

RESEARCH ARTICLE

Intelligent fault detection strategy for knowledge entities in fault semantic networks of distribution network based on siamese networks

Xinjie Sun ^{*}, Tao Qin, Lingyun Tong, Haoliang Zhang, Weihai Xu

State Grid Nanjing Power Supply Company, Nanjing, China

* XinjieSun_StateGrid@outlook.com



Abstract

The advent of smart grid technologies has brought about a paradigm shift in the management and operation of distribution networks, allowing for intricate system information to be encapsulated within semantic network models. These models, while robust, are not immune to faults within their knowledge entities, which can arise from a myriad of issues, potentially leading to verification failures and operational disruptions. Addressing this critical vulnerability, our research delves into the development of a novel fault detection methodology specifically tailored for the knowledge entity variables of semantic networks in distribution networks. In our approach, we first construct a state space equation that models the behavior of knowledge entity variables in the presence of faults. This foundational framework enables us to apply an unknown input observer strategy to effectively detect anomalies within the system. To bolster the fault identification process, we introduce the innovative use of a siamese network, a neural network architecture which is proficient in differentiating between similar datasets. Through simulation scenarios, we demonstrate the efficacy of our proposed fault detection method.

OPEN ACCESS

Citation: Sun X, Qin T, Tong L, Zhang H, Xu W (2024) Intelligent fault detection strategy for knowledge entities in fault semantic networks of distribution network based on siamese networks. PLoS ONE 19(5): e0303084. <https://doi.org/10.1371/journal.pone.0303084>

Editor: Ibrahim Sadek, Helwan University Faculty of Engineering, EGYPT

Received: January 24, 2024

Accepted: April 18, 2024

Published: May 16, 2024

Copyright: © 2024 Sun et al. This is an open access article distributed under the terms of the [Creative Commons Attribution License](https://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Data Availability Statement: All data files are available from the <https://www.elia.be/en/grid-data/power-generation/wind-power-generation>.

Funding: This work is supported by the 2022 State Grid Jiangsu Electric Power Co., Ltd. Science and Technology Project (J2022103 to X.S.).

Competing interests: NO authors have competing interests.

Introduction

The inception of smart grid technology has precipitated a paradigm shift in the domain of power distribution networks, heralding unprecedented levels of operational efficiency, enhanced reliability, and a harmonious integration of renewable energy sources [1–3]. As conduits between electricity suppliers and end-users, distribution networks have evolved into intricate and dynamic systems [4]. This evolution has necessitated the deployment of sophisticated information and communication technologies to adeptly manage the burgeoning data landscape, ensuring fluid grid operations [5, 6].

Within this advanced operational context, semantic network models have risen to prominence, providing an essential framework for the representation of system information. These models are instrumental in elucidating and orchestrating the complex interplay among the diverse components of the smart grid ecosystem [7, 8].

Central to these semantic networks are the knowledge entities, which serve as proxies for the system's components and their elaborate interconnections [9]. These entities are the linchpin in the accurate representation of distribution network behavior, embodying critical data pertaining to the operational states of tangible infrastructure elements, including transformers, power lines, and load-bearing units. The fidelity of these knowledge entities is non-negotiable, as any divergence from their true state can trigger a cascade of operational inefficiencies, misguided decision-making, or in the worst cases, outright system failures [10]. Thus, the reliability of distribution networks is inextricably linked to the precision and steadfastness of the data held within these knowledge entities [11].

Despite their foundational role, knowledge entities are not impervious to faults, which can emanate from a variety of sources such as sensor dysfunctions, communication breakdowns, or anomalies in data processing [12–14]. These faults pose a significant threat, potentially undermining the verification processes and jeopardizing the operational integrity of the distribution network [15–17].

Confronting these challenges is of paramount importance, necessitating focused research efforts towards the development of intelligent fault detection methodologies that are specifically designed for the nuanced requirements of knowledge entities in semantic networks [18, 19]. In this paper, we introduce a cutting-edge fault detection approach for knowledge entity variables within distribution networks. This approach is underpinned by a state space equation that anticipates potential faults, coupled with the implementation of an unknown input observer adept at discerning system states amidst the presence of unmeasured disturbances.

To augment the fault detection capabilities, we incorporate Siamese networks into our methodology. These neural networks are renowned for their proficiency in similarity detection and pattern recognition, which significantly bolsters our ability to identify and rectify dual source data discrepancies within knowledge entities. Through this research, we aim to not only underscore the criticality of maintaining knowledge entity integrity but also deliver a robust and reliable framework to protect the smart grid infrastructure from the adverse effects of data faults.

The contributions of this paper are multifaceted and represent a significant advancement in the field of smart grid management.

1. We develop a state space equation tailored to the state variables of knowledge entities, explicitly taking into account the potential fault scenarios that may afflict distribution networks. This formulation provides a comprehensive description of the system's operational state, reflecting a deep understanding of the dynamics at play within the smart grid.
2. We employ an unknown input observer, a sophisticated tool designed to discern fault information within the distribution network. This approach leverages the observer's inherent capability to detect anomalies, thereby enhancing the reliability of the fault diagnosis process.
3. We apply Siamese networks, leveraging their exceptional pattern recognition abilities, to identify and isolate fault information in the distribution network. This application showcases the potential of advanced neural networks in improving fault detection mechanisms within complex systems.

Modeling of state space for knowledge entities considering the fault scenarios

The operational status methodology for the distribution network that this article presents meticulously incorporates considerations of power shortage and scheduling costs [20, 21].

Within this framework, power-related state space variables serve to estimate the magnitude of power shortages afflicting the distribution network, while cost-related state space variables are instrumental in calculating the incremental costs associated with the optimal scheduling solutions for the distribution network’s challenges.

It is critical to acknowledge that the integrity of knowledge entity information within the semantic network is foundational to the precision of our estimations. Any deviation in this data directly impacts the accuracy of power shortage assessments and the computation of incremental costs, which, in turn, bears upon the stability and economic viability of the distribution network’s operations.

The operational state space equation that accounts for power shortages and scheduling costs within a distribution network is formulated as follows:

$$\begin{cases} x(k + 1) = Ax(k) + Bu(k), & \text{normal} \\ x(k + 1) = Ax(k) + Bu(k) + Mm(k), & \text{compromised} \end{cases} \tag{1}$$

where

$$\begin{aligned} x &= [x_p^p \ x_p^c \ x_h^c \ x_h^h]^T \\ u &= [u_p^p \ u_p^c \ u_h^c \ u_h^h]^T \end{aligned}$$

where x_p^p and x_p^c respectively represent the fault handling capabilities of traditional and distributed resources in the distribution network; x_h^c and x_h^h represent the fault handling costs of traditional and distributed resources in the distribution network, respectively; u_p^p and u_p^c respectively represent the deviation between the fault handling capabilities of traditional and distributed resources in the distribution network and the expected ones; u_h^c and u_h^h respectively represent the deviation between the fault handling cost of traditional and distributed resources in the distribution network and the expected cost; A and B are knowledge graph matrices for fault handling in distribution networks; $m(k)$ and M are the matrixes to represent the fault.

It can be understood that changes in the state variables of knowledge entities in different stages of the distribution network fault model will affect the effectiveness of distribution network fault handling. In the next section, observers with different fault knowledge entity variables were designed to observe faults in the distribution network.

Design of observers for detecting compromised variables in knowledge graph of distribution network

Observer design of fault handling capabilities considering faults

In this subsection, we focus on the observer for fault handling capabilities. The original system Σ_{fhc} is

$$\begin{cases} x(k + 1) = Ax(k) + Bu(k) + Mm(k) \\ y(k) = Cx(k) \end{cases} \tag{2}$$

By incorporating the fault vector $m(k - 1)$ from time $k - 1$ as an additional state, we enhance our analytical capabilities. This incorporation leads to the formulation of an augmented state vector $\bar{x}(k) = [x(k) \ m(k - 1)]^T$. With this enriched state representation, we are able to construct an augmented system that provides a more comprehensive understanding of the network’s dynamics in the presence of faults. This augmented system is presented as

follows:

$$\begin{cases} \bar{E}\bar{x}(k+1) = \bar{A}\bar{x}(k) + \bar{B}u(k) \\ y(k) = \bar{C}\bar{x}(k) \end{cases} \tag{3}$$

where

$$\bar{E} = \begin{bmatrix} I_n & -M \\ 0 & 0 \end{bmatrix}, \bar{A} = \begin{bmatrix} A & 0 \\ 0 & 0 \end{bmatrix}, \bar{B} = \begin{bmatrix} B \\ 0 \end{bmatrix}, \bar{C} = \begin{bmatrix} C \\ 0 \end{bmatrix}^T$$

The observer for the augmented system is delineated as follows:

$$\begin{cases} z(k+1) = R\bar{A}\hat{x}(k) + R\bar{B}u(k) + L(y(k) - \bar{C}\hat{x}(k)) \\ \hat{x}(k) = z(k) + Ty(k) \end{cases} \tag{4}$$

Within this framework, let z represent the dynamics of system (3); $\hat{x}(k)$ signifies the estimate of the augmented state vector $\bar{x}(k)$. To optimize the observer’s performance, we introduce gain matrices R, L and T each carefully dimensioned to align with the system’s parameters. These matrices are not arbitrary; they are the result of a rigorous design process aimed at achieving optimal state estimation fidelity.

Theorem 1. The state observer, as delineated in form (4), must adhere to a set of precisely defined criteria to ensure its effectiveness and reliability. These requirements are twofold: 1) The first condition necessitates an algebraic relationship where the matrix R , when multiplied by the augmented system matrix \bar{E} , and the matrix T , when multiplied by the augmented output matrix \bar{C} , must collectively yield the identity matrix I_{n+q} . This identity matrix has dimensions that correspond to the sum of the system’s state dimensions and the fault vector’s dimensions, ensuring that the observer gain matrices are correctly calibrated for accurate state reconstruction. 2) The second condition requires the existence of symmetric positive definite matrices P and W . These matrices are not merely mathematical constructs; they are pivotal in defining a Lyapunov function that guarantees the convergence and stability of the observer. The satisfaction of these conditions is essential for the observer to perform its function with the requisite level of precision and robustness. The precise mathematical formulations that codify these requirements are as follows:

$$\begin{bmatrix} -P & (R\bar{A})^T P - \bar{C}^T W^T \\ * & -P \end{bmatrix} < 0 \tag{5}$$

proof. We have the following matrices $U \in \mathbb{R}^{(n+q) \times (n+q)}$ and $V \in \mathbb{R}^{(n+q) \times (n+q)}$ satisfied

$$U\bar{E}V = \begin{bmatrix} I_N & 0 \\ 0 & 0 \end{bmatrix} \tag{6}$$

So that

$$\begin{aligned} \text{rank} \begin{bmatrix} I_n & 0 \\ 0 & 0 \\ C & 0 \end{bmatrix} &= \text{rank} \left\{ \begin{bmatrix} U & 0 \\ 0 & I_m \end{bmatrix} \begin{bmatrix} \bar{E} \\ \bar{C} \end{bmatrix} V \right\} \\ &= \text{rank} \begin{bmatrix} \bar{E} \\ \bar{C} \end{bmatrix} = n + q \end{aligned} \tag{7}$$

Therefore

$$\text{rank} \begin{bmatrix} I_N & 0 \\ C & 0 \end{bmatrix} = \text{rank} \begin{bmatrix} \bar{E} \\ \bar{C} \end{bmatrix} = n + q \tag{8}$$

$$\text{rank}(U\bar{E}V + \bar{C}V) = \text{rank} \begin{bmatrix} I_N & 0 \\ C & 0 \end{bmatrix} = n + q \tag{9}$$

R satisfied

$$R = V(U\bar{E}V + \bar{C}V)^{-1}U \tag{10}$$

T satisfied

$$T = V(U\bar{E}V + \bar{C}V)^{-1} \tag{11}$$

So, $R\bar{E} + T\bar{C} = I_{n+q}$, $[R, T]$ and $[\bar{E}\bar{C}]^T$ satisfied

$$\begin{bmatrix} \bar{E} \\ \bar{C} \end{bmatrix} [R \quad T] \begin{bmatrix} \bar{E} \\ \bar{C} \end{bmatrix} = \begin{bmatrix} \bar{E} \\ \bar{C} \end{bmatrix} \tag{12}$$

Therefore, we can derive

$$[R \quad T] = \begin{bmatrix} \bar{E} \\ \bar{C} \end{bmatrix}^\dagger + \Theta \left(I_{n+q+m} - \begin{bmatrix} \bar{E} \\ \bar{C} \end{bmatrix} \begin{bmatrix} \bar{E} \\ \bar{C} \end{bmatrix}^\dagger \right) \tag{13}$$

The matrix Θ , which resides in the real-valued space $\mathbb{R}^{(n+q) \times (n+q+m)}$ is not arbitrarily chosen. rather, it is selected with a deliberate intention that is grounded in the fundamental principles of system design.

As to the $e(k)$, we have

$$e(k) = \bar{x}(k) - \bar{\hat{x}}(k) \tag{14}$$

Therefore

$$\begin{aligned} e(k+1) &= (R\bar{E} + T\bar{C})x(k+1) - z(k+1) - Ty(k+1) \\ &= R\bar{E}x(k+1) - z(k+1) \\ &= (R\bar{A} - L\bar{C})e(k) \end{aligned} \tag{15}$$

Since

$$V(k) = e^T(k)Pe(k), \quad P > 0 \tag{16}$$

We have

$$\begin{aligned} \Delta V(k) &= V(k+1) - V(k) \\ &= e^T(k)[(R\bar{A} - L\bar{C})^T P(R\bar{A} - L\bar{C}) - P]e(k) \end{aligned} \tag{17}$$

If the following equation holds

$$\begin{bmatrix} -P & (R\bar{A} - L\bar{C})^T P \\ P(R\bar{A} - L\bar{C}) & -P \end{bmatrix} < 0 \tag{18}$$

By invoking the Schur complement theorem in conjunction with the principles of Lyapunov stability theory, we rigorously establish that $\Delta V(k) < 0$. This result is not merely a theoretical assertion but a demonstrable guarantee of the system’s performance. It signifies that the Lyapunov function $V(k)$ is strictly decreasing, thereby providing a robust mathematical argument for the convergence of the error term $e(k)$.

The completion of the proof provides a substantive insight into the resilience of the proposed observer within our control system. Specifically, it has been demonstrated that, even in the event of a compromise to the incremental cost estimator, the defender retains the capability to accurately monitor system variables. This resilience is not an incidental feature but a deliberate design element, ensuring that the integrity of the system’s observational mechanisms is preserved under adverse conditions. The robustness of the proposed observer is thus affirmed, underscoring its potential as a reliable tool for maintaining situational awareness and operational continuity within the system.

Observer design of fault handling costs calculation under faults

In this subsection, we focus on the observer for compromised fault handling costs calculation. The system Σ_{fhc} can be expressed as

$$\begin{cases} x(k+1) = Ax(k) + Bu(k) \\ y(k) = Cx(k) + Nm(k) \end{cases} \tag{19}$$

Incorporating the fault vector $m(k)$ as an integral component of the system’s state representation, we construct an augmented state vector $\bar{x}(k) = [x(k) \ m(k)]^T$. This expansion of the state space enables us to formulate a comprehensive augmented system that encapsulates both the original dynamics and the fault conditions. This approach not only enhances the descriptive power of our model but also facilitates the development of more sophisticated control strategies that can account for and adapt to fault-induced variations within the system.

$$\begin{cases} \bar{E}\bar{x}(k+1) = \bar{A}\bar{x}(k) + \bar{B}u(k) \\ y(k) = \bar{C}\bar{x}(k) \end{cases} \tag{20}$$

where

$$\bar{E} = \begin{bmatrix} I_n & 0 \\ 0 & 0 \end{bmatrix}, \bar{A} = \begin{bmatrix} A & 0 \\ 0 & 0 \end{bmatrix}, \bar{B} = \begin{bmatrix} B \\ 0 \end{bmatrix}, \bar{C} = \begin{bmatrix} C \\ N \end{bmatrix}^T$$

In parallel with the development of the augmented system, we have successfully extended our observer design to accommodate this enhanced framework, as delineated by formula (4). The theoretical underpinnings that guarantee the feasibility of our observer are meticulously laid out in Theorem 1. While the constraints of this manuscript preclude a detailed repetition of the proof for the observer’s existence within this subsection, it is imperative to acknowledge the robust applicability of our observer design methodology.

Observer design in situations of multiple modules being compromised considering uncertainties

In this subsection, we delve into a more complex scenario where multipoint faults are concurrently taken into account. To accurately capture the dynamics of the system under such conditions, we define the compromised system with a formulation that reflects the intricate interplay between these faults. The representation is given as follows:

$$\begin{cases} x(k+1) = Ax(k) + Bu(k) + Mm(k) + E_a\omega_a(k) \\ y(k) = Cx(k) + Nm(k) + E_s\omega_s(k) \end{cases} \tag{21}$$

Within this analysis, the terms $\omega_a(k)$ and $\omega_s(k)$ represent unknown input vectors that encapsulate the inherent uncertainties present within the system. The matrices E_a and E_s are known constant coefficient matrices, each carefully dimensioned to align with the system’s structure. To adeptly incorporate the fault vector into our analytical framework, we introduce it as an additional state. This strategic maneuver allows us to construct the augmented state vector $\bar{x}(k) = [x(k) \ m(k)]^T$, which embodies both the system’s state and the fault vector in a unified representation. With this enhanced state vector, we can articulate the following augmented system

$$\begin{cases} \bar{x}(k+1) = \bar{A}\bar{x}(k) + \bar{B}u(k) + \bar{E}_a\omega_a(k) + Gm^d(k) \\ y(k) = \bar{C}\bar{x}(k) + E_s\omega_s(k) \\ m^d(k) = m(k+1) - m(k) \end{cases} \tag{22}$$

where

$$\bar{A} = \begin{bmatrix} A & M \\ 0 & I_q \end{bmatrix}, \bar{B} = \begin{bmatrix} B \\ 0 \end{bmatrix}, \bar{C} = \begin{bmatrix} C \\ N \end{bmatrix}^T, \bar{E}_a = \begin{bmatrix} E_a \\ 0 \end{bmatrix}^T, G = \begin{bmatrix} 0 \\ I_q \end{bmatrix}^T$$

Therefore, we can have

$$\begin{cases} z(k+1) = Rz(k) + Su(k) + (L_1 + L_2)y(k) \\ \hat{x}(k) = z(k) + Ty(k) \end{cases} \tag{23}$$

Therefore

$$\begin{aligned}
 e(k+1) &= (I - T\bar{C})\bar{x}(k+1) - z(k+1) - TE_s\omega_s(k) \\
 &= [(I - T\bar{C})\bar{A} - L_1\bar{C}]e(k) + [(I - T\bar{C})\bar{A} \\
 &\quad - L_1\bar{C} - R]z(k) + [(I - T\bar{C})\bar{B} - S]u_k + \\
 &\quad [((I - T\bar{C})\bar{A} - L_1\bar{C})T - L_2]y(k) \\
 &\quad + (I - T\bar{C})\bar{E}_a\omega_a(k) + (I - T\bar{C})Gm^d(k) \\
 &\quad - L_1E_s\omega_s(k) - TE_s\omega_s(k+1)
 \end{aligned} \tag{24}$$

If

$$(I - T\bar{C})\bar{E}_a = 0 \tag{25}$$

$$(I - T\bar{C})\bar{A} - L_1\bar{C} = R \tag{26}$$

$$(I - T\bar{C})\bar{B} = S \tag{27}$$

$$RT = L_2 \tag{28}$$

We can have

$$e(k+1) = Re(k) + (I - T\bar{C})Gm^d(k) - L_1E_s\omega_s(k) - TE_s\omega_s(k+1) \tag{29}$$

Theorem 2. Upon examination of the augmented system delineated in Eq 22, we postulate the existence of a robust observer, characterized by Eq 23. This observer is meticulously designed to ensure that the norm of the error vector $e(k)$, when measured in the l_2 space, is bounded by the inequality $\|e(k)\|_{l_2} \leq \sqrt{2}r\|\gamma(k)\|_{l_2}$.

The establishment of such a robust observer is contingent upon the fulfillment of a specific matrix inequality condition. This condition is met if one can ascertain the existence of a positive definite matrix P and a suitably dimensioned matrix Q , such that:

$$\begin{bmatrix}
 -P + I_n & * & * & * \\
 0_{l_y \times \bar{n}} & -r^2 I_{l_y} & * & * \\
 0_{l_y \times \bar{n}} & 0_{l_y \times l_y} & -r^2 I_{l_y} & * \\
 PA_1 - Q\bar{C} & PV_1 - QV_2 & P\bar{V}_2 & -P
 \end{bmatrix} < 0 \tag{30}$$

where $A_1 = (I - T\bar{C})\bar{A}$, $Q = PL_1$, $V_1 = [(I - T\bar{C})G \ 0_{\bar{n} \times l_n}]$, $V_2 = [0_{p \times q} \ E_s]$, and $\bar{V}_2 = -TV_2$.

Proof. Considering that

$$V(k) = e^T(k)Pe(k) \tag{31}$$

We have

$$\begin{aligned} \Delta V(k) &= V(k+1) - V(k) \\ &= \begin{bmatrix} e(k) \\ \gamma(k) \\ \gamma(k+1) \end{bmatrix}^T \left(\begin{bmatrix} R \\ V_1 - L_1 V_2 \\ \bar{V}_2 \end{bmatrix} P \begin{bmatrix} R \\ V_1 - L_1 V_2 \\ \bar{V}_2 \end{bmatrix} \right)^T \\ &\quad + \begin{bmatrix} -P & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} e(k) \\ \gamma(k) \\ \gamma(k+1) \end{bmatrix} \end{aligned} \tag{32}$$

The system is asymptotically stable since $\gamma(k) = 0$.
And

$$\begin{aligned} \Gamma &= \sum_{k=0}^{\infty} (\Delta V(k) + e^T(k)e(k) - r^2\gamma^T(k)\gamma(k) \\ &\quad - r^2\gamma^T(k+1)\gamma(k+1)) \end{aligned} \tag{33}$$

Therefore

$$\begin{aligned} \Gamma &= \sum_{k=0}^{\infty} \begin{bmatrix} e(k) \\ \gamma(k) \\ \gamma(k+1) \end{bmatrix}^T \left[\begin{bmatrix} R \\ V_1 - L_1 V_2 \\ \bar{V}_2 \end{bmatrix} P \right] P^{-1} \\ &\quad \left(\begin{bmatrix} R \\ P \\ V_1 - L_1 V_2 \\ \bar{V}_2 \end{bmatrix} \right) + \begin{bmatrix} -P + I & 0 \\ 0 & -r^2 I \end{bmatrix} \begin{bmatrix} e(k) \\ \gamma(k) \\ \gamma(k+1) \end{bmatrix} \end{aligned} \tag{34}$$

Therefore

$$\begin{aligned} &\sum_{k=0}^{\infty} (e^T(k)e(k) - r^2\gamma^T(k)\gamma(k) \\ &\quad - r^2\gamma^T(k+1)\gamma(k+1)) + V(\infty) - V(0) < 0 \end{aligned} \tag{35}$$

We have

$$\sum_{k=0}^{\infty} e^T(k)e(k) - 2r^2\gamma^T(k)\gamma(k) < 0 \tag{36}$$

Proofed.

Drawing upon the proposed observer framework, we are equipped to deduce the observed data corresponding to the system’s variables, juxtaposed with the directly measured data. For

the dispatcher, it is imperative to discern the congruence between the observed and measured data sets during periods of normal operation. This alignment serves as a benchmark for system integrity.

Conversely, it is equally vital for the dispatcher to detect and characterize any discrepancies between the two data sets that may emerge under compromised conditions. Such anomalies are indicative of potential system faults or malicious interventions, and their timely identification is crucial for implementing corrective measures.

To facilitate this dual analysis, robust statistical or algorithmic methods must be employed to systematically compare the observed and measured data.

Identification scheme against fault based on dual source data

In this section, we delve into an in-depth analysis of a fault identification scheme tailored to effectively counteract faults by leveraging dual-source data. We propose a sophisticated relation-based detection network that is meticulously engineered to distill the inherent similarity within the dual-source data. This network is pivotal in unraveling the intricate patterns that may otherwise be obscured in the multidimensional data space.

- The conventional methodology for quantifying the similarity of dual-source data vectors via Euclidean distance presents a notable challenge; it presupposes a substantial degree of prior knowledge on the part of system defenders, which may not always be feasible in dynamic and complex operational environments. Recognizing this limitation, our research introduces an innovative approach that circumvents the need for extensive a priori understanding. In this paper, we present a novel framework comprising an embedding module coupled with a relation module, both of which are designed to autonomously extract the similarity from dual-source data. The embedding module is responsible for transforming the raw data into a lower-dimensional, information-rich representation. This process is achieved through advanced feature learning techniques that capture the underlying structure and relationships within the data without relying on manual feature engineering.
- Traditional machine learning methodologies typically necessitate the computation of distances within the feature space to facilitate identification tasks. This approach, inherently reliant on the geometry of the feature space, often requires a substantial volume of training data to achieve satisfactory performance. The demand for large-scale datasets poses significant challenges, including increased computational resources, potential overfitting, and the practical difficulties associated with data acquisition and labeling. In contrast, the research presented in this paper adopts a more nuanced and efficient strategy. We eschew the conventional paradigm of learning feature distances and instead propose a direct learning framework for discerning the relationships inherent in dual-source data. Our approach is predicated on the insight that understanding the interconnections between data sources can be more informative and less resource-intensive than traditional distance-based learning.

As shown in [Fig 1](#), we propose a twin network for detecting faults in distribution networks. In the architecture of our identification network, we integrate a measured data set and an observed data set, alongside an embedding module and a relation module. The observed data set serves as a reliable reflection of the system's current operational state, unadulterated by potential external manipulations. Conversely, the measured data set is a composite that includes both potentially compromised and normal data subsets, which necessitates careful scrutiny to ensure the integrity of the fault detection process.

Our fault detection network employs a comparative analysis between the observed data and the measured data to ascertain the presence of anomalies. This comparison is crucial as it

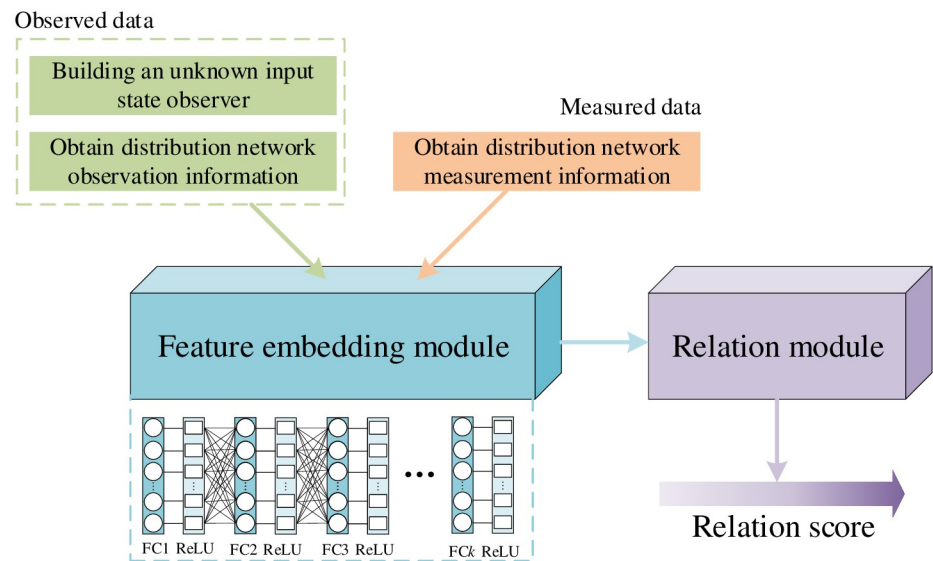


Fig 1. Schematic diagram of distribution network fault detection process.

<https://doi.org/10.1371/journal.pone.0303084.g001>

allows us to distinguish between authentic operational data and data that may have been altered or tampered with.

To elaborate, when the comparative analysis involves data from the compromised subset, we typically observe a strong similarity in the relationship between the dual-source data. This strong similarity is indicative of a discrepancy that could suggest a fault or a cyber intrusion. On the other hand, when the comparison is drawn from the normal data subset, the relationship between the dual-source data exhibits weak similarity, which aligns with the expected behavior of a system free from faults or external interference.

The distinction between strong and weak similarity in the dual-source data relationship is pivotal for the accurate identification of faults. It is through this nuanced understanding of data relationships that our network can effectively discern and flag inconsistencies, thereby enhancing the reliability and security of the system it monitors.

In our dataset formulation, we represent each data vector as a time series encapsulating the dynamic behavior of the target variables. This time-dependent structure is critical for capturing the temporal correlations intrinsic to the system under study.

The core of our feature extraction process is an embedding module, ingeniously architected with fully connected layers and rectified linear units (ReLU). This module employs a sophisticated nonlinear function, denoted by \mathcal{E} , to distill the salient features from the raw sample data. This automated feature extraction paradigm, facilitated by the fully connected layers, offers a marked improvement over traditional manual techniques by substantially reducing the dependency on prior knowledge of fault characteristics. The FC layer operates on the principle of weighted connections, where each neuron in this layer is connected to all neurons in the previous layer. These connections are weighted, embodying the learned significance of each feature in the context of fault detection. The neurons in the FC layer combine these inputs linearly (using their respective weights), followed by the application of a non-linear activation function. By synthesizing this information, the FC layer can discern patterns indicative of normal operation or fault conditions within the distribution network. It effectively acts as a decision-making entity, where the learned weights reflect the importance of each feature in predicting

the network’s status. The incorporation of ReLUs is a strategic choice aimed at enhancing the generalization capabilities of the embedding module, thereby enabling it to perform robustly across diverse operational scenarios. Upon processing by the embedding module, the feature vectors corresponding to the measured data and observed data are denoted by $\mathcal{F}(d_m)$ and $\mathcal{F}(d_o)$. These vectors encapsulate the distilled essence of the data, ready for subsequent analysis. In configuring the FC layer, one must consider the number of neurons, which directly correlates to the layer’s capacity to model complex relationships. A higher number of neurons allows for a more detailed representation but can also lead to overfitting and increased computational demands. Thus, the design of the FC layer requires a balance, ensuring it is sufficiently comprehensive to capture essential decision-making patterns while remaining computationally efficient and generalizable to unseen data. In the practical application of fault detection in distribution networks, it is necessary to fine tune the parameters of the FC layer based on the current operating scenario of the power grid, so as to maximize the detection of distribution network faults.

To address the perennial challenge of overfitting within the embedding module, we adopt a class prototype approach for each category of feature vectors. This innovative strategy involves the computation of representative prototypes for the feature vectors from both measured and observed datasets. The measured data feature vector prototype is represented as \mathcal{P}_i^m , while the observed data feature vector prototype is denoted by \mathcal{P}_i^o . These prototypes serve as archetypal points in the feature space, around which the corresponding class’s feature vectors are expected to cluster. This method not only mitigates the risk of overfitting but also provides a more intuitive understanding of the feature space structure, which is instrumental for the subsequent stages of fault detection analysis.

$$\mathcal{P}_i^m = \frac{1}{N_i^m} \sum_{j=1}^{N_i^m} \mathcal{F}(d_m) \tag{37}$$

$$\mathcal{P}_i^o = \frac{1}{N_i^o} \sum_{j=1}^{N_i^o} \mathcal{F}(d_o) \tag{38}$$

Within our analytical framework, let N_i^m and N_i^o denote the number of samples for class i within the measured and observed data feature vectors, respectively. To construct the class feature vector, denoted as $\mathcal{C}(\mathcal{P}_i^m, \mathcal{P}_i^o)$, we employ a methodical approach by concatenating the class prototypes. The relation module, an integral component of our system, leverages a nonlinear relation function \mathcal{R} to discern the degree of similarity between these concatenated class feature vectors. The similarity metric, \mathcal{S} is thus formulated as:

$$\mathcal{S} = \mathcal{R}(\mathcal{C}(\mathcal{P}_i^m, \mathcal{P}_i^o)) \tag{39}$$

Mean square error (MSE) is used to train the proposed identification loss L_m .

$$L_m = \begin{cases} \sum \sum (\mathcal{S} - 1)^2, l_m = l_o \\ \sum \sum (\mathcal{S} - 0)^2, l_m \neq l_o \end{cases} \tag{45}$$

In our analysis, we denote l_m and l_o as the labels corresponding to the measured and observed data, respectively. These labels are paramount as they represent the ground truth against which the integrity of the data is assessed.

The crux of our fault detection algorithm hinges on the comparison of these labels. In the event of a discrepancy between the measured data and the observed baseline, indicated by $l_m \neq l_o$ and \mathcal{S} is closed to 0.

Case study

In this section, we present a series of simulations designed to rigorously evaluate the efficacy of our proposed observer and the associated fault detection network for monitoring system variables.

Performance of the observer for the compromised system

In the test system, let

$$A = \begin{bmatrix} 0.9988 & 0.0007 & 0.0006 & -0.0037 \\ 0.0014 & 0.98 & -0.0012 & -0.0206 \\ 0.001 & 0.0037 & 1.0467 & 9.5584 \\ 0 & 0 & 0.0101 & 1.0234 \end{bmatrix}$$

$$B = \begin{bmatrix} 0.0052 & 0.0012 \\ 0.0315 & -0.0755 \\ -0.0582 & 0.0454 \\ -0.0003 & 0.0002 \end{bmatrix}, C = \begin{bmatrix} 0.45 & 0.32 & 0.12 & 0.11 \\ 0.38 & 0.42 & 0.13 & 0.07 \\ 0.27 & 0.31 & 0.33 & 0.09 \\ 0.07 & 0.13 & 0.43 & 0.37 \end{bmatrix}$$

where

$$m_1(k) = \begin{cases} 0, & k < 60 \\ 0.05(k - 60), & 60 \leq k < 100 \\ 2, & k \geq 100 \end{cases} \quad (41)$$

$$m_2(k) = \begin{cases} 0, & k < 60 \\ 1, & k \geq 60 \end{cases} \quad (42)$$

In this section, we commence by delineating the efficacy of our observer's fault handling capabilities. We focus on the fault target variable x_p^p , which serves as a key indicator within our system's diagnostic framework.

Employing the methodology delineated in the paper, we acquire the observed data for the variable x_p^p . The fidelity of the observer is then assessed through a series of simulations, the outcomes of which are visually encapsulated in Fig 2. These simulations provide a dual-source data comparison, juxtaposing observed and actual measurements.

Furthermore, the discrepancies between the observed and measured data are quantitatively depicted in Fig 3 showcasing the observation error. Our analysis reveals that when the fault magnitude is static, the observer exhibits a commendable capacity to track the measured data with high precision. Conversely, in scenarios where the fault magnitude is dynamic, a

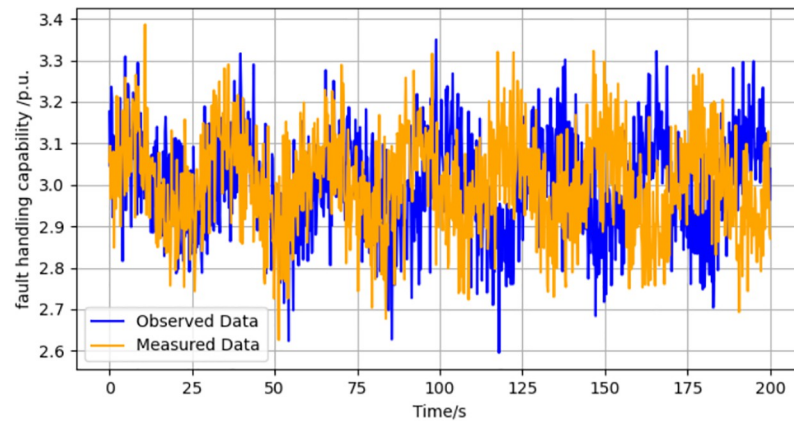


Fig 2. Dual source data of variable x_p^p under faults on fault handling capabilities.

<https://doi.org/10.1371/journal.pone.0303084.g002>

discernible observation error emerges. This error is attributable to the dynamic nature of the fault, which introduces a variable disturbance akin to a moving target for the observer.

The magnitude and behavior of the observation error are not merely artifacts; rather, they are instrumental in the operationalization of our fault detection network. The disparity between the observed and measured data forms a critical metric, serving as a cornerstone for the network's algorithms to ascertain the integrity of the system. It is this nuanced interplay between observed discrepancies and fault detection that underpins the robustness of our proposed diagnostic approach.

Subsequently, we rigorously evaluate the observer's performance in the context of faults affecting the output power decision-making process. The focal point of this assessment is the fault target variable y_C^p , which is indispensable for ensuring the reliability and accuracy of power output decisions.

Leveraging the methodology articulated in the paper, we derive the observed data for the state variable x_C^p . This process is underpinned by a robust analytical framework designed to capture the nuances of the observer's operation under fault conditions.

The results of our simulations, which are pivotal to our investigation, are depicted in Fig 4. These figures are not merely illustrative but are also analytical tools that provide insight into the observer's performance metrics and fault tolerance capabilities.

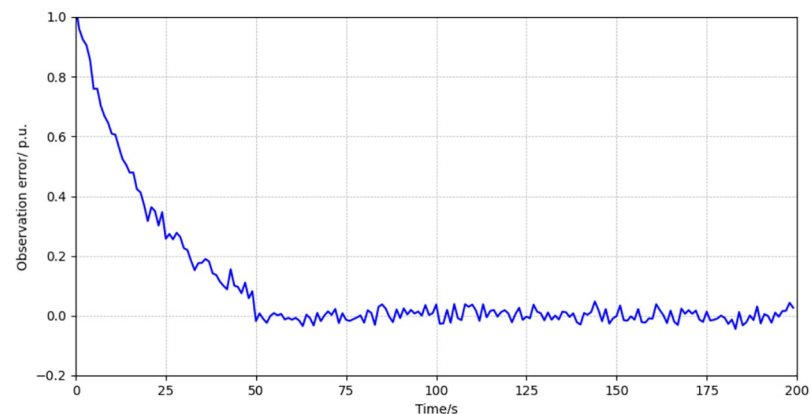


Fig 3. Observation error of variable x_p^p under faults on fault handling capabilities.

<https://doi.org/10.1371/journal.pone.0303084.g003>

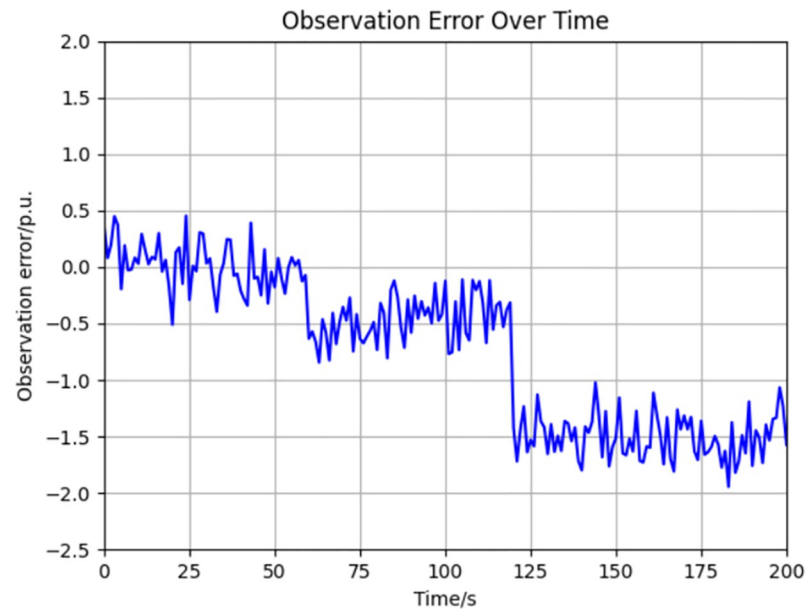


Fig 4. Observation error of variable x_p^c under faults on fault handling cost.

<https://doi.org/10.1371/journal.pone.0303084.g004>

It is imperative to note that the simulation results extend beyond a mere presentation of data; they encapsulate the observer's ability to maintain the integrity of the decision-making process in the face of perturbations. The implications of these findings are profound, informing the development of more resilient and secure power system infrastructures.

To elucidate the robustness of the proposed observer when confronted with the simultaneous compromise of multiple modules, we conduct a detailed analysis of simulation results under these multifaceted fault conditions. This analysis is crucial for understanding the observer's performance in a realistic scenario where multiple variables may be subjected to adversarial interventions.

Employing the proposed methodology, we obtain the observed data for the compromised variables. The fidelity of our observer is then rigorously assessed through simulations, the results of which are presented in Fig 5. These figures are not merely visual aids but serve as critical evidence of the observer's diagnostic capabilities.

A careful examination of the simulation outcomes reveals pronounced discrepancies between the measured data and the observed data. This discrepancy is indicative of the complex interplay between the fault magnitude and other system perturbations, such as noise, disturbances, and delays. Such findings underscore the imperative for a sophisticated fault detection scheme capable of discerning whether the system's integrity has been undermined.

Accordingly, the necessity for an effective fault detection mechanism becomes apparent, one that can reliably ascertain the presence of a compromise within the system. This mechanism is integral to the maintenance of system reliability and security, particularly in the presence of faults that could otherwise go undetected.

Performance of the observer for the relation-based fault detection scheme

In this subsection, we undertake a comprehensive evaluation of the performance of the proposed fault detection scheme, which is a cornerstone of our research. The architecture of the embedding module within this scheme incorporates three fully connected layers, each

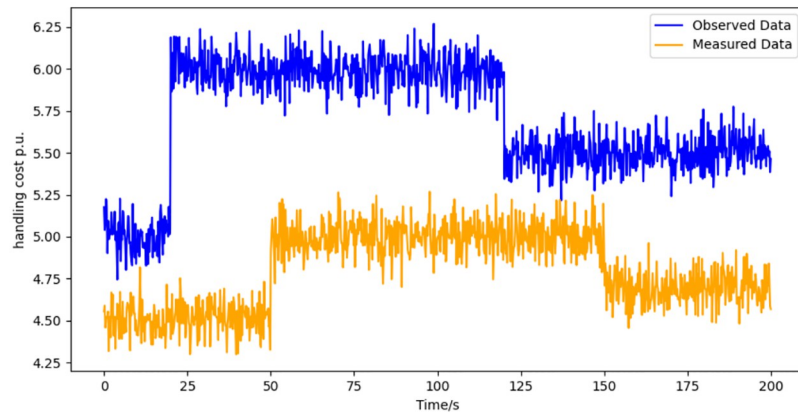


Fig 5. Dual source data of variable x_h^c under faults on multiple modules.

<https://doi.org/10.1371/journal.pone.0303084.g005>

followed by rectified linear units (ReLU) to introduce non-linearity and enhance feature learning capabilities.

For the training of the relation network, we judiciously select a batch size of 20. This choice balances computational efficiency with the network’s ability to generalize from the training data. In compiling the measured data set, we draw upon a historical database to amass 500 samples representative of normal system behavior and an additional 500 samples indicative of compromised system states. This balanced approach ensures that the fault detection scheme is exposed to an array of conditions reflective of the system’s operational spectrum.

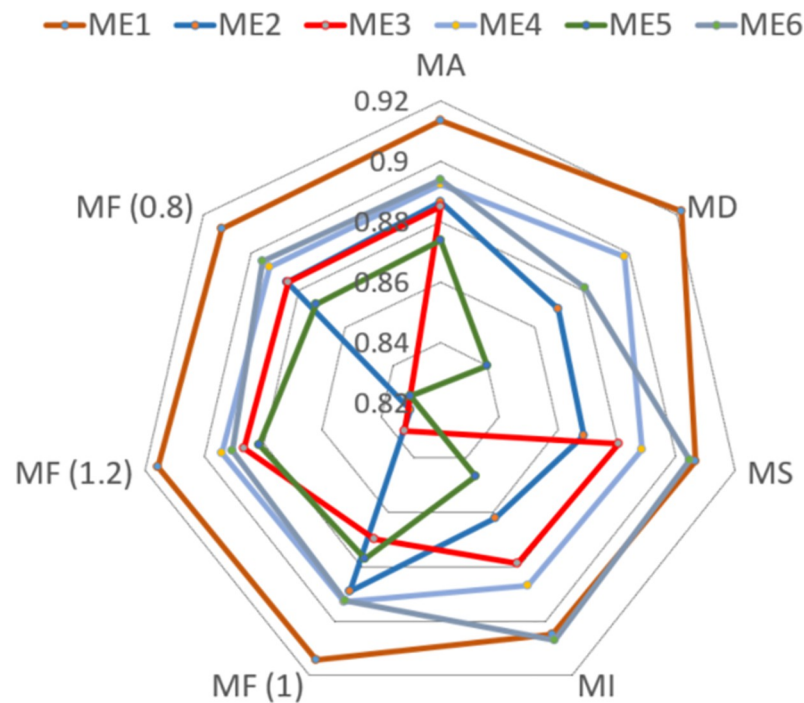


Fig 6. Performance of different fault detection method.

<https://doi.org/10.1371/journal.pone.0303084.g006>

In parallel, the observer generates a set of 1000 observed data points, employing the methodological framework proposed. These observed data serve as the testbed for our fault detection scheme, providing a robust dataset against which the scheme's efficacy is measured.

To ascertain the fault detection scheme's performance with precision, we employ a suite of indexes as follows.

1) MA:

$$MA = \frac{TP + TN}{TP + TN + FP + FN} \tag{43}$$

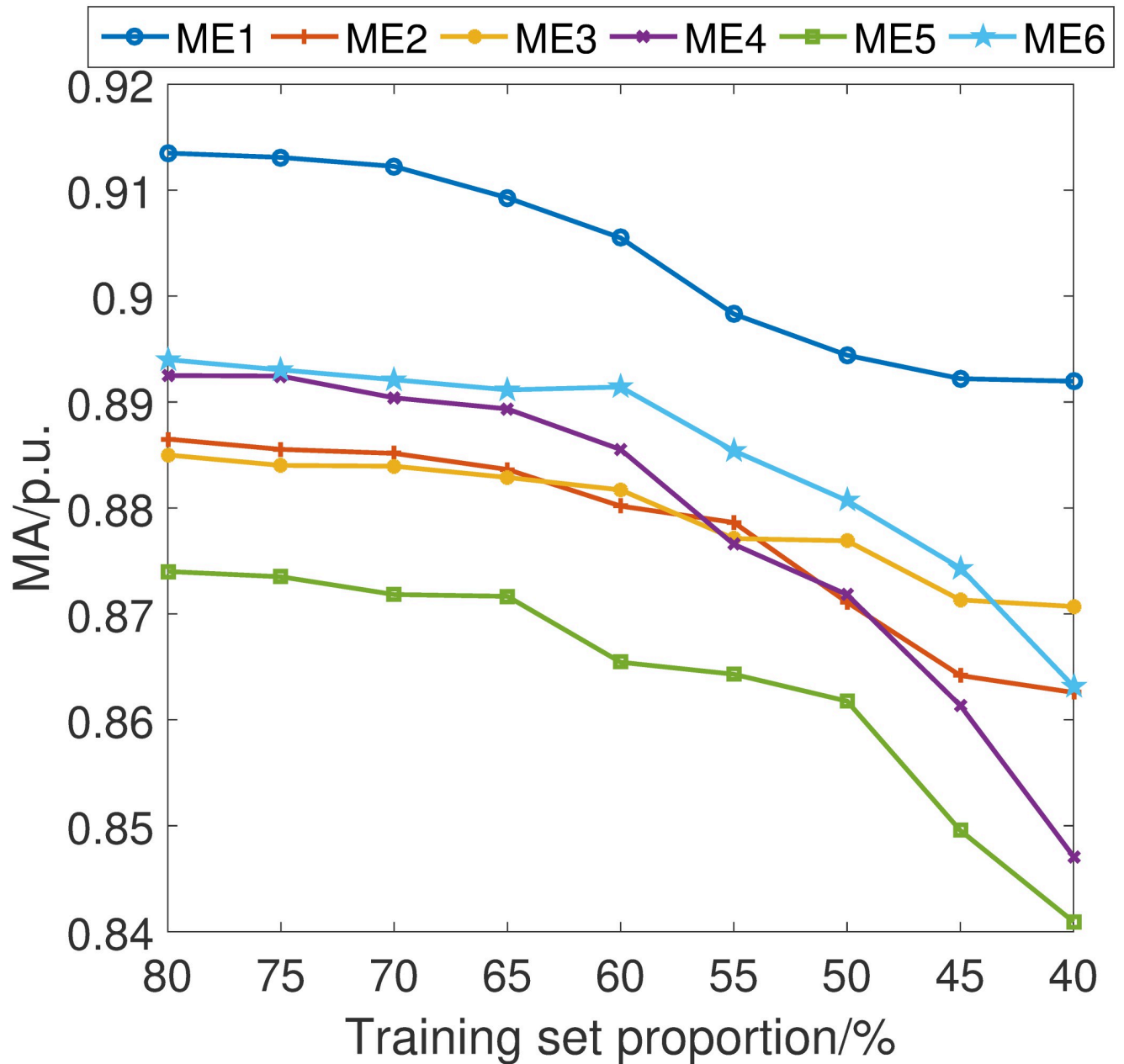


Fig 7. MA index considering different training set proportion.

<https://doi.org/10.1371/journal.pone.0303084.g007>

2) MD:

$$MD = \frac{TP}{TP + FN} \tag{44}$$

3) MS:

$$MS = \frac{TP}{TP + FP} \tag{45}$$

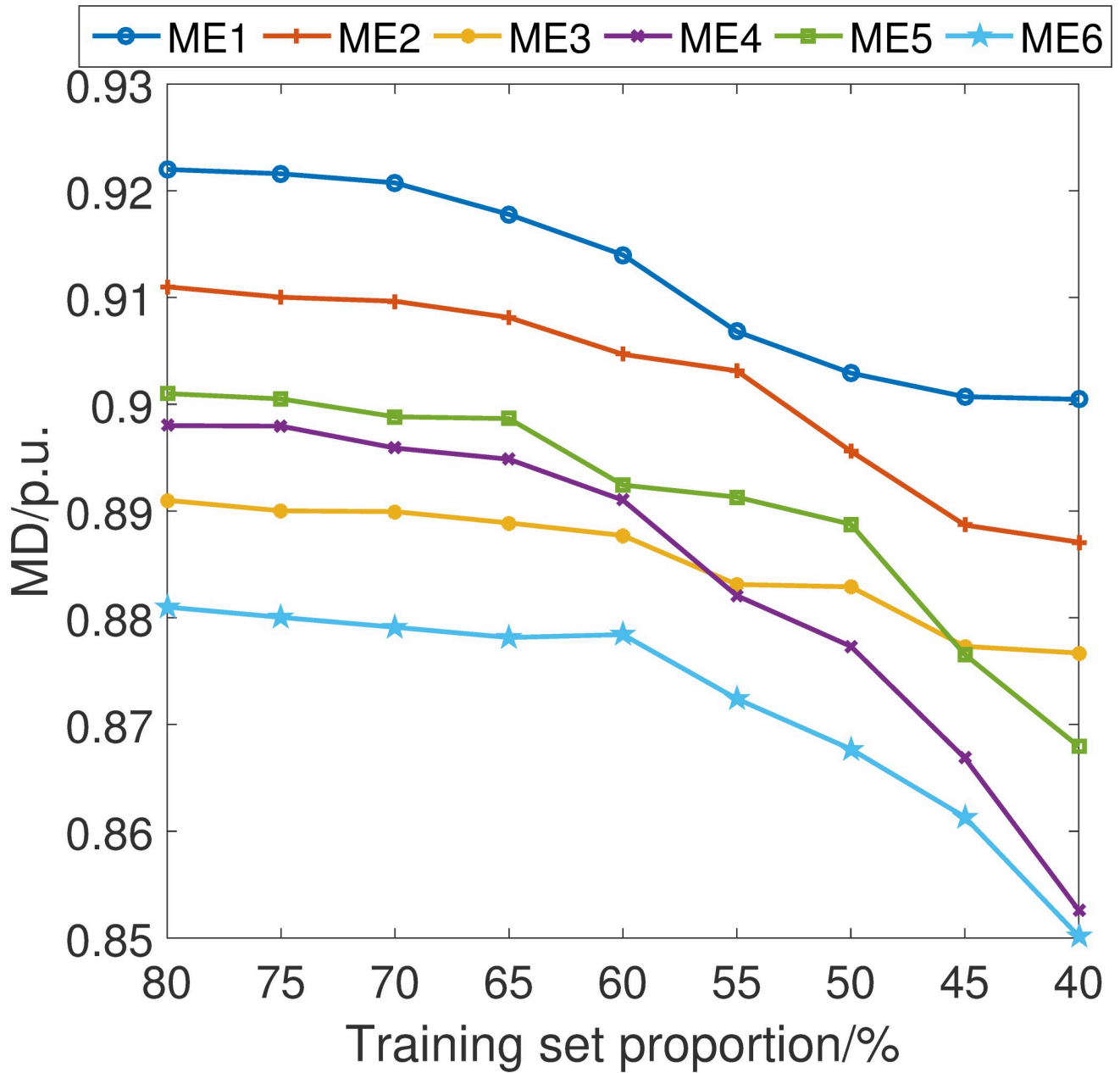


Fig 8. MD index considering different training set proportion.

<https://doi.org/10.1371/journal.pone.0303084.g008>

4) MI:

$$MI = \frac{TN}{TN + FP} \tag{46}$$

5) MF:

$$MF(T) = \frac{(1 + T^2) \cdot MD \cdot MS}{T^2 \cdot MD + MS} \tag{47}$$

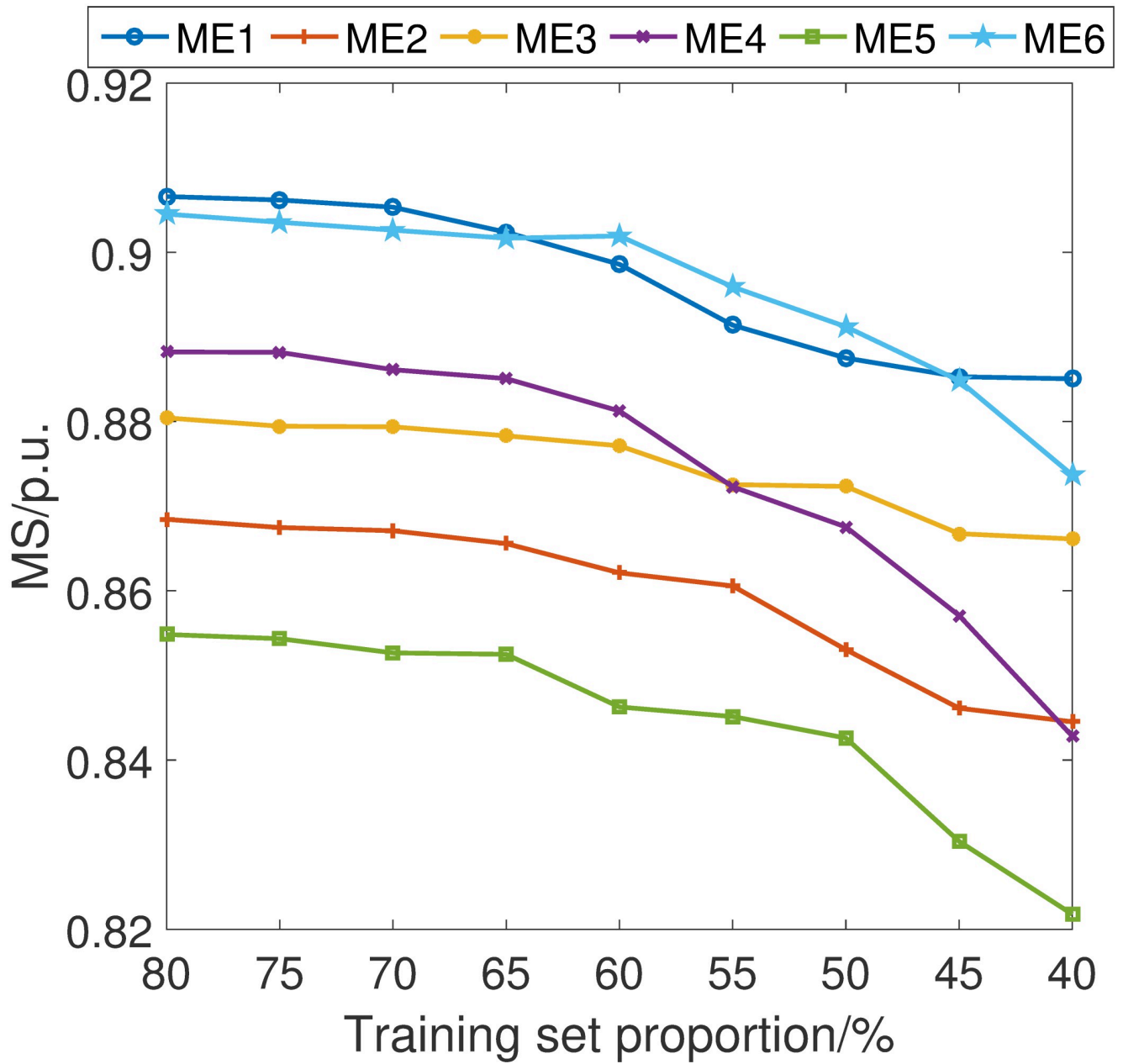


Fig 9. MS index considering different training set proportion.

<https://doi.org/10.1371/journal.pone.0303084.g009>

where TP represents the number of samples correctly predicted as positive class, TN represents the number of samples correctly predicted as negative class, FP represents the number of negative class samples incorrectly predicted as positive class, FN represents the number of positive class samples incorrectly predicted as negative class. MA represents accuracy, MD represents precision, MS represents recall, MI represents false detection rate, and MF represents a comprehensive performance indicator that can comprehensively consider the performance of the model in terms of both miss detection rate and false detection rate.

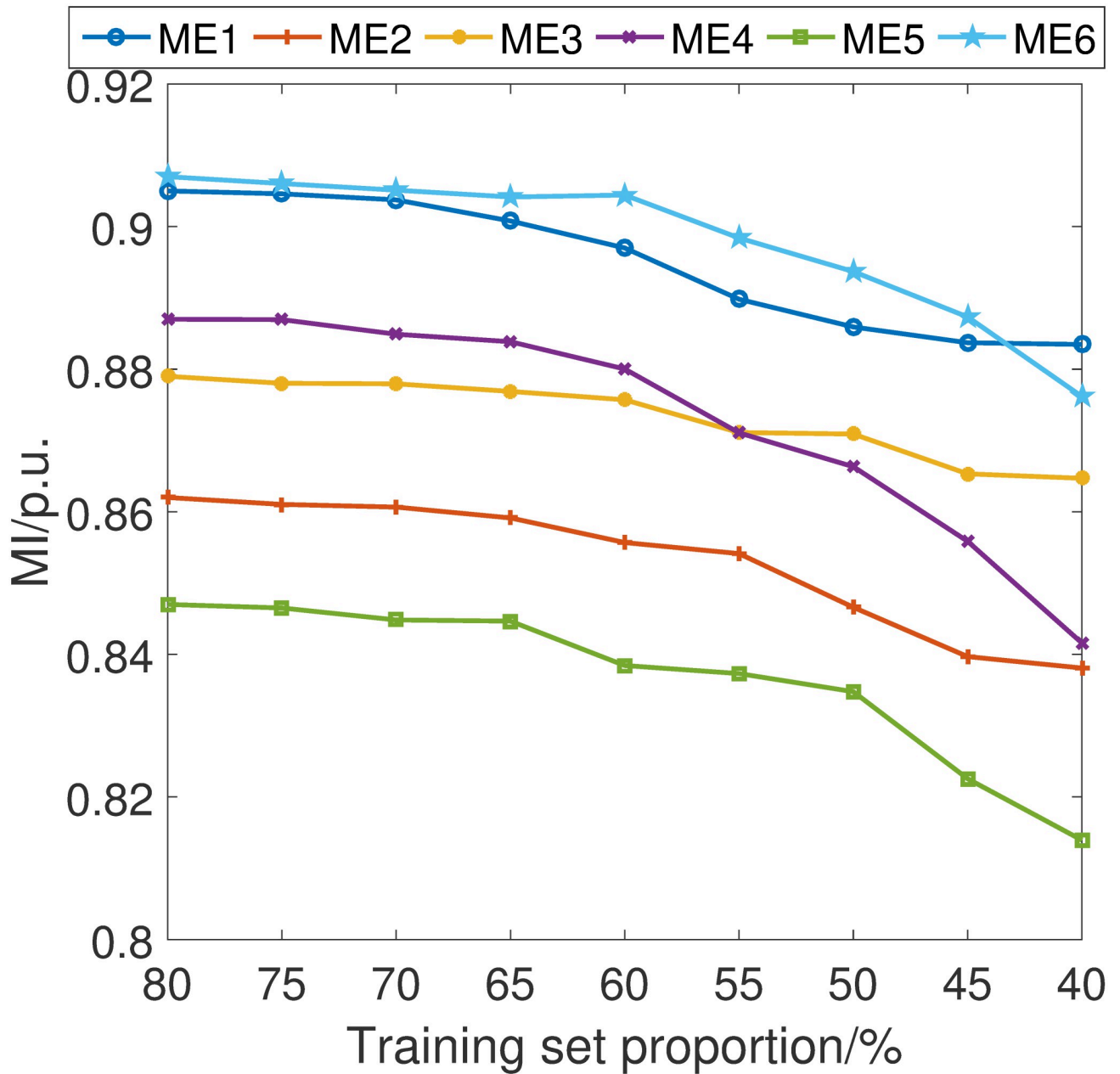


Fig 10. MI index considering different training set proportion.

<https://doi.org/10.1371/journal.pone.0303084.g010>

To comprehensively evaluate the efficacy of our proposed relation-based fault detection scheme, we have rigorously compared it against a suite of five alternative methods. These methods, each with its distinct approach to fault detection, are enumerated as follows:

ME1: Our novel relation-based fault detection scheme, which stands at the forefront of our research. ME2: A related fault detection scheme utilizing a relation network, yet lacking the prototype module, to discern the value added by this component [22]. ME3: A fault detection scheme employing a multilayer perceptron, representing a standard in neural network applications [23]. ME4: A scheme that applies signal forecasting methods, offering a perspective on the utility of time-series predictive analysis in fault detection [24]. ME5: A support vector machine-based fault detection scheme, capitalizing on the strengths of SVMs in pattern recognition [25]. ME6: A fault detection scheme that incorporates a clustering artificial bee colony

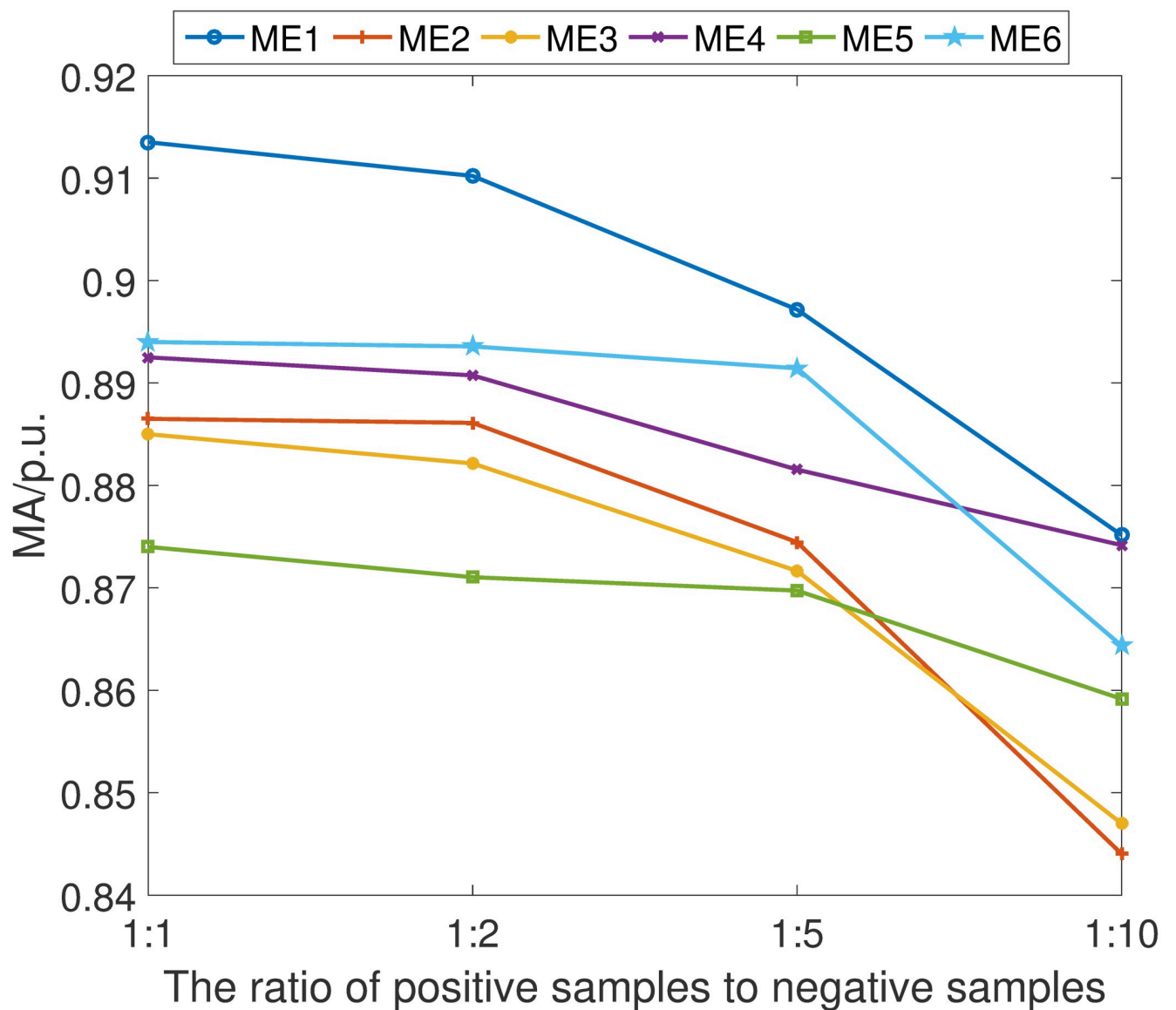


Fig 11. MA index under different ratio of positive samples.

<https://doi.org/10.1371/journal.pone.0303084.g011>

algorithm, reflecting the innovative use of swarm intelligence in anomaly detection [26]. Our simulation results, as depicted in Fig 6, clearly demonstrate that the proposed fault detection scheme (ME1) outperforms its counterparts across all algorithmic evaluation indices. This superior performance is attributable to the scheme’s strategic focus on exploiting the discrepancies between normal and compromised data. In contrast, the other fault detection schemes primarily emphasize feature extraction.

The distinctive advantage of the proposed scheme arises from its ability to discern the subtle variances that distinguish authentic data from manipulated data. This is in stark contrast to other schemes, which may inadvertently learn commonalities between normal and compromised data, thereby diminishing their detection capabilities.

In pursuit of a comprehensive understanding of the stability and robustness of our proposed fault detection scheme, we have conducted an in-depth analysis of its performance

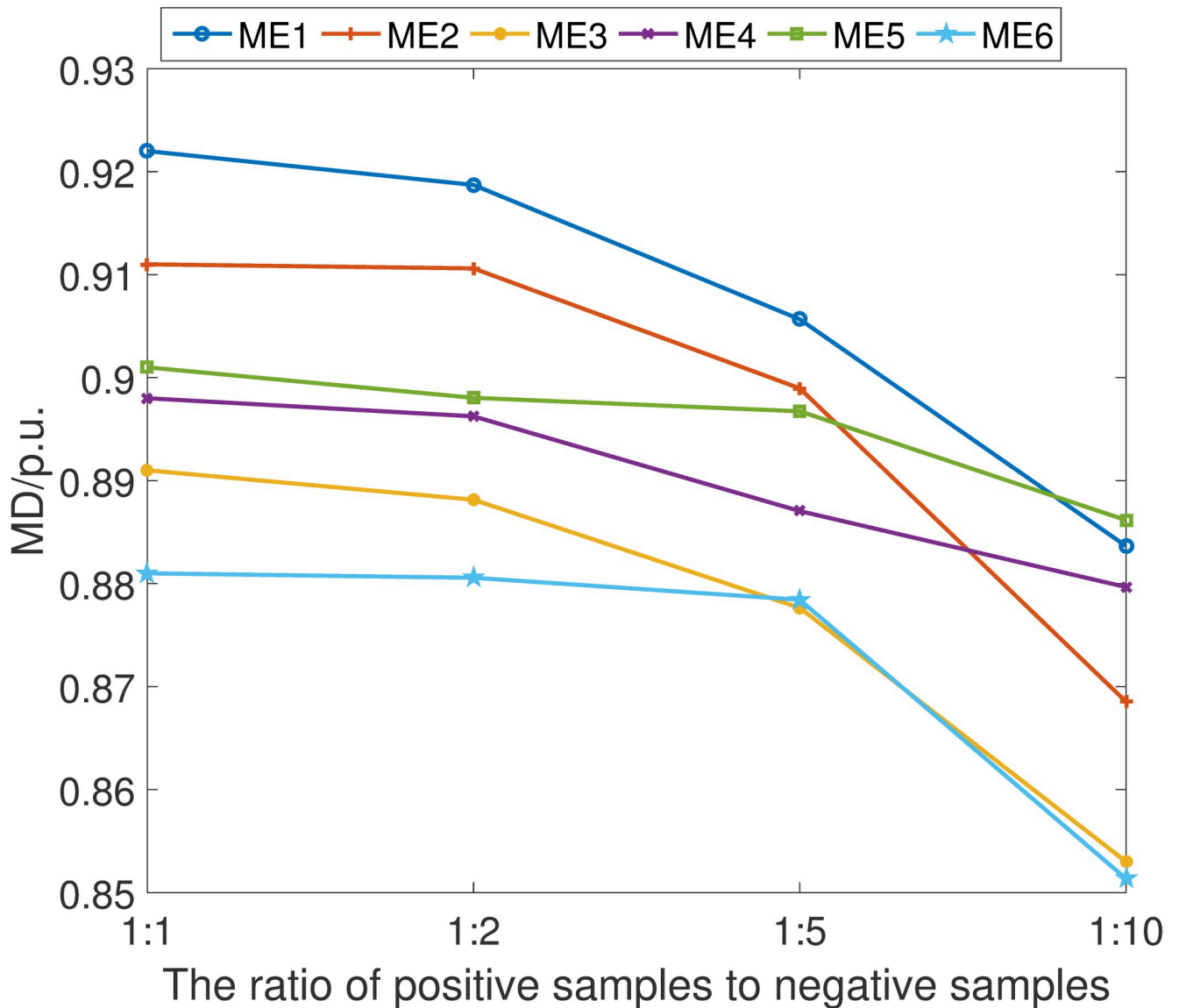


Fig 12. MD index under different ratio of positive samples.

<https://doi.org/10.1371/journal.pone.0303084.g012>

across varying training set sizes. Specifically, we have incrementally adjusted the proportion of the data used for training by 5% intervals, ranging from 40% to 80% of the total dataset.

The simulations are shown in Figs 7–10. It can be learned that while there is an expected decline in the performance of the proposed fault detection scheme as the training sample size decreases, it nonetheless maintains a position within the upper echelon of performance metrics. This observation holds true even when compared with alternative schemes, some of which may occasionally surpass our method at certain training sample sizes. Crucially, these results confirm that our fault detection scheme consistently delivers an excellent detection capability within the sample size parameters explored in this study.

The resilience of the proposed scheme, as evidenced by these simulations, underscores its robustness and affirms its effectiveness in fault detection, even under constraints of limited data availability. This finding is particularly significant for practical applications where data

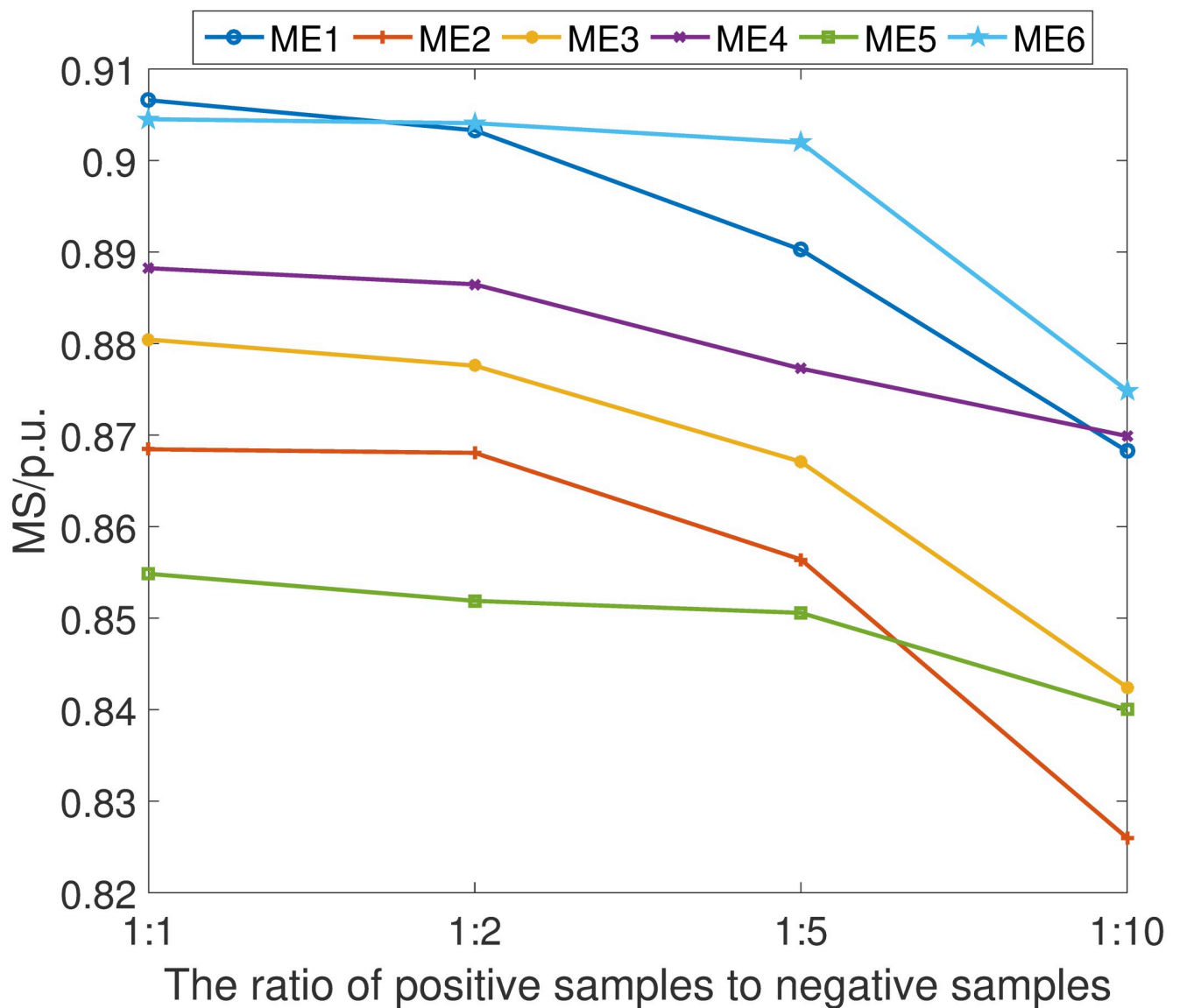


Fig 13. MS index under different ratio of positive samples.

<https://doi.org/10.1371/journal.pone.0303084.g013>

may be scarce or costly to acquire, further attesting to the versatility and practicality of our approach.

In light of the practical scenario where compromised data samples may be sparse, we have undertaken a thorough examination of the proposed fault detection scheme’s reliability and stability across varying ratios of positive (compromised) to negative (normal) samples. We have methodically evaluated the scheme at the following ratios: 1:1, 1:2, 1:5, and 1:10, thereby encompassing a broad spectrum of imbalanced datasets.

The empirical results are shown in Figs 11–14. It can be learned that while there is a discernible decrement in the scheme’s performance as the proportion of positive samples diminishes relative to negative samples, the scheme’s overall efficacy remains comparatively advantageous against other detection methods. This performance degradation is primarily

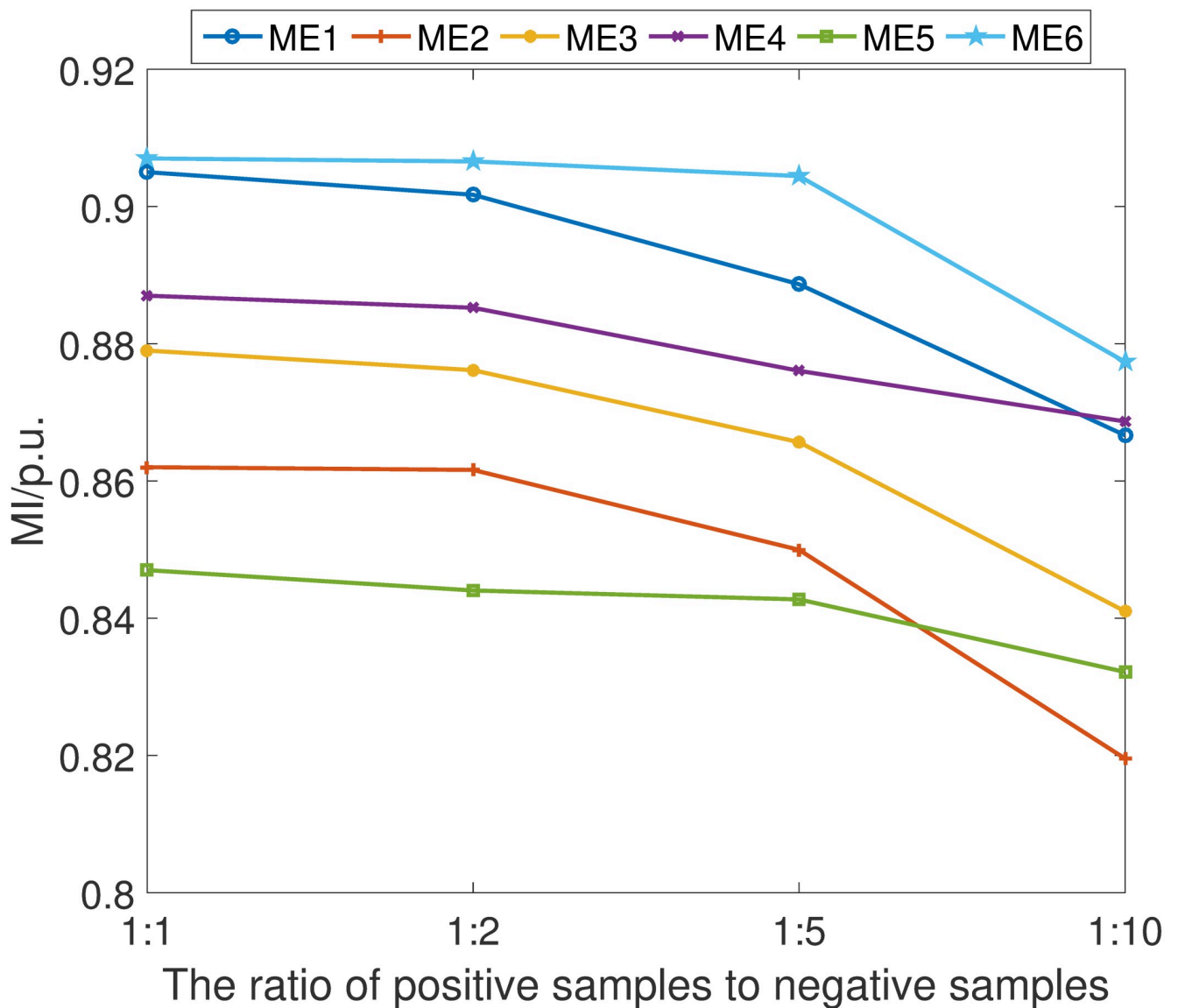


Fig 14. MI index under different ratio of positive samples.

<https://doi.org/10.1371/journal.pone.0303084.g014>

attributed to the network's constrained ability to adequately learn and distinguish the characteristics of positive samples when they are underrepresented.

Despite this challenge, it is noteworthy that the proposed fault detection scheme continues to demonstrate a commendable level of fault identification accuracy. This resilience is a testament to the robust design of our detection network, which has been engineered to cope with the inherent difficulties posed by sample imbalance. Furthermore, the findings elucidate the critical need for a detection system that can maintain high performance levels even when faced with the realistic limitations of data availability, thus reinforcing the practical applicability and superiority of our proposed scheme in real-world settings.

Conclusion

In this study, we address the critical issue of fault management within the distributed controllers of active distribution networks. To this end, we have meticulously developed observers capable of tracking anomalous data indicative of system faults. These observers have been intricately designed to accommodate a variety of fault targets, ensuring a comprehensive monitoring framework. Building upon the data procured by these observers, we have introduced an innovative relation-based fault detection scheme. This scheme leverages the interdependencies between observed data and actual measurements to pinpoint discrepancies that may signal the presence of faults. The simulation results robustly validate the efficacy of our observers and the relation-based fault detection scheme.

Author Contributions

Formal analysis: Tao Qin.

Investigation: Lingyun Tong.

Software: Haoliang Zhang.

Visualization: Weihang Xu.

Writing – original draft: Xinjie Sun.

References

1. Shafiei M, Golestaneh F, Ledwich G, Nourbakhsh G, Gooi HB, Arefi A. Fault detection for low-voltage residential distribution systems with low-frequency measured data. *IEEE Systems Journal*. 2020; 14(4):5265–5273. <https://doi.org/10.1109/JSYST.2020.2970491>
2. Wang X, Wei X, Gao J, Song G, Kheshti M, Guo L. High-impedance fault detection method based on stochastic resonance for a distribution network with strong background noise. *IEEE Transactions on Power Delivery*. 2021; 37(2):1004–1016. <https://doi.org/10.1109/TPWRD.2021.3075472>
3. Nsaif YM, Hossain Lipu MS, Hussain A, Ayob A, Yusof Y, Zainuri MAA. A new voltage based fault detection technique for distribution network connected to photovoltaic sources using variational mode decomposition integrated ensemble bagged trees approach. *Energies*. 2022; 15(20):7762. <https://doi.org/10.3390/en15207762>
4. Gao J, Wang X, Wang X, Yang A, Yuan H, Wei X. A high-impedance fault detection method for distribution systems based on empirical wavelet transform and differential faulty energy. *IEEE Transactions on Smart Grid*. 2021; 13(2):900–912. <https://doi.org/10.1109/TSG.2021.3129315>
5. Srivastava I, Bhat S, Vardhan BS, Bokde ND. Fault detection, isolation and service restoration in modern power distribution systems: A review. *Energies*. 2022; 15(19):7264. <https://doi.org/10.3390/en15197264>
6. Gu JC, Huang ZJ, Wang JM, Hsu LC, Yang MT. High impedance fault detection in overhead distribution feeders using a DSP-based feeder terminal unit. *IEEE Transactions on Industry Applications*. 2020; 57(1):179–186. <https://doi.org/10.1109/TIA.2020.3029760>

7. Sapountzoglou N, Lago J, De Schutter B, Raison B. A generalizable and sensor-independent deep learning method for fault detection and location in low-voltage distribution grids. *Applied Energy*. 2020; 276:115299. <https://doi.org/10.1016/j.apenergy.2020.115299>
8. Guo MF, Liu WL, Gao JH, Chen DY. A data-enhanced high impedance fault detection method under imbalanced sample scenarios in distribution networks. *IEEE Transactions on Industry Applications*. 2023;. <https://doi.org/10.1109/TIA.2023.3256975>
9. Jia K, Yang B, Bi T, Zheng L. An improved sparse-measurement-based fault location technology for distribution networks. *IEEE Transactions on Industrial Informatics*. 2020; 17(3):1712–1720.
10. Mirshekali H, Dashti R, Keshavarz A, Shaker HR. Machine learning-based fault location for smart distribution networks equipped with micro-PMU. *Sensors*. 2022; 22(3):945. <https://doi.org/10.3390/s22030945> PMID: 35161696
11. Furse CM, Kafal M, Razzaghi R, Shin YJ. Fault diagnosis for electrical systems and power networks: A review. *IEEE Sensors Journal*. 2020; 21(2):888–906. <https://doi.org/10.1109/JSEN.2020.2987321>
12. Jan SU, Lee YD, Koo IS. A distributed sensor-fault detection and diagnosis framework using machine learning. *Information Sciences*. 2021; 547:777–796. <https://doi.org/10.1016/j.ins.2020.08.068>
13. Xue T, Zhong M, Li L, Ding SX. An optimal data-driven approach to distribution independent fault detection. *IEEE Transactions on Industrial Informatics*. 2020; 16(11):6826–6836. <https://doi.org/10.1109/TII.2020.2976043>
14. Li B, Delpha C, Diallo D, Migan-Dubois A. Application of Artificial Neural Networks to photovoltaic fault detection and diagnosis: A review. *Renewable and Sustainable Energy Reviews*. 2021; 138:110512. <https://doi.org/10.1016/j.rser.2020.110512>
15. Rivas AEL, Abrao T. Faults in smart grid systems: Monitoring, detection and classification. *Electric Power Systems Research*. 2020; 189:106602. <https://doi.org/10.1016/j.epsr.2020.106602>
16. Liang YL, Li KJ, Ma Z, Lee WJ. Typical fault cause recognition of single-phase-to-ground fault for overhead lines in nonsolidly earthed distribution networks. *IEEE Transactions on Industry Applications*. 2020; 56(6):6298–6306. <https://doi.org/10.1109/TIA.2020.3020526>
17. Sapountzoglou N, Lago J, Raison B. Fault diagnosis in low voltage smart distribution grids using gradient boosting trees. *Electric Power Systems Research*. 2020; 182:106254. <https://doi.org/10.1016/j.epsr.2020.106254>
18. Yuan Y, Dehghanpour K, Bu F, Wang Z. Outage detection in partially observable distribution systems using smart meters and generative adversarial networks. *IEEE Transactions on Smart Grid*. 2020; 11(6):5418–5430. <https://doi.org/10.1109/TSG.2020.3008770>
19. Alhanaf A S, Balik H H, Farsadi M. Intelligent fault detection and classification schemes for smart grids based on deep neural networks. *Energies*, 2023, 16(22): 7680. <https://doi.org/10.3390/en16227680>
20. Li Y, Wei X, Lin J, Niu G. A robust fault location method for active distribution network based on self-adaptive switching function. *International journal of electrical power and energy systems*. 2023;.
21. Zhang W, Chang Z, Zhang C, Song G, Tan W. A quick fault location and isolation method for distribution network based on adaptive reclosing. *IET Generation, Transmission & Distribution*. 2022; 16.
22. Wang Yuxin and Xie Hongtao and Zha Zhengjun and Tian Youliang and Fu Zilong and Zhang Yongdong. R-Net: A relationship network for efficient and accurate scene text detection. *IEEE Transactions on Multimedia*, 2020, 23: 1316–1329. <https://doi.org/10.1109/TMM.2020.2995290>
23. Kilincer Ilhan Firat and Ertam Fatih and Sengur Abdulkadir and Tan Ru-San and Acharya U Rajendra. Automated detection of cybersecurity attacks in healthcare systems with recursive feature elimination and multilayer perceptron optimization. *Biocybernetics and Biomedical Engineering*, 2023, 43(1): 30–41. <https://doi.org/10.1016/j.bbe.2022.11.005>
24. Neelima Medikonda and Prabha I Santi. Optimized deep network based spoof detection in automatic speaker verification system. *Multimedia Tools and Applications* 83.5 (2024): 13073–13091. <https://doi.org/10.1007/s11042-023-16127-w>
25. Arunkumar M and Kumar K Ashok. GOSVM: Gannet optimization based support vector machine for malicious attack detection in cloud environment. *International Journal of Information Technology*, 2023, 15(3): 1653–1660. <https://doi.org/10.1007/s41870-023-01192-z>
26. Aghakhani Sina and Larjani Ata and Sadeghi Fatemeh and Martín Diego and Shahrakht Ali Ahmadi. A Novel hybrid artificial bee colony-based deep convolutional neural network to improve the detection performance of backscatter communication systems. *Electronics*, 2023, 12(10): 2263. <https://doi.org/10.3390/electronics12102263>