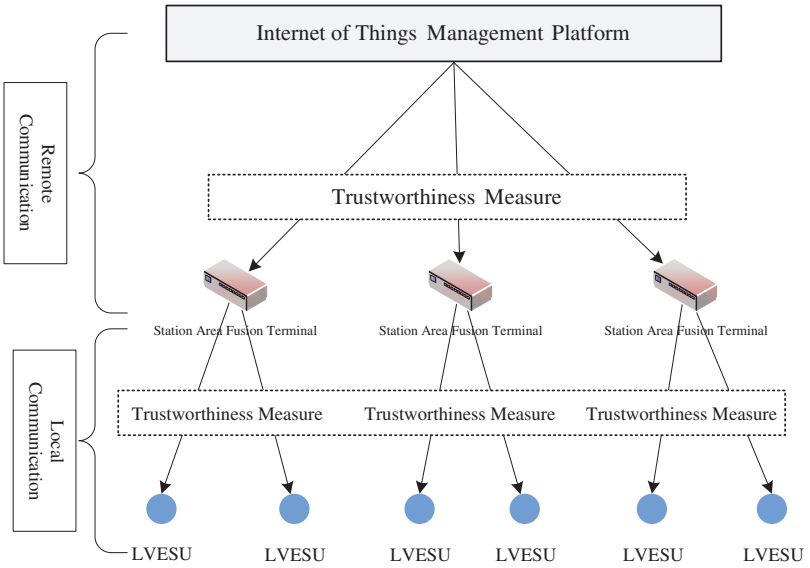


Figure 1: Trusted metrics architecture for smart IoT terminals in power distribution network

The assessment metrics include three aspects, which are static credible metrics, dynamic credible metrics, and energy credible metrics. The measurement process of the station fusion terminal to the LVESU is shown in Fig. 2. In addition, the trustworthiness metric or the LVESU is set in the range of 0–1. Here, '0' indicates that the terminal is completely untrustworthy while '1' indicates that the terminal is completely trustworthy.

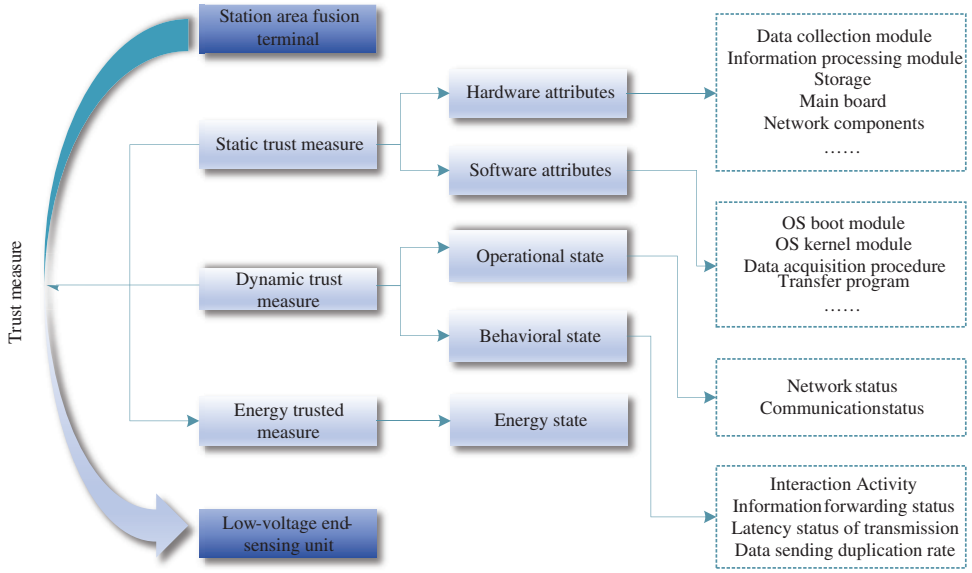


Figure 2: Specific contents of trustworthiness

3.2 Static Trust Measure for LVESUs

The static trusted metric is mainly a metric for the computing environment of the LVESU itself, which generally includes Software (SW) and Hardware (HW) attributes. Hence, the computing environment of the station fusion terminal can be rendered as $IA = (h, s)$, signifying the intrinsic properties of the LVESU within the smart grid. Here, *he* and *se* denote the characteristics of the HW and SW components of the LVESU, respectively.

The characteristics of HW components of the LVESU are referred to as $h = (h_0, h_1, h_2, \ldots, h_x)$, here $h_i\,(0 \le i \le x)$ specifies the characteristic values of individual HW components associated with the LVESU, and x is the amount of hardware attributes. These key HW components include network equipment, data processing module, data acquisition module, memory, motherboard, etc. The SW related information of the LVESU is denoted by $s = (s_0, s_1, s_2, \ldots, s_y)$, where each $s_i\,(0 \le i \le y)$ indicates the characteristic values of SW executing on LVESU, and y is the amount of software attributes. The main SW modules include the OS kernel module, OS boot module, data acquisition program, transmission program and other upper-layer running SW, etc.

In the centralized network approach, a LVESU in a region is denoted as $(p_1, p_2, \ldots, p_n)$, while a station area fusion terminal in the region is denoted as p_{fusion}, where n is the amount of LVESU. In this region, p_{fusion} is required to reliably verify the sensing environment of LVESU p_i based on security requirements. At time t, p_{fusion} acquires the static trustworthiness of p_i via the static trust assessment function $StmF_i(IA, t)$, based on the inherent property $IA_i = (h_i, s_i)$ of p_i. It then determines the trustworthiness of the sensing environment of p_i, similarly, the environmental trustworthiness of p_{fusion} is measured by its upper-level IoT management platform in a similar process. The following description solely focused on the measurement process of a regional station area fusion terminal for the low-voltage end-perception unit in the domain.

Based on the given information of running environment of p_i, the static trust metric function, $StmF_i(IA, t)$, initially needs to perform trust evaluation of HW attribute h_i and the SW attribute s_i, respectively.

For the HW attribute, $h_i = (h_{i0}, h_{i1}, h_{i2}, \ldots, h_{ix})$ of p_i, its reliability is determined through the HW static trust metric function $HStmF_i(IA\,(h_i), t)$, represented by Eq. (1).

$$HStmF_i\,(IA\,(h_i), t) = \prod_{j=0}^{x'} diff\left(h_{ij}, h_{ij}^{'}\right) * \frac{1}{x}\sum_{j=k+1}^{x} diff\left(h_{ij}, h_{ij}^{'}\right) \tag{1}$$

Here, $h_{ij}^{'}\,(0 \le j \le x')$ denotes the incipient HW state reported by p_i to its superior station fusion terminal p_{fusion} at the inception, $h_{ij}\,(0 \le j \le x)$ represents the HW condition of p_i at the moment t, and $diff\left(h_{ij}, h_{ij'}\right)$ signifies the difference between h_{ij} and $h_{ij}^{'}$. To emphasize the significance of core firmware, including data processing and data acquisition modules in the LVESU, $(h_{i0}, h_{i1}, \ldots, h_{ix'})$ is employed to denote the fundamental firmware characteristics of p_i, and x' denotes the amount of the core hardware attributes.

Similarly, for the SW attribute $s_i = \left(s_{i0}, s_{i1}, s_{i2}, \ldots, s_{iy}\right)$ of p_i, its reliability is determined through the SW static trust metric function $SStmF_i(IA\,(se_i), t)$, represented by Eq. (2).

$$SStmF_i\,(IA\,(s_i), t) = \prod_{j=0}^{y'} diff\left(s_{ij}, s_{ij}^{'}\right) * \frac{1}{y}\sum_{j=k+1}^{y} diff\left(s_{ij}, s_{ij}^{'}\right) \tag{2}$$

where $s_{ij}^{'}\ (0 \le j \le y')$ denotes the incipient SW state reported by p_i to p_{fusion} at the inception, $s_{ij}\ (0 \le j \le y)$ denotes the SW state of p_i at moment t, and $diff\left(s_{ij}, s_{ij}^{'}\right)$ signifies the variance from s_{ij} to $s_{ij}^{'}$. To emphasize the importance of core SW modules such as data processing program, operating system bootstrap program, operating system kernel program, and core data acquisition in the LVESU, $\left(h_{i0}, h_{i1}, \ldots, h_{iy'}\right)$ is employed to denote the core SW module of LVESU, and y' denotes the amount of the core software attributes.

Finally, at time t, the station fusion terminal p_{fusion} uses the function $StmF_i\ (IA, t)$ to compute the static trusted measure $StmV_i\ (t)$ of p_i, represented by Eq. (3).

$$StmV_i\ (t) = StmF_i\ (IA, t) = \alpha_1 HStmF_i\ (IA\ (h_i), t) + \alpha_2 SStmF_i\ (IA\ (s_i), t) \tag{3}$$

Here, α_1 and α_2 are the measurement weights for the HW and SW components, respectively and satisfy the condition $\alpha_1 + \alpha_2 = 1$. The exact values of α_1 and α_2 may be determined depending upon the specific scenario. The HW environment is generally considered to be equally important as the SW environment, i.e., $\alpha_1 = \alpha_2 = 1/2$.

3.3 Dynamic Trust Measure for LVESUs

The dynamic trusted measurement primarily involves the evaluation of the behavior and status of the LVESU during the data interaction process. Consequently, the station fusion terminal p_{fusion} should be evaluated separately by the operation behavior and status of the LVESU p_i. Likewise, the dynamic trusted measurement of the station fusion terminal p_{fusion} is mainly conducted by the IoT management platform.

The feature vector for the operational state of p_i is defined as $OperateStatus_i\ (OpS_0, OpS_1, \cdots, OpS_m)$, encompassing the network state, activity level, communication state, and more of the LVESU. The station fusion terminal p_{fusion} can compute a state trust metric for the operational state of the LVESU p_i based on Eq. (4).

$$SDtmV_i\ (OperateStatus_i, t) = \sum_{i=0}^{m} \left(\beta_i diff\left(OpS_i, OpS_i^{'}\right)\right) \tag{4}$$

where $OpS_i^{'}$ denotes the operational attributes of LVESU p_i at the previous moment step $t-1$. The $diff\left(OpS_i, OpS_i^{'}\right)$ signifies the distinction between $OpS_i^{'}$ and OpS_i, which is the difference between the current and previous states of sensing unit in question. The variable β_i denotes the importance or influence of Sta_i among all states and complies with $\beta_0 + \beta_1 + \cdots + \beta_m = 1$.

The behavioral state of the LVESU p_i is monitored by the station fusion terminal p_{fusion}, which can classify its behavior into 'expected behavior' or 'unintended behavior'. Expected behaviors generally include normal execution of commands, correct data transmission, correct data reception, timely data transmission, etc. Conversely, unintended behaviors generally include actions such as discarding commands or data, tampering with commands or data, and delayed data transmission. The station fusion terminal p_{fusion} measures the behavioral status of LVESU p_i, including interaction activity, the information forwarding status, the latency status of transmission, and status of Data Transmission Repetition Rate (DTRR), denoted respectively as $ActiveSta(p_{fusion}, p_i)$, $ForwardSta(p_{fusion}, p_i)$, $DelaySta(p_{fusion}, p_i)$, and $RepeatSta(p_{fusion}, p_i)$. The detailed formulations of the functions corresponding to *ActiveSta*, *ForwardSta*, *DelaySta* and *RepeatSta*, respectively, are given in the following paragraphs.

The formula for the Activity Metric Function, $ActiveSta\left(p_{fusion}, p_i\right)$ is as follows:

$$ActiveSta\left(p_{fusion}, p_i\right) = \frac{TotalComm\left(p_{fusion}, p_i\right)}{\sum_{j=0}^{j=n} TotalComm\left(p_{fusion}, p_j\right)} \tag{5}$$

where $TotalComm\left(p_{fusion}, p_i\right)$ denotes the total amount of communications between the station fusion terminal p_{fusion} and LVESU p_i, while n denotes the overall count of LVESUs.

$ActiveSta\left(p_{fusion}, p_i\right)$ specifies the share of the overall communications involving the station fusion terminal p_{fusion} and the LVESU p_i, with respect to all the interactions of the station fusion terminal p_{fusion}. A larger value of $ActiveSta\left(p_{fusion}, p_i\right)$ indicates a greater activity and interaction by the LVESU p_i, which in turn vouches for a stronger credibility of the unit. Conversely, a lower value implies a reduced credibility.

Next, the data forwarding status metric function, $ForwardSta\left(p_{fusion}, p_i\right)$ is formulated as:

$$ForwardSta\left(p_{fusion}, p_i\right) = \frac{TotalRequest\left(p_{fusion}, p_i\right)}{RealForward\left(p_{fusion}, p_i\right) + 1} \tag{6}$$

where $TotalRequest\left(p_{fusion}, p_i\right)$ indicates the aggregate amount of packets requested by the station fusion terminal p_{fusion} from the LVESU p_i, and $RealForward\left(p_{fusion}, p_i\right)$ indicates the aggregate amount of packets indeed forwarded by the LVESU p_i to the station fusion terminal p_{fusion}. $ForwardSta\left(p_{fusion}, p_i\right)$ shows the real data forwarding rate of the LVESU p_i. A higher result indicates a greater data forwarding capability with a low possibility of malicious behavior, which in turn signifies a higher trustworthiness in data forwarding; conversely, a lower value implies lower trustworthiness.

Then, the data transfer delay condition metric function, $DelaySta\left(p_{fusion}, p_i\right)$ is formulated as:

$$DelaySta\left(p_{fusion}, p_i\right) = \begin{cases} \delta^{\frac{Time_{Threshold} - Time_{Transmission}}{Time_{Threshold}}}, Time_{Threshold} \geq Time_{Transmission} \\ 1 \qquad\qquad\qquad\qquad\quad , Time_{Threshold} < Time_{Transmission} \end{cases} \tag{7}$$

where $\delta > 1$, $Time_{Transmission}$ represents the real Data Transmission Time (DTT) of LVESU p_i, while $Time_{Threshold}$ represents the DTT threshold. The δ and $Time_{Threshold}$ are decided by the security guidelines specified by p_{fusion} for the LVESU p_i. If the real DTT of LVESU falls within the acceptable range and the larger result of $DelaySta\left(p_m, p_i\right)$ suggests a negligible DTT for the LVESU, which means that the sensing unit is deemed effective in terms of data delay. On the other hand, if the DTT is long enough, it results in a smaller result of $DelaySta(p_{fusion}, p_i)$, indicating a weaker credibility of the LVESU.

Finally, the data sending repetition rate metric function, $RepeatSta\left(p_{fusion}, p_i\right)$ is formulated as follows:

$$RepeatSta\left(p_{fusion}, p_i\right) = \begin{cases} 2 - \delta^{ReRate}, ReRate < ReRate_{Threshold} \\ 0 \qquad\quad , ReRate \geq ReRate_{Threshold} \end{cases} \tag{8}$$

where $\delta > 1$, $ReRate$ is the DTRR of the LVESU p_i and the DTRR threshold is $ReRate_{Threshold}$. The values δ and $ReRate_{Threshold}$ are defined by the security policy specified by the station fusion terminal p_{fusion} for the LVESU p_i. If the DTRR of p_i increases than predefined threshold value, the sensing unit is deemed to exhibit malicious behavior, indicating a potential malicious sensing unit.

As a result, its trust value in this regard is set to 0, lowering the overall trustworthiness of this sensing unit. On the other hand, if the DTRR of the LVESU is within the threshold, and the repetition

rate is lower (i.e., a smaller *ReRate*), a larger value of $RepeatSta\,(p_m, p_i)$ under these conditions suggests a high credibility of the LVESU with respect to DTRR. Conversely, a higher repetition rate (i.e., a larger *ReRate*) results in a smaller value of $RepeatSta\,(p_m, p_i)$ indicating a lower credibility of the sensing unit in question.

The station fusion terminal p_{fusion} can assess the confidence in the behavioral performance state of the LVESU p_i through the Eq. (9).

$$BDtmV_i\,(BehaviorState_i, t) = \kappa_1 ActiveSta + \kappa_2 ForwardSta + \kappa_3 DelaySta + \kappa_4 RepeatSta \tag{9}$$

where $\kappa_1, \kappa_2, \kappa_3, \kappa_4$ suggest the relative weights of the interaction activity, the information forwarding status, the latency status of transmission, and DTRR, respectively, of the LVESU p_i in evaluating its overall behavioral performance. These weights meet $\kappa_1 + \kappa_2 + \kappa_3 + \kappa_4 = 1$, and their specific values can be decided based on the actual environment and security policy.

After obtaining the state trusted metric as well as the behavioral trust metric of p_i, the station fusion terminal p_{fusion} executes the dynamic trust measurement function $DtmF_i(OperateStatus_i, BehaviorState_i, t)$ to compute the dynamic trusted measurement value, $DtmV_i(t)$, for the LVESU p_i based on Eq. (10).

$$\begin{aligned} DtmV_i\,(t) &= DtmF_i\,(OperateStatus_i, BehaviorState_i, t) \\ &= \lambda_1 SDtmV_i\,(OperateStatus_i, t) + \lambda_2 BDtmV_i\,(BehaviorState_i, t) \end{aligned} \tag{10}$$

where λ_1, λ_2 denote the weight factors for the state metric and the behavior metric, respectively, and satisfy the condition $\lambda_1 + \lambda_2 = 1$.

3.4 Energy Trusted Measure for LVESUs

The LVESUs are generally deployed in environments where they cannot be charged in a timely manner; therefore, the energy status of the LVESUs is critical for terminal information collection.

The energy consumption of a LVESU primarily involves sensing data collection, packet transmission, packet reception, and ensuring the regular functioning of this unit. Therefore, the remaining energy state of LVESU p_i at moment t in the following manner.

$$\begin{aligned} RemainEnergy_i\,(t) &= InitialEnergy_i - Energy_i\,(Reception) \\ &\quad - Energy_i\,(Send) - Energy_i\,(Collection) - Energy_i\,(Run) \end{aligned} \tag{11}$$

where $InitialEnergy_i$ denotes the incipient energy value of p_i, i.e., its energy at time 0. $Energy_i\,(Reception)$ shows the total energy consumed by unit p_i for packet reception from time 0 to t, while $Energy_i\,(Send)$ shows the total energy consumed for packet transmission in this time interval time. Finally, $Energy_i\,(Collection)$ shows the total value of energy consumption during the data collection and $Energy_i\,(Run)$ accounts for other energy consumed by the LVESU p_i to maintain its own normal operation. The calculations for $Energy_i\,(Reception)$ and $Energy_i\,(Send)$ are given in the following paragraphs.

The energy required for packet reception by LVESU p_i is computed as:

$$Energy_i\,(Reception) = PacketNum_{Reception} * len_{Reception} * SingleEnergy_{Reception} \tag{12}$$

where $PacketNum_{Reception}$ denotes the overall count of packets received by p_i in the time interval ranging from 0 to t. $len_{Reception}$ indicates the length of individual packets, while the amount of energy consumed by the LVESU p_i to receive one-unit length of data is denoted by $SingleEnergy_{Reception}$.

The energy required for packet transmission by LVESU p_i is calculated as:

$$Energy_i(Send) = PacketNum_{Send} * len_{Send} * SingleEnergy_{Send} \tag{13}$$

Eq. (13) illustrates the calculation of $Energy_i(Send)$. Here, $PacketNum_{Send}$ signifies the overall count of data packets sent by p_i during the time period from 0 to t. len_{Send} denotes the length of individual data packets, while $SingleEnergy_{Send}$ denotes the energy consumed by unit p_i to send one-unit long data.

After obtaining the remaining energy status $RemainEnergy_i(t)$ of sensing unit p_i, the station fusion terminal conducts a credible energy measurement of this unit using the energy credibility measurement function $EtmF_i(RemainEnergy_i, t)$. Thus, calculating the energy credibility measurement value $EtmV_i(t)$, as formulated in Eq. (14).

$$\begin{aligned} EtmV_i(t) &= EtmF_i(InitialEnergy_i, RemainEnergy_i(t)) \\ &= \begin{cases} 2^{\frac{RemainEnergy_i(t)}{InitialEnergy_i}} - 1 & , RemainEnergy_i(t) \geq Energy_{Threshold} \\ 0 & , RemainEnergy_i(t) < Energy_{Threshold} \end{cases} \end{aligned} \tag{14}$$

where $Energy_{Threshold}$ indicates the energy threshold of the LVESU p_i; its value is determined by the corresponding power distribution network convergence terminal p_{fusion}. If the remaining energy of p_i falls below the predefined threshold value, indicating that this unit may no longer function as a reliable data collection and transmission unit. Therefore, when the remaining energy of this LVESU surpasses the specified threshold, a higher energy trust value is assigned due to a larger remaining energy; conversely, if the remaining energy falls below the threshold, a lower energy trust value is assigned, impacting the overall reliability of the LVESU.

3.5 Detection and Rejection of Malicious LVESUs

With the passage of time, LVESUs may be subjected to attacks or natural damage. It, therefore, becomes necessary to periodically perform measurements over these units and timely identify and eliminate malicious or non-functional units. The remaining energy of some of the sensing units may not be enough to perform their computational tasks, or they may have certain vulnerabilities in their operational environment, or can even exhibit malicious behaviors. Collectively, these units are referred to as malicious LVESUs. Fig. 3 illustrates the process of detecting such a malicious unit.

The station fusion terminal calculates cumulative trustworthiness using the trust measurement results of the static environment, dynamic behavior, and energy state of the LVESU. The weights assigned to these three aspects can be fine-tuned based on the specific circumstances. When assessing the overall trustworthiness of LVESUs in the domain, or upon receiving information from the IoT management platform, the terminal first determines whether the cumulative trustworthiness of each sensing unit in the domain falls below the trust threshold $CtmV^{ON}_{Threshold}$ for inter-domain LVESUs.

If the cumulative trustworthiness $CtmV_i(t)$ of LVESU p_i at the time t meets the condition $CtmV_i(t) \geq CtmV^{ON}_{Threshold}$, it means that the unit p_i is within the normal range in terms of its operating environment, behavior and energy state in that assessment cycle. It is considered a normal LVESU for that evaluation cycle. However, if $CtmV_i(t) < CtmV^{ON}_{Threshold}$, the LVESU p_i may be malicious and is subsequently detected for the subsequent phase. The primary component of the detection method involves assessing whether the difference $CtmVDev_i(t, t-1)$ among the current value of the cumulative trustworthiness $CtmV_i(t)$ of LVESU p_i and its previous value $CtmV_i(t-1)$ is less than a predefined threshold $CtmVDev_{Threshold}$, where Eq. (15) is the calculation method for the deviation

$CtmVDev_{Threshold}$. The calculation of the deviation $CtmVDev_{Threshold}$ is depicted in the following manner:

$$CtmVDev_i(t, t-1) = |CtmV_i(t-1) - CtmV_i(t)| \tag{15}$$

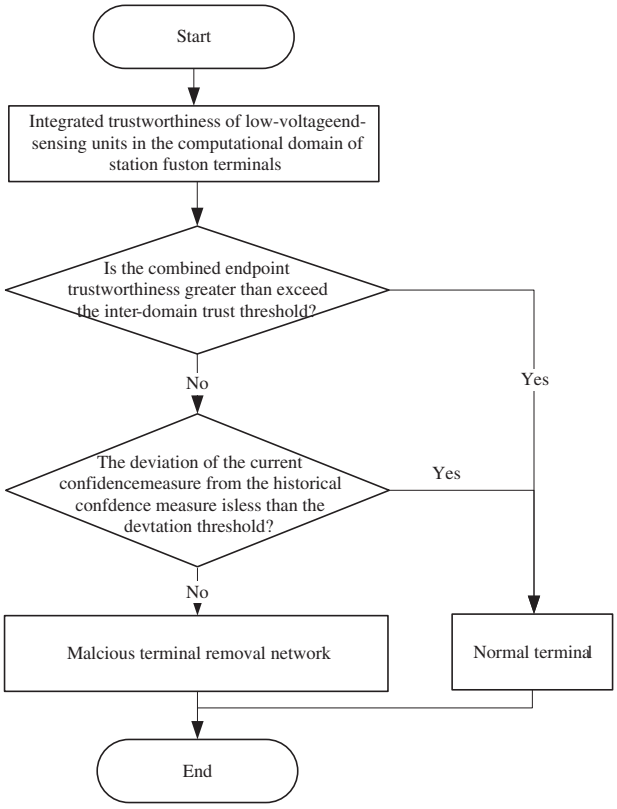


Figure 3: Malicious low voltage end sensing unit detection process

If the deviation is small, it indicates that the LVESU is a normal sensing unit. In the event of a significant deviation, two scenarios may occur:

1. When $CtmV_i(t) - CtmV_i(t-1) > CtmVDev_{Threshold}$, it suggests a substantial increase in trustworthiness, indicating that the LVESU is engaging in masking behavior.
2. When $CtmV_i(t-1) - CtmV_i(t) > CtmVDev_{Threshold}$, it means that the trust level of the LVESU has significantly diminished, suggesting either insufficient energy or a compromised state.

4 Experimental Verification and Analysis

This section presents a comprehensive simulation replicating a communication scenario within a power distribution network.

4.1 Experimental Environment Configuration

The simulations has been run using Matlab on a Windows System equipped with Intel (R) Core (TM) i5-6500 CPU @ 3.20 GHz 3.19 GHz processor. Table 1 provides an overview of the simulation parameters applied during these numerical experiments. In our work, we set the parameters in the table

because it aligns with the specific requirements of our experimental setup and is consistent with the characteristics of LVESU in the context of our smart grid background.

Table 1: Simulation variables

Parameter	Value
Simulation area size	100 m × 100 m
The overall count of LEVSUs	100
The count of malicious LEVSU	5%∼30%
Data transfer efficiency	15∼100 Kbps
Packet size	40 bit
Detection interval	1000 ms
Initial energy of low-pressure terminal sensing unit	1 J
Initial energy of fusion terminal in power distribution network	5 J

The initial distribution of network devices is illustrated in Fig. 4. In this figure, the black node represents the LVESU, the blue node represents the fusion terminal of the station area, and the red node represents the malicious LVESU.

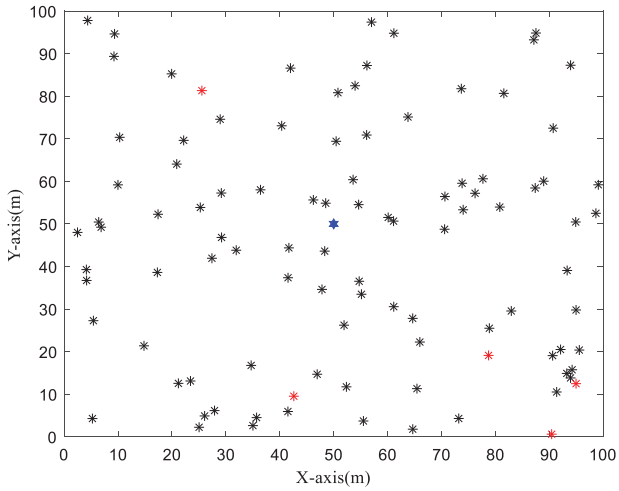


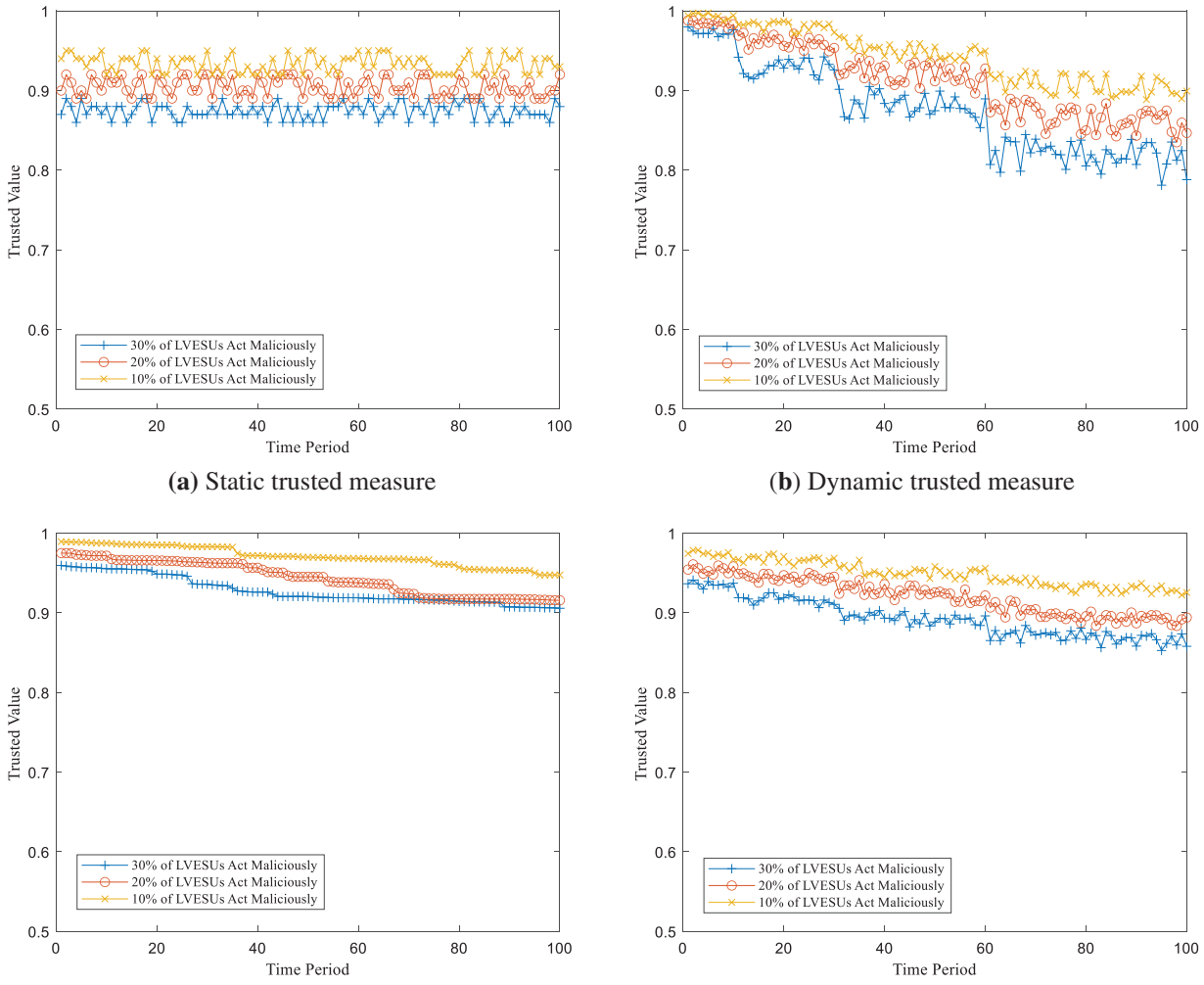
Figure 4: The initial position and state of nodes

4.2 Experimental Results and Analysis

We offer a thorough analysis of the trust measures within the proposed scheme which include the static, dynamic and energy trust measures. The effectiveness of detecting various proportions of malicious terminals is then analyzed. Finally, the energy consumption is compared with that of relevant schemes.

Fig. 5a shows the static environment trust measures corresponding to each terminal. With the increase of detection period, its static reliability value almost remains unchanged. This is because for the entire network, the probability of the basic software and hardware environment coming under attack remains the same, leading to fluctuations between 85% and 95%. However, it is evident that

a higher proportion of malicious devices leads to lower average trust values among terminals. Since malicious terminals may carry viruses themselves, the corresponding software environment undergoes change over time, thus, reducing the overall average trust value.



(a) Static trusted measure

(b) Dynamic trusted measure

(c) Energy trusted measure

(d) Comprehensive trusted measure

Figure 5: Static trusted measure

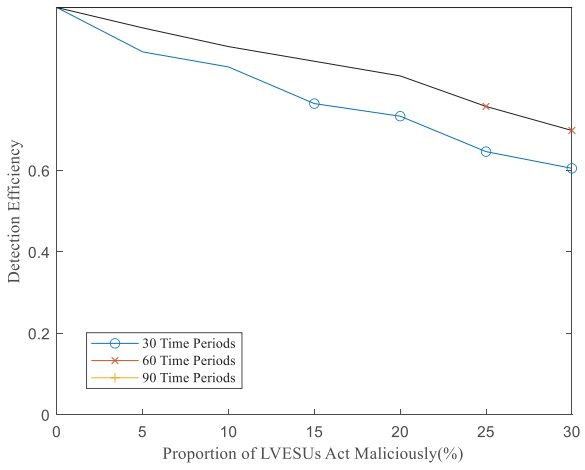
Fig. 5b shows the trust measure for dynamic behavior and the state corresponding to the terminal. With the extension of detection cycle, the dynamic trust value gradually decreases. As the time passes by, the behavior of the malicious LVESU is gradually discovered by the platform fusion terminal, which results in a reduced credibility value. In line with the static measures, an increased proportion of malicious devices leads to lower average trust values for the terminals.

Fig. 5c represents a trusted measure of the energy state corresponding to the terminal sensing units. As the detection period is extended, the energy trust value gradually decreases. This is attributed to the fact that, over time, various communication and interaction activities of the LVESU deplete the energy of the terminals, resulting in a decline in energy trust values. Furthermore, a higher proportion of malicious devices leads to smaller average trust values for the terminals. It is important to note that

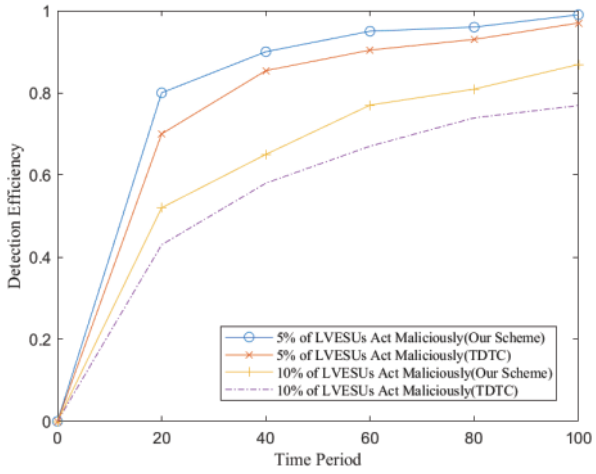
a terminal cannot be classified as malicious unless it engages in malicious behaviors. However, if it does, it consumes more energy for sending and receiving packets than a normal terminal.

Fig. 5d represents the result of the average trustworthiness measure of all the nodes in the network. It is easy to see that the combined trustworthiness value of the nodes decreases gently over time, and the higher the proportion of malicious nodes, the relatively lower the overall trustworthiness value. This result indicates the adverse impact of malicious LVESUs on the network's trustworthiness. With the gradual decline of trustworthiness, especially when there are a large number of malicious entities, the integrity of the network exposes potential vulnerabilities. This provides a key condition in the security defense strategy to mitigate the adverse impact of malicious LVESUs on the overall trustworthiness of the network.

In Fig. 6, we performed an in-depth analysis of the effectiveness in detecting malicious nodes, illustrating the ratio of detected malicious nodes to the true number of malicious LVESUs. In experiment, the malicious LVESU performs abnormal operations by simulating specific network events or behaviors, aiming to mislead the fusion terminal in the station area to evaluate it. This includes deceptive behavior, as well as illegal LVESUs launching attacks by means such as transmitting false information. We employed the detection method introduced in Section 3.5.



(b) Variation of detection rate with proportion of malicious nodes



(b) Comparison of detection rate with TDTC

Figure 6: Malicious terminal identification efficiency

Fig. 6a illustrates the variation in detection efficiency of our approach as the proportion of malicious nodes increases. Within the same detection cycle, the efficiency gradually decreases with the rising proportion of malicious terminals, reaching an overall detection rate of around 80%. The substantial presence of malicious terminals has a notable impact on the dynamic behavior assessment between terminals, influencing the judgment of fusion terminals and subsequently leading to a decline in detection efficiency. However, as the detection cycle extends, malicious terminals are almost always successfully identified.

Additionally, we compared our approach with TDTC [29], and the results are depicted in Fig. 6b. As the detection cycle is prolonged, both approaches exhibit enhanced efficiency in detection. In scenarios with an equivalent proportion of malicious nodes, our approach demonstrates higher detection

efficiency. This superiority arises from our approach not only integrating static trust metrics, dynamic trust metrics, and energy trust metrics for comprehensive terminal assessment but also introducing a bias threshold determination method in malicious node detection. This prevents malicious nodes from engaging in deceptive evaluations, thereby crucially enhancing detection efficiency.

Energy consumption refers to the energy consumed through trust evaluation and data transmission. The residual energy of the terminal is calculated by Eq. (16).

$$E_{Res} = E_{Initial} - E_{Transfer} - E_{Compute} \tag{16}$$

where $E_{Initial}$ represents the terminal initial energy, $E_{Transfer}$ is the energy consumed for data transmission, and $E_{Compute}$ is the energy consumed for computation. In the same time period, the less energy consumption, the more residual energy of the terminal, the higher energy efficiency, otherwise, vice versa.

Fig. 7 plots a comparison of the proposed scheme with that presented in TDTC concerning energy consumption usage. It is evident that, like the energy reliability value, the energy consumption gradually increases while the energy residual rate gradually decreases over the passage of time. Furthermore, it is readily noticeable that as the number of malicious terminals rises, there is a gradual rise in energy consumption, leading to a gradual decrease in the energy residual rate. It is further observed that, initially, the proposed scheme has a shorter detection cycle, with little difference in energy residual rate in comparison to TDTC. However, with the passage of time, the proposed scheme witnesses higher energy residual rate than TDTC. This is because the proposed scheme comprehensively evaluates the network status, communication status, and activity of LVESUs during dynamic measurements, promptly identifying abnormal terminal data and taking preventive measures such as strategic repairs and warnings to reduce unnecessary energy consumption.

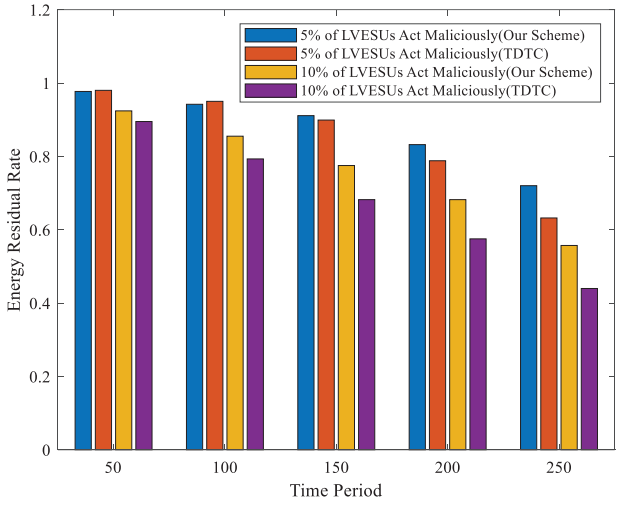


Figure 7: Terminal transmission energy consumption

5 Conclusion

This paper focuses on the power distribution network and introduces a dynamic trust measurement method utilizing the hierarchical structure of LVESU in the distribution network. The trust measurement process consists of three key components: environmental trust evaluation, behavioral

trust judgment, and energy residual state calculation. Through these steps, the secure operation of the local communication network within the distribution network is ensured. The environmental trust evaluation focuses on the trust level of LVESU in specific environments, behavioral trust judgment considers whether the operational behavior of LVESU meets expectations, and energy residual state calculation focuses on the energy consumption of LVESU. The comprehensive assessment of these three aspects constitutes the overall trust level evaluation of LVESU. Through simulated experiments, the proposed trust measurement method demonstrates lower energy utilization in identifying and removing non-trusted nodes in the network compared to previous models. This not only contributes to improving the performance and response speed of LVESU but also lays the foundation for maintaining the security and service quality of the entire smart grid. In conclusion, this trust measurement method provides strong support for the trustworthy operation of the smart grid, addressing the limitations of existing approaches in LVESUs' resource constraints and trust relationship establishment. However, the work in this paper is validated through simulated experiments, and there may be differences between the experimental environment and actual application scenarios. Therefore, future research and improvements will focus on enhancing the practicality and applicability of the proposed method.

Acknowledgement: The authors acknowledge the support from King Khalid University for funding this research through the Large Group Project under Grant Number RGP.2/312/44.

Funding Statement: This project is partly funded by Science and Technology Project of State Grid Zhejiang Electric Power Co., Ltd. "Research on active Security Defense Strategies for Distribution Internet of Things Based on Trustworthy, under Grant No. 5211DS22000G".

Author Contributions: The authors' contributions are outlined as follows: Yilei Wang: Conceptualization, Software, Validation, Formal analysis, Writing-original draft; Xin Sun, Guiping Zheng: Software, Formal analysis, Investigation, Writing-original draft, Writing-review editing; Ahmar Rashid, Sami Ullah, Hisham Alasmary, Muhammad Waqas: Writing-review editing, Visualization, Supervision, Project administration.

Availability of Data and Materials: The data will be available on demand.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] M. Talezari *et al.*, "Recent development, trends and challenges in IoT security," in *ICAIS 2021: Artif. Intell. Secur.*, Dublin, Ireland, Springer International Publishing, 2021, pp. 633–646.

[2] W. D. Niu, "Study on smart grid technology based on Internet of Things," *Appl. Mech. Mater.*, vol. 686, pp. 190–194, 2014. doi: 10.4028/www.scientific.net/AMM.686.190.

[3] L. Chhaya, P. Sharma, A. Kumar, and G. Bhagwatikar, "IoT-based implementation of field area network using smart grid communication infrastructure," *Smart Cities*, vol. 1, no. 1, pp. 176–189, 2018. doi: 10.3390/smartcities1010011.

[4] J. Gao and Y. Tang, "Intelligent distribution system based on IoT technology," in *ICTE 2011*, 2011, pp. 2211–2216.

[5] L. Chhaya, P. Sharma, A. Kumar, and G. Bhagwatikar, "Communication theories and protocols for smart grid hierarchical network," *J. Electr. Electron. Eng.*, vol. 10, no. 1, pp. 43, 2017.

[6] J. Wu, Y. Hu, and C. Huang, "Research on intelligent monitoring technology of substation and distribution station driven by big data," in *IOP Conf. Ser.: Earth Environ. Sci.*, IOP Publishing, vol. 714, 2021, pp. 42005.

[7] G. R. Kumar, A. S. Prasad, B. Padma, and B. R. Koti, "Smart grid communication and information technologies for cyber security, data privacy, and policy issues," in *Sustain. Netw. in Smart Grid*, Elsevier, Academic Press, 2022, pp. 1–29. https://www.sciencedirect.com/science/article/abs/pii/B9780323856263000089.
[8] M. Waqas, S. Tu, Z. Halim, S. U. Rehman, G. Abbas and Z. H. Abbas, "The role of artificial intelligence and machine learning in wireless networks security: Principle, practice and challenges," *Artif. Intell. Rev.*, vol. 55, no. 7, pp. 5215–5261, 2022. doi: 10.1007/s10462-022-10143-2.
[9] M. Ghiasi, T. Niknam, Z. Wang, M. Mehrandezh, M. Dehghani and N. Ghadimi, "A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future," *Electr. Pow. Syst. Res.*, vol. 215, pp. 108975, 2023. doi: 10.1016/j.epsr.2022.108975.
[10] L. Chhaya, P. Sharma, G. Bhagwatikar, and A. Kumar, "Wireless sensor network based smart grid communications: Cyber attacks, intrusion detection system and topology control," *Electron.*, vol. 6, no. 1, pp. 5, 2017. doi: 10.3390/electronics6010005.
[11] M. K. Hasan, A. A. Habib, Z. Shukur, F. Ibrahim, S. Islam and M. A. Razzaque, "Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations," *J. Netw. Comput. Appl.*, vol. 209, no. 23, pp. 103540, 2023. doi: 10.1016/j.jnca.2022.103540.
[12] D. Gambetta, "Can we trust trust," *Trust: Mak. Break. Coop. Relat.*, vol. 13, pp. 213–237, 2000.
[13] K. Cook, *Trust in Society*, USA: Russell Sage Foundation, 2003, vol. 2, pp. 432.
[14] A. Badshah *et al.*, "LAKE-BSG: Lightweight authenticated key exchange scheme for blockchain-enabled smart grids," *Sustain. Energ. Technol. Assess.*, vol. 52, no. 1, pp. 102248, 2022. doi: 10.1016/j.seta.2022.102248.
[15] V. Boulgourasa, T. Ioannidis, I. Politis, and C. Xenakis, "RETINA: Distributed and secure trust management for smart grid applications and energy trading," arXiv preprint arXiv:2306.08074, 2023.
[16] J. Zong, C. Wang, J. Shen, C. Su, and W. Wang, "ReLAC: Revocable and lightweight access control with blockchain for smart consumer electronics," *IEEE Trans. Consum. Electr.*, 2023. doi: 10.1109/TCE.2023.3279652.
[17] W. Wang, Z. Han, T. R. Gadekallu, S. Raza, J. Tanveer and C. Su, "Lightweight blockchain-enhanced mutual authentication protocol for UAVs," *IEEE Intern. Things J.*, 2023. doi: 10.1109/JIOT.2023.3324543.
[18] W. Wang, Y. Yang, Z. Xiong, and D. Niyato, "Footstone of metaverse: A timely and secure crowdsensing," *IEEE Netw.*, 2023. doi: 10.1109/MNET.134.2200598.
[19] A. Bhatia *et al.*, "Networked control system with MANET communication and AODV routing," *Heliyon*, vol. 8, no. 11, pp. e11678, 2022. doi: 10.1016/j.heliyon.2022.e11678.
[20] X. Wu, J. Huang, J. Ling, and L. Shu, "BLTM: Beta and LQI based trust model for wireless sensor networks," *IEEE Access*, vol. 7, pp. 43679–43690, 2019. doi: 10.1109/ACCESS.2019.2905550.
[21] S. A. Soleymani *et al.*, "A secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing," *IEEE Access*, vol. 5, pp. 15619–15629, 2017. doi: 10.1109/ACCESS.2017.2733225.
[22] R. K. Sinha and A. K. Jagannatham, "Gaussian trust and reputation for fading mimo wireless sensor networks," in *2014 IEEE Int. Conf. Electron., Comput. Commun. Technol. (CONECCT)*, IEEE, 2014, pp. 1–6.
[23] R. Feng, X. Han, Q. Liu, and N. Yu, "A credible bayesian-based trust management scheme for wireless sensor networks," *Int. J. Distrib. Sens. Netw.*, vol. 11, no. 11, pp. 678926, 2015. doi: 10.1155/2015/678926.
[24] W. Luo, W. Ma, and Q. Gao, "A dynamic trust management system for wireless sensor networks," *Secur. Commun. Netw.*, vol. 9, no. 7, pp. 613–621, 2016. doi: 10.1002/sec.1384.
[25] W. Fang, C. Zhang, Z. Shi, Q. Zhao, and L. Shan, "BTRES: Beta-based trust and reputation evaluation system for wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 59, no. 2, pp. 88–94, 2016. doi: 10.1016/j.jnca.2015.06.013.
[26] M. Singh, A. R. Sardar, K. Majumder, and S. K. Sarkar, "A lightweight trust mechanism and overhead analysis for clustered WSN," *IETE J. Res.*, vol. 63, no. 3, pp. 297–308, 2017. doi: 10.1080/03772063.2017.1284613.

[27] A. M. Shabut, K. P. Dahal, S. K. Bista, and I. U. Awan, "Recommendation based trust model with an effective defence scheme for manets," *IEEE Trans. Mobile Comput.*, vol. 14, no. 10, pp. 2101–2115, 2014. doi: 10.1109/TMC.2014.2374154.

[28] N. Khanna and M. Sachdeva, "Study of trust-based mechanism and its component model in manet: Current research state, issues, and future recommendation," *Int. J. Commun. Syst.*, vol. 32, no. 12, pp. e4012, 2019. doi: 10.1002/dac.4012.

[29] J. Xu *et al.*, "An algorithm for determining data forwarding strategy based on recommended trust value in manet," *Int. J. Embedded Syst.*, vol. 12, no. 4, pp. 544–553, 2020. doi: 10.1504/IJES.2020.107635.

[30] K. Boakye-Boateng, A. A. Ghorbani, and A. H. Lashkari, "A novel trust model in detecting final-phase attacks in substations," in *2021 18th Int. Conf. Privacy Secur. Trust (PST)*, 2021, pp. 1–11.

[31] K. Boakye-Boateng, A. A. Ghorbani, and A. H. Lashkari, "A trust-influenced smart grid: A survey and a proposal," *J. Sens. Actuator Netw.*, vol. 11, no. 3, pp. 34, 2022. doi: 10.3390/jsan11030034.

[32] K. Boakye-Boateng, A. A. Ghorbani, and A. H. Lashkari, "Securing substations with trust, risk posture, and multi-agent systems: A comprehensive approach," in *2023 20th Annu. Int. Conf. Privacy, Secur. Trust (PST)*, Copenhagen, Denmark, 2023, pp. 1–12.

[33] X. Li, F. Zhou, and J. Du, "LDTS: A lightweight and dependable trust system for clustered wireless sensor networks," *IEEE Trans. Inf. Foren. Secur.*, vol. 8, no. 6, pp. 924–935, 2013. doi: 10.1109/TIFS.2013.2240299.

[34] W. Alnumay, U. Ghosh, and P. Chatterjee, "A trust-based predictive model for mobile ad hoc network in internet of things," *Sens.*, vol. 19, no. 6, pp. 1467, 2019. doi: 10.3390/s19061467.

[35] S. Dhelim, N. Aung, M. T. Kechadi, H. Ning, L. Chen and A. Lakas, "Trust2Vec: Large-scale IoT trust management system based on signed network embeddings," *IEEE Intern. Things J.*, vol. 10, no. 1, pp. 553–562, 2022. doi: 10.1109/JIOT.2022.3201772.

[36] F. Dang, L. Yan, S. Li, and D. Li, "Trusted dynamic threshold caculation method in power IoT," in *2022 14th Int. Conf. Commun. Softw. Netw. (ICCSN)*, IEEE, 2022, pp. 19–22.