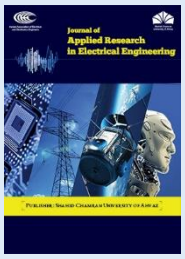
Shahid Chamran University of Ahvaz

Iranian Association of Electrical and Electronics Engineers

Journal of Applied Research in Electrical Engineering

E-ISSN: 2783-2864
P-ISSN: 2717-414X
Homepage: https://jaree.scu.ac.ir/



Research Article

Entropy-Based and Deep Learning–Driven Detection of Stealthy Cyberattacks in Smart Distribution Networks

Hamidreza Amiri [1,*]

[1]*Electrical Power Distribution Company of Sari, Mazandaran, Iran*

* *Corresponding Author: hamidrezaamiry@yahoo.com*

Abstract: This study investigates and evaluates the performance and accuracy of advanced techniques for detecting concealed and stealthy cyber-attacks within the standard IEEE 33-bus distribution network. Two representative attack scenarios, Replay Attack and Slowly-Varying/Low-Amplitude Stealth Attack, were simulated in the MATLAB environment to evaluate their impact on system operation. Simulation results indicate that these attacks induce gradual deviations and disturbances in the power flow and voltage profiles of buses No. 6 and 25. To identify such anomalies, two detection mechanisms were employed: a Shannon entropy–based approach and an autoencoder neural network architecture. The evaluation outcomes demonstrate that the entropy-based method provides high sensitivity and low latency in attack identification; however, it exhibits a higher false alarm rate (FAR) in response to minor fluctuations and normal network variations. Conversely, the Autoencoder architecture significantly reduces the false alarm rate and enhances detection accuracy for stealthy and progressive attacks. Ultimately, the hybrid integration of both methods yields a substantial improvement in the overall performance of the intrusion detection system (IDS) for smart distribution networks.

Keywords: **Autoencoder, Entropy shannon, Deep Learning, Stealthy Cyberattacks, Smart Distribution Networks.**

Article history
Received 06 February 2026; Revised 26 June 2026; Accepted 23 September 2026; Published online 15 October 2026.
© 2026 Published by Shahid Chamran University of Ahvaz & Iranian Association of Electrical and Electronics Engineers (IAEEE)
How to cite this article
H. Amiri, "Entropy-based and deep learning-driven detection of stealthy cyberattacks in smart distribution networks," *J. Appl. Res. Electr. Eng.*, vol. 5, no. 1, pp. 01-11, 2026. DOI:10.22055/jaree.2026.51755.1293

Check for updates

1. INTRODUCTION

Electrical energy has become an indispensable component of modern human life, constituting the backbone of nearly all industrial, commercial, and domestic activities. The electrical energy supply chain comprises three fundamental stages: generation, transmission, and distribution, among which distribution networks represent the most widespread and operationally diverse segment. These networks, which may be implemented as overhead or underground systems, receive electrical power from the transmission grid and deliver it to consumers at various voltage levels in accordance with standardized regulations. Distribution companies continuously track, analyse, and regulate system parameters to ensure the delivery of stable and high-quality power to end users. Since disturbances and faults in distribution networks are inevitable, modern utilities employ state-of-the-art equipment and advanced monitoring schemes to minimize operational disruptions and enhance customer satisfaction. Nonetheless, since no system or device is entirely immune to malfunction, any form of fault or anomaly can result in technical or economic losses across the network. Generally, the root causes of distribution network faults can be categorized as either natural or human-induced. Natural phenomena such as lightning strikes, landslides, snowstorms, or severe weather conditions can cause significant damage to electrical infrastructures; conventional mitigation strategies are typically employed to mitigate their effects. However, due to the extensive scale, complex topology, and high level of automation in modern distribution systems, non-natural or human-related errors have become increasingly prevalent and often more challenging to detect and mitigate. While most non-natural incidents are visible and can be identified after occurrence, cyber-attacks represent a distinct class of hidden threats whose presence cannot be directly observed but is inferred through abnormal variations in system parameters. Counteracting such attacks is particularly challenging and costly due to their adaptability,

stealthiness, and ability to exploit the communication and control layers of smart grids. Consequently, distribution utilities are compelled to employ more advanced and optimized detection and mitigation frameworks. Among the promising methodologies for cyber-attack detection are Artificial Neural Networks (ANNs) and pattern recognition algorithms. For instance, Ref. [1] utilized ANN-based techniques to enhance the resilience of a DC microgrid under False Data Injection (FDI) and Denial-of-Service (DoS) attacks. Moreover, cyber threats are capable of compromising distribution systems integrated with photovoltaic (PV) resources. In [2], possible attack vectors were examined, and a three-layer physical topology was proposed as a defensive architecture against such intrusions. A further example is the Distributed Denial-of-Service (DDoS) attack, whose detection through spline function analysis was explored in [3], demonstrating a high degree of detection accuracy. In addition, Ref. [4] applied a Nonlinear Auto Regressive with eXogenous input (NARX) observer to detect FDI attacks in DC microgrids based on estimation residuals. Ref. [5] introduced a machine learning–based framework to record system parameters during attack scenarios, thereby enhancing the system's detection and adaptation capability against newly emerging threats in smart grids. Given the variety of attack vectors and the complexity of communication infrastructures interconnecting AC and DC microgrids, the development of comprehensive detection and defense strategies remains essential. In this regard, Ref. [6] formulated mathematical models of prevalent cyber-attacks and discussed corresponding cyber-defense strategies. Furthermore, energy management during cyber incidents constitutes one of the critical responsibilities of distribution companies. Ref. [7] analysed the impact of common cyber-attacks and proposed an outlier elimination–based approach to enhance the resilience of islanded microgrids during adversarial events. Considering the scope of this research and the findings reported in previous studies, the subsequent sections address various categories of cyber-attacks and their corresponding detection approaches in distributed power systems.

2. Cyber-Attacks (Compact and Stealthy Attacks)

A cyber-attack can be defined as a deliberate and coordinated attempt aimed at gaining unauthorized access to or manipulating the data and operations of computer systems belonging to a predetermined target. Such attacks may be conducted by individual hackers or state-sponsored entities. The most common forms of cyber-attacks include Distributed Denial-of-Service (DDoS), Phishing, Malware, and False Data Injection (FDI) attacks, each of which is designed to achieve specific malicious objectives. Historically, these attacks primarily targeted conventional computer systems and servers. However, with the rapid advancement of science and technology, as well as the widespread integration of the Internet and intelligent control systems, a growing number of industrial systems have become vulnerable to cyber threats. Furthermore, the increasing complexity and interconnectivity of modern digital infrastructures have led to more diverse and severe consequences of cyber intrusions, making their detection and mitigation more challenging than ever before. One of the most critical infrastructures susceptible to malicious cyber-attacks is the electric power distribution network, which is often targeted with the intent to cause operational disruption, information theft, or financial damage. Regardless of the specific attack type, such as DDoS, social engineering, or malware-based attacks, any successful intrusion can impose substantial operational and economic costs on distribution utilities. Therefore, timely detection and mitigation of such cyber threats are of paramount importance for maintaining system reliability and security. For example, in [8], various types of cyber-attacks were introduced into a benchmark WSCC 3-machine 9-bus system, demonstrating that these attacks are capable of triggering unintended circuit breaker operations, consequently leading to system instability. Similarly, Ref. [9] analyzed a cyber-attack on a smart grid incorporating renewable energy sources, revealing that such an intrusion can significantly disturb network voltage levels and effectively disrupt overall system performance. In another study [10], it was shown that cyber-attacks are not necessarily aimed at causing direct physical damage; for instance, DDoS attacks can distort Local Electricity Markets (LEMs) and corrupt operational data. Within the context of the present study, particular attention is given to compact and stealthy cyberattacks in power distribution networks, which exhibit operational behaviors distinct from those of conventional intrusion types. Compact attacks are typically characterized by low data volume and short duration, whereas stealthy attacks are intentionally designed to evolve gradually and remain undetectable by conventional monitoring methods. Representative examples of such attacks include Compact FDI Attacks, Stealthy Replay Attacks, and Coordinated Stealthy Attacks, all of which focus on a limited number of network nodes and operate progressively over a defined time horizon. The objectives of compact and stealthy cyber-attacks are similar to those of other malicious intrusions, including disabling protection relays, inducing instability, altering voltage and frequency parameters, and deteriorating overall power quality. These effects can lead to equipment failures, parameter distortions, and increased operational costs. Given the crucial importance of maintaining stable operational parameters in distribution systems and minimizing operational expenditures, the deployment of advanced and intelligent detection methodologies to identify and mitigate the effects of compact and stealthy attacks is both essential and inevitable.

3. Entropy Analysis and Deep Learning

Entropy analysis serves as a statistical and quantitative indicator of uncertainty, randomness, and structural disorder within a dataset. In the context of power distribution networks, entropy provides a valuable indication of hidden variations in parameters such as voltage, power, current, and power factor. Generally, entropy-based analysis is computationally lightweight and easily interpretable. For a discrete random variable $X$with n possible states and a probability distribution$P(x_i)$, entropy is defined as:

$$p(x_i)\ \log_b(p(x_i)) - \sum_{i=1}^{n} = H(X) \quad (1)$$

Where $H(X)$denotes the entropy of the random variable$X$, $P(x_i)$ represents the probability of the i^{th}state, and $\log_b$is the logarithmic base determined according to natural or binary representation. This method operates by identifying repetitive signal structures, quantifying temporal fluctuations, and analysing the time-evolving complexity of system signals. Consequently, entropy analysis can be effectively applied to monitor data variations in distribution networks, detect hidden imbalances through temporal pattern analysis, and identify sudden parameter changes that may indicate anomalous or malicious behaviour.

Deep learning, a subset of machine learning, primarily relies on multi-layer neural network architectures. The output of a neuron in the j^{th}layer can be expressed as:

$$f\left(w^{(j)}.a^{(j-1)}+b^{(j)}\right)=f\left(z^{(j)}\right)=a^{(j)} \quad (2)$$

where $W^{(j)}$denotes the weight matrix of the j^{th}layer, $a^{(j-1)}$ represents the output vector from the preceding layer, $b^{(j)}$ is the bias term, and $f(\cdot)$ is the activation function. Deep learning algorithms possess exceptional capabilities for feature learning, pattern recognition, and extracting hierarchical representations from large-scale and complex datasets. By leveraging multiple interconnected neural layers, they can efficiently learn spatial and temporal correlations within data, enabling robust detection of anomalies and complex behavioral patterns. Due to the massive data volume and high dimensionality of modern networks, deep learning algorithms are widely used in smart grid cybersecurity. They help model complex data patterns, extract high-level feature representations, and improve the accuracy and reliability of anomaly detection.

4. Simulation of Attacks and Their Detection

Simulating cyber-attacks in distribution networks constitutes a fundamental phase in cybersecurity assessment and in the formulation of robust detection frameworks. It provides distribution companies with a logical and reliable perspective on potential vulnerabilities. Through accurate attack simulations, the behavior of a sample network under real-world threats can be effectively predicted, and weak points within the network can be identified. This process enables an evaluation of the effectiveness of detection algorithms and their ability to mitigate cyberattacks. To achieve this, variations in key network parameters such as voltage level, current, and active power are introduced to simulate a compact cyberattack. This approach enables us to assess the sensitivity and detection capabilities of the aforementioned algorithms when exposed to network anomalies. For a more accurate assessment of algorithmic performance, two types of attacks Stealth—Attack and Replay Attack are—simulated compactly and covertly on a standard IEEE 33-bus network. The IEEE 33-bus system was selected because it is one of the most widely used benchmark distribution networks in the literature, featuring a realistic radial topology and sufficient operational complexity for evaluating the effectiveness of cyberattack detection algorithms. As illustrated in Fig. 1, the attack injection points on the sample network are indicated.

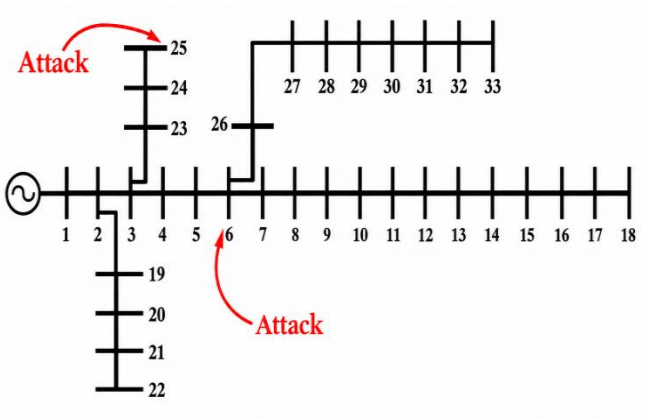


Fig. 1: The network under attack

Based on selected target buses and the initial conditions of the 33-bus test network, the initial values of critical parameters for buses 6 and 25, considering more realistic conditions, are provided in Table 1.

Table 1: key operating parameters of the test network prior to the cyberattack

Bus	Voltage(pu)	Current(A)	Active Power(kW)
6	1.0100	50	500
25	0.9950	45	450

Considering these baseline configurations and the characteristics of the implemented attack models, the subsequent sections investigate and evaluate the network's operational response and the performance of the proposed detection mechanisms under the simulated cyber-attack scenarios.

4.1. Replay Attack

In the Replay Attack analysis, we focus on a replay-based scenario in which previously recorded (and manipulated) measurements are injected into the system; a complementary stealthy variant that evolves gradually is also examined on the test network. Due to the sudden nature of this compact attack, the parameters of voltage, current, and active power at buses 6 and 25 exhibit abrupt variations. The falsified data are equivalent in magnitude to previous real changes in the network, and the attack duration is kept within a few seconds (a few sampling intervals) to remain undetected by the network's monitoring and detection units. Fig. 2 depicts the time-series traces of the affected variables at buses 6 and 25, highlighting pre-attack and post-injection behavior. As observed, the attack duration is only a few seconds, preventing detection by supervisory units. However, this duration and intensity are fully adjustable by the attacker depending on their objectives. The modified parameter values are summarized in Table 2. The results presented in Table 2 correspond to the output of the executed attack, illustrating the potential negative or positive effects of this attack type. Moreover, such attacks, due to the use of previously recorded parameter values and their short duration, are highly dangerous, as they can result in the issuance of incorrect control commands.

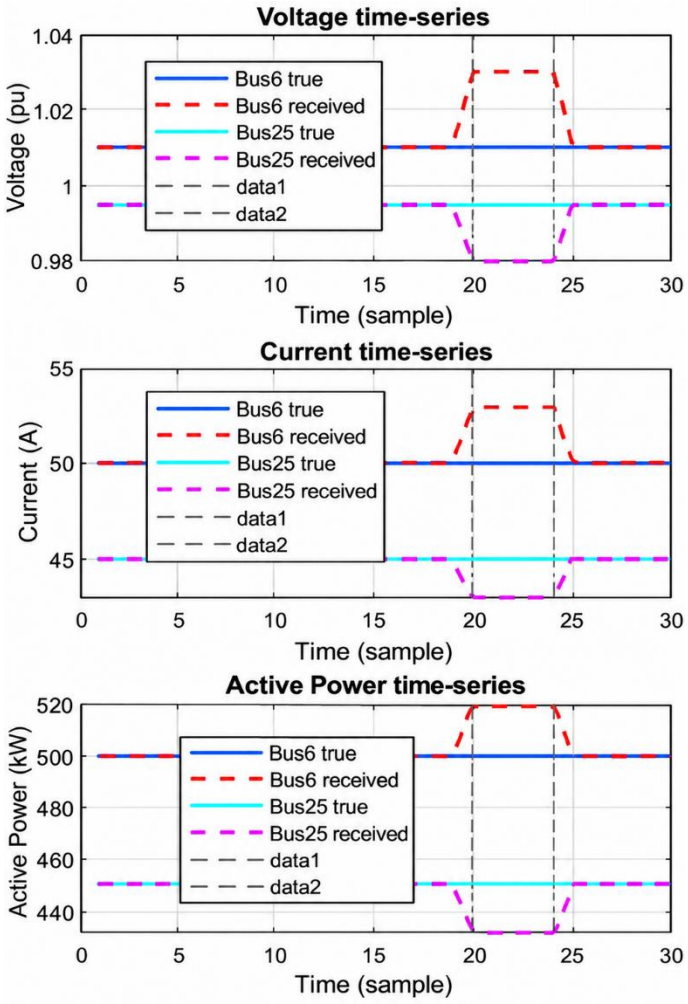


Fig. 2: Simulation results before and after the attack on buses 6 and 25

Table 2: Comparison of system values before and after the cyberattack

	Before	After	Change (%)
V_{bus6}(pu)	1.0100	1.0300	+1.98
(a)I_{bus6}	50	53	+6
(kW)P_{bus6}	500	520	+4
(pu)V_{bus25}	0.9950	0.9800	-1.51
(a)I_{bus25}	45	43	-4.44
(kW)P_{bus25}	450	430	-4.44

4.2. Detection Using Entropy Analysis

Given the destructive impact of this type of attack, entropy analysis is first employed to detect such anomalies. Specifically, the Shannon Information Entropy criterion is used to identify anomalies induced by the Replay Attack. Due to the stable statistical structure of the monitored parameters (voltage, current, and power), replacing real-time data with replayed samples alters their distribution within a defined time window, which manifests as a change in the entropy value. The entropy $E(t)$is computed based on discrete probability estimation as follows:

$$E(t) = -\sum_{j=1}^{B} p_j(t)\ \log_2\big(p_j(t)\big) \qquad (3)$$

where B denotes the total number of histogram bins used for probability estimation (B = 10), $p_j(t)$ is the probability associated with the jth histogram bin within the time window [t, t+ω−1], and ω represents the window length, set to five samples. The probability distribution was obtained using a normalized histogram, where $p_j(t)$was calculated as the ratio of the number of samples falling into the jth bin to the total number of samples within the sliding window. The value of *E(t)* numerically expresses the uncertainty or dispersion of the distribution within the defined window. Using the above parameter settings, Fig. 3 and Fig. 4 illustrate the entropy-based detection results for Replay Attacks applied to buses 6 and 25, respectively.

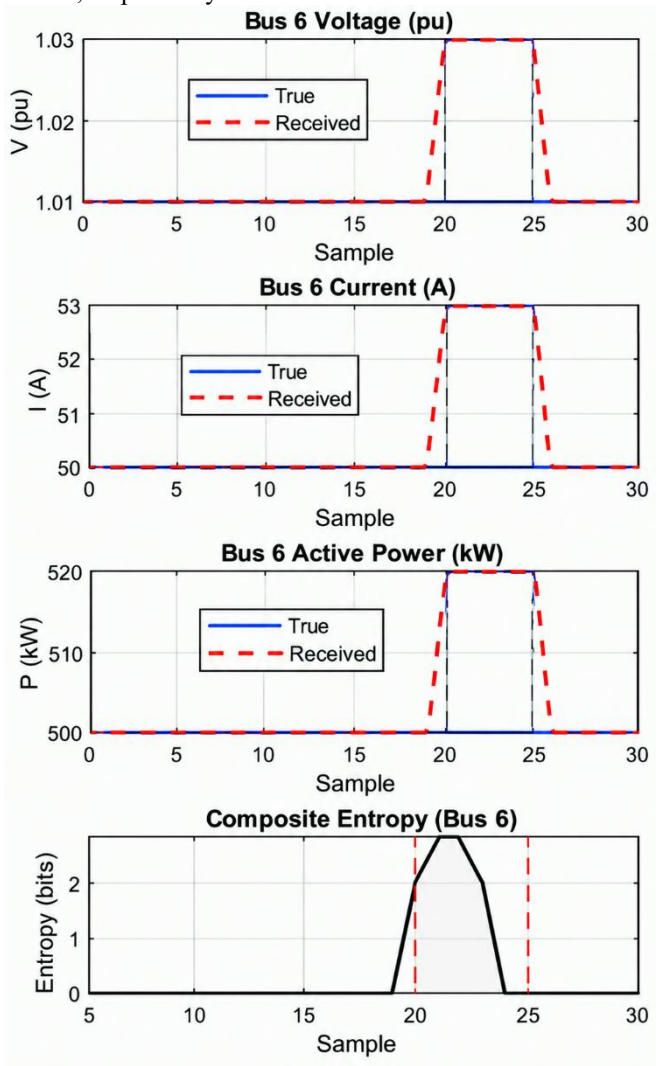


Fig. 3: Replay Attack detection based on Entropy analysis at Bus 6

To enhance detection sensitivity against multi-parameter attacks, three separate analysis windows are computed per bus, and a composite metric is defined. This composite value is compared with a statistical threshold to determine the occurrence of an attack. It should be noted that the entropy computation employs a sliding window mechanism, where each entropy estimate corresponds to the averaged statistics of several preceding samples. As a result, any observable decline in entropy may not coincide exactly with the final attack sample; this delay stems from the cumulative data aggregation and the discrete nature of histogram-based estimation. However, entropy-based detection in isolation demonstrates restricted sensitivity to extremely stealthy or

continuous intrusion patterns [11, 12]. Hence, an integrated deep learning framework is concurrently implemented to augment detection robustness and improve overall reliability.

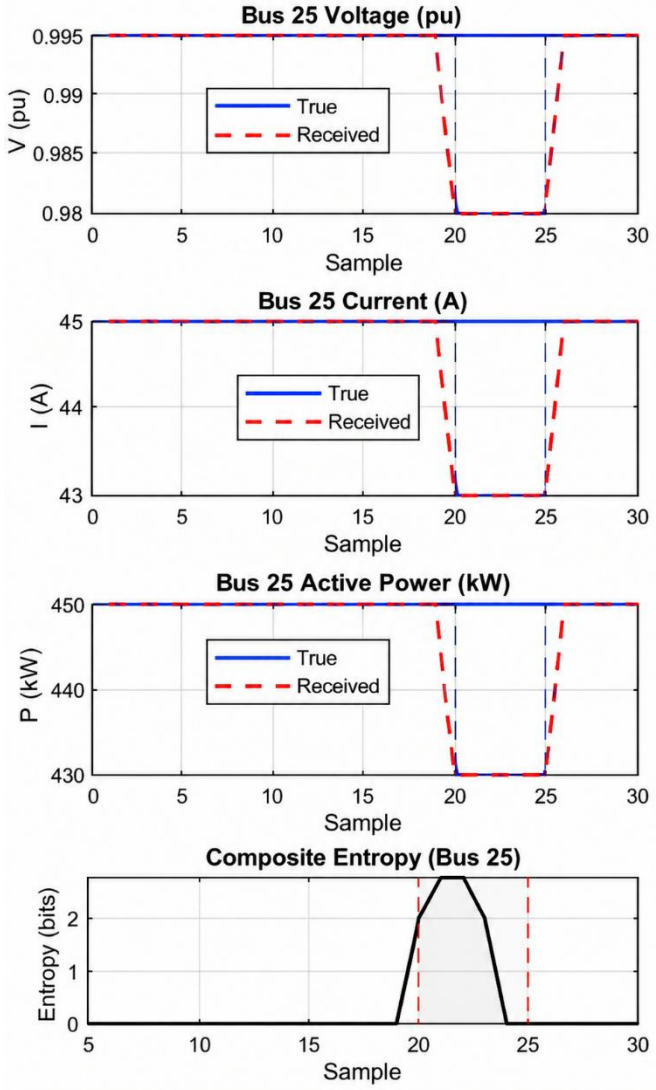


Fig. 4: Replay Attack detection based on Entropy analysis at Bus 25

4.3. Detection Using Combined Entropy and Deep Learning Analysis

Given the properties of the attack and the characteristics of entropy analysis, a deep learning algorithm is integrated to improve detection accuracy. In this study, an Autoencoder (AE) architecture is employed concurrently with entropy analysis. The input data, including voltage, current, power, and entropy results for each time sample, are fed into the Autoencoder network. The network then reconstructs pre-attack values, and the reconstruction error is used to identify anomalies. The reconstruction error for each time instance $t$is calculated as the mean difference between the input and output values of the Autoencoder, as expressed below:

$$E_{AE}(t) = (X_d(t) - X'_d(t))^2 . \sum_{d=1}^{D} \frac{1}{D} \quad (4)$$

where $t$denotes the time index, D is the number of measured parameters (features), $X_d(t)$ represents the actual value of the d^{th} parameter at time t, and $X'_d(t)$ is the corresponding reconstructed value by the Autoencoder. Overall, fault or anomaly detection within the Autoencoder framework relies on evaluating the statistical deviation between actual and reconstructed parameter values. Fig. 5 and Fig. 6 illustrate the detection results obtained using the combined Autoencoder and entropy analyses for buses 6 and 25, respectively.

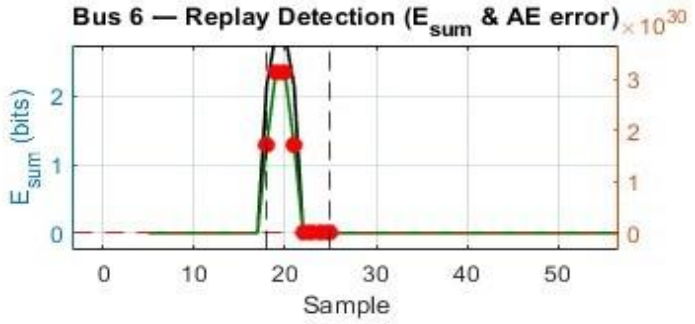


Fig. 5: Fault detection output by Autoencoder and entropy analysis for bus 6

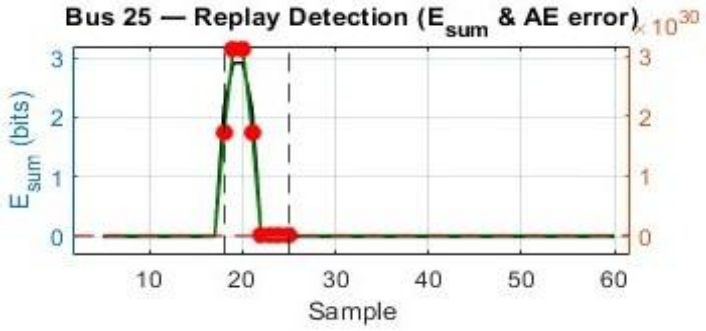


Fig. 6: Fault detection output by Autoencoder and entropy analysis for bus 25

As observed, the integration of entropy-derived features as auxiliary input parameters within the Autoencoder framework establishes a comprehensive physico-statistical detection scheme, substantially enhancing anomaly recognition accuracy across the simulated distribution network. To better understand the performance of these detection mechanisms, Table 3 presents the numerical results of the Replay Attack in terms of detection delay, which serves as a key metric in smart grid systems. It is evident that entropy analysis, owing to its purely statistical formulation, demonstrates higher responsiveness to rapid fluctuations; however, the Autoencoder model—due to its reconstruction-driven nature-incurs a relatively longer detection latency while achieving notably lower false alarm rates.

Table 3: Comparison of attack detection delays among different detection mechanisms

	Entropy	Autoencoder
Bus6	2 samples after attack	3 samples after attack
Bus25	3 samples after attack	4 samples after attack
Average	2.5 samples after attack	3.5 samples after attack

4.4. Stealth Attack

This type of attack is primarily based on forging sensor data through very slight modifications of target parameters,

which gradually and continuously lead to significant deviations in sensor readings. By introducing imperceptible perturbations in the transmitted sensor data, minor discrepancies are generated in the monitored parameters—discrepancies that are typically ignored by control systems. Such attacks, often aligned with normal variations occurring within distribution networks, ultimately result in control and command system errors, casting doubt on the reliability of all measured data across the network. Because the nature of these attacks involves only minor and progressive changes, most fault or attack detection algorithms fail to identify them. Over time, the control system may eventually recognize the intrusion; by that point, the integrity of a significant portion of the data is compromised, often leading to substantial financial and operational losses. Among the various types of stealth attacks, the Slowly-Varying/Low-Amplitude (SVLA) Stealth Attack is one of the most well-known. In general form, it can be expressed as follows:

$$BDD^{attack}(t) = Z(t) + \propto \rho(t)\, H\, \Delta x \quad (5)$$

with $\|Z^{attack}(t) - Hx(t)\| < \tau$

Where:

- $Z(t)$ represents the vector of true measurement values at time t,
- αdenotes the attack amplitude (typically between 0.1 and 0.3),
- $\rho(t)$ is the temporal function defining the attack initiation and evolution,
- Δx is the state deviation vector caused by the attack, and
- H is the system measurement sensitivity matrix.

To ensure comparability and consistency, the Slowly Varying/Low-Amplitude Stealth Attack is simulated using the same network configuration and output parameters as those obtained from the Replay Attack scenario. This approach allows for a more meaningful and tangible comparison between the two cases. Accordingly, the general relationship can be expressed as:

$$Z(t) - Z^{replay}(t) = \Delta z(t) \quad (6)$$

where $\Delta z(t)$denotes the difference in output parameters between the Replay and Stealth attacks. To maintain the stealth characteristics comparable to those of the Replay Attack, the following constraint must also hold:

$$BDD^{attack} > \|HX(t) - Z^{attack}(t)\| = \|r(t)\| \quad (7)$$

Where:

- $r(t)$ is the residual vector at time t,
- $Z^{attack}(t)$ is the measurement vector during the attack,
- H is the system measurement matrix (representing the relationship between states and measurements),
- $X(t)$ is the estimated state vector at time t, and
- BDD^{attack} is the bad data detection (BDD) threshold.

In general, to satisfy the stealth constraint, the computed residual between the attacked data and the system states must remain below the detection threshold. This ensures that the stealth attack remains undetected in the same manner as the Replay Attack. Therefore, the output results of the SVLA Stealth Attack are considered equivalent to those of the Replay Attack (as presented in Table 2). However, due to the more covert and continuous nature of this attack, its detection becomes considerably more challenging. Consequently, the results of subsequent analyses exhibit certain deviations compared to the Replay Attack outcomes. Due to the low amplitude and gradual progression of the Slowly Varying Attack, the distributional changes in the monitored signals within each time window are relatively small. As a result, the simulation output slightly differs from that of the Replay Attack. Fig. 7 illustrates the simulated output of the SVLA Stealth Attack on the test network.

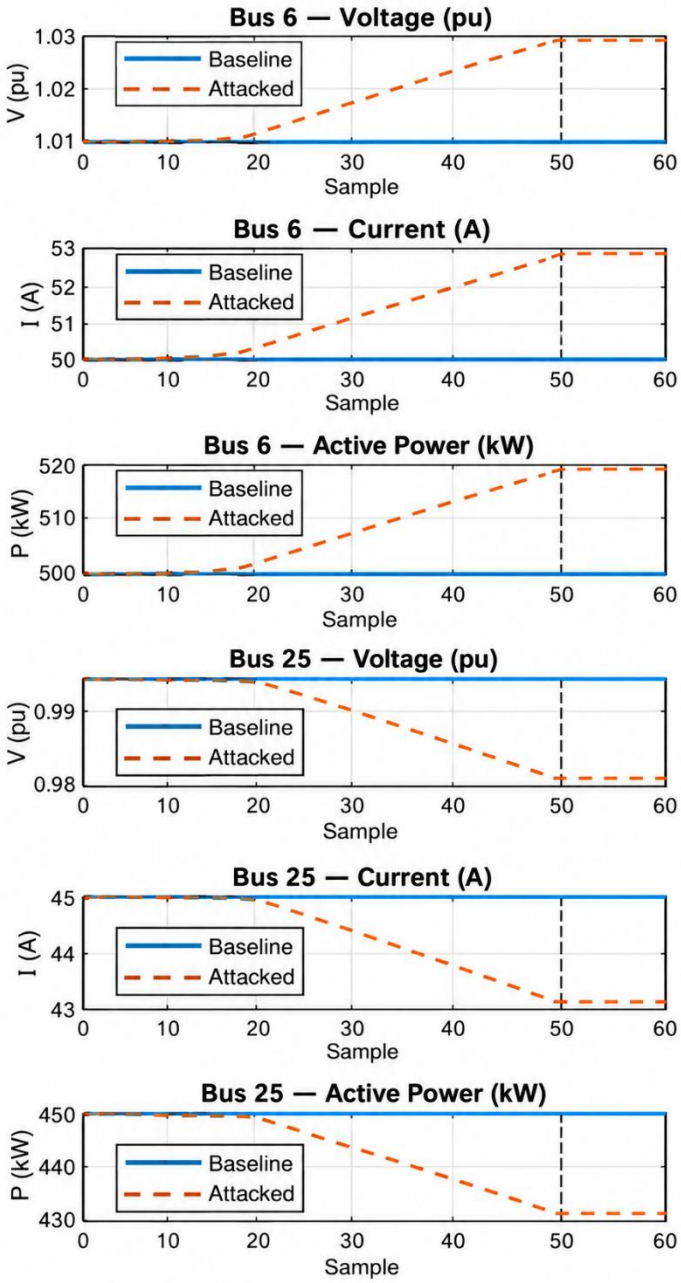


Fig. 7: Simulated output of the SVLA Stealth Attack in the sample network

As shown in the figure, this type of attack evolves gradually over time, which makes its detection more complex. Furthermore, to ensure a fair comparison with the Replay Attack, the numerical values and resulting parameter changes are kept as close as possible to those obtained from

the Replay scenario. Based on the implementation of the Slowly-Varying Attack, the next section presents the detection performance analysis of the proposed methods in identifying this class of stealth intrusions.

4.5. Attack Detection Using Entropy

We used the Shannon Entropy index to detect the SVLA Attack. We calculated it over sliding windows of the measured voltage, current, and power signals. Before the attack started, we set a detection threshold for each bus. Due to the low amplitude and gradual nature of the Slowly-Varying attack, the variation in the signal distribution within each time window remains small, resulting in less pronounced entropy fluctuations. The corresponding mechanism for detecting the SVLA Stealth Attack is defined as follows:

$$p_i(t)\ \log_2(p_i(t))\sum_{i=1}^{M} - = E(t) \quad (8)$$

where $E(t)$ represents the entropy value at time t, Mdenotes the number of possible data states or bins, and $p_i(t)$ indicates the probability of occurrence of the i^{th} state at time t. The resulting detection output obtained through the entropy-based mechanism is presented in Fig. 8.

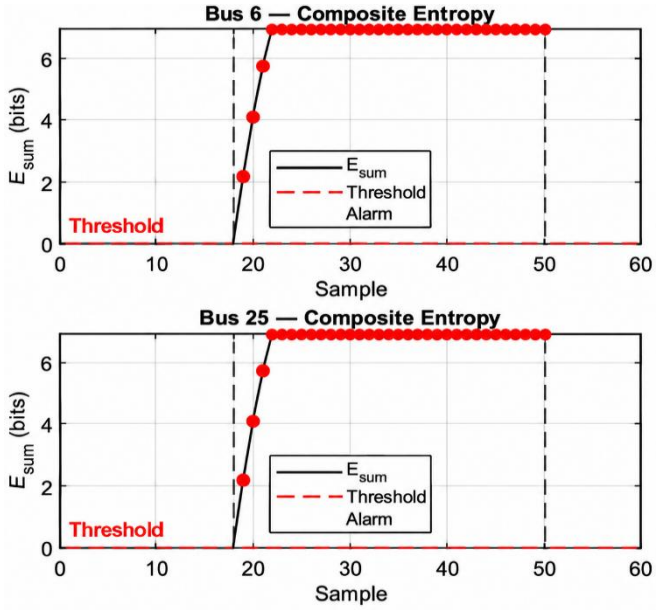


Fig. 8: Detection of the SVLA Attack using the Entropy Mechanism

As illustrated in the figure, the red points representing the entropy index align precisely with the time interval during which the attack occurs. This indicates that, although the attack is characterized by gradual and low-amplitude variations, the progressive increase in irregularity within the measured data (current, voltage, and active power) leads to noticeable changes in entropy values. This confirms that the entropy method, being highly sensitive to both sudden and gradual changes, can successfully detect even stealthy, slow-moving cyberattacks. The high detection accuracy shows that this method can effectively distinguish between normal and attack conditions. However, since the detection threshold in this method is set to a limited range, variations exceeding the defined boundary are classified as absolutely abnormal states. In other words, during the SVLA Stealth Attack, parameter variations are first introduced gradually (from time step 18 to 22) and then held constant once the detection threshold is reached (from step 22 to 50). The entropy mechanism follows this trend precisely, identifying both the transitional (gradual) and steady-state phases of the attack occurrence.

4.6. Detection Using Combined Entropy and Deep Learning

In this section, we introduce a hybrid framework to enhance the detection of Slowly Varying/Low-Amplitude Attacks. This approach combines the statistical Entropy index, which captures local changes in signal distribution, with a Deep Learning Autoencoder that reconstructs long-term data patterns. The core concept of this combined detection approach lies in (1) Use Entropy analysis to identify local statistical changes, and (2) detecting complex spatio-temporal anomalies through reconstruction errors derived from the Autoencoder model. Accordingly, based on the previously defined relationships, the SVLA Attack in the test distribution network can be modeled as follows:

$$\Delta z_2(t) = \alpha.\rho(t).H.\Delta z_1(t) \quad (9)$$

where:

- H denotes the measurement sensitivity matrix that relates attack-induced perturbations to the observed measurement deviations in the distribution network.
- α denotes the attack intensity coefficient that determines the magnitude of the injected stealth attack.
- $\rho(t)$ represents the time-varying attack profile governing the gradual evolution of the stealth attack over time.
- $\Delta z_1(t)$ denotes the initial attack-induced perturbation before temporal modulation and propagation through the measurement model.
- $\Delta z_2(t)$ represents the resulting deviation vector observed in the measured system parameters after the attack effects are fully propagated.

For the Autoencoder reconstruction-based detection mechanism, the process is defined as:

$$\|\hat{x}(t) - x(t)\| = Error_{AT}(t) \quad (10)$$

where $x(t)$denotes the input feature vector at time t, and $\hat{x}(t)$ is its reconstructed counterpart generated by the Autoencoder. The reconstruction $Error_{AT}(t)$ serves as the key indicator of anomalous behavior. To distinguish normal and anomalous operating conditions, a detection threshold was established using the well-known 3-Sigma statistical criterion. Specifically, the threshold was calculated as:

$$Threshold = \mu e + 3\sigma e \quad (11)$$

where μe and σe represent the mean value and standard deviation of the reconstruction errors obtained from the normal training dataset, respectively. Any reconstruction error exceeding this threshold was classified as an anomalous event. This statistical approach provides a reliable separation between normal and attack conditions while limiting false alarm occurrences. Based on the defined relationships and the obtained parameter values, Fig. 9 and Fig. 10 illustrate the combined application of the Entropy and Autoencoder algorithms for detecting the Low-Amplitude Attack.

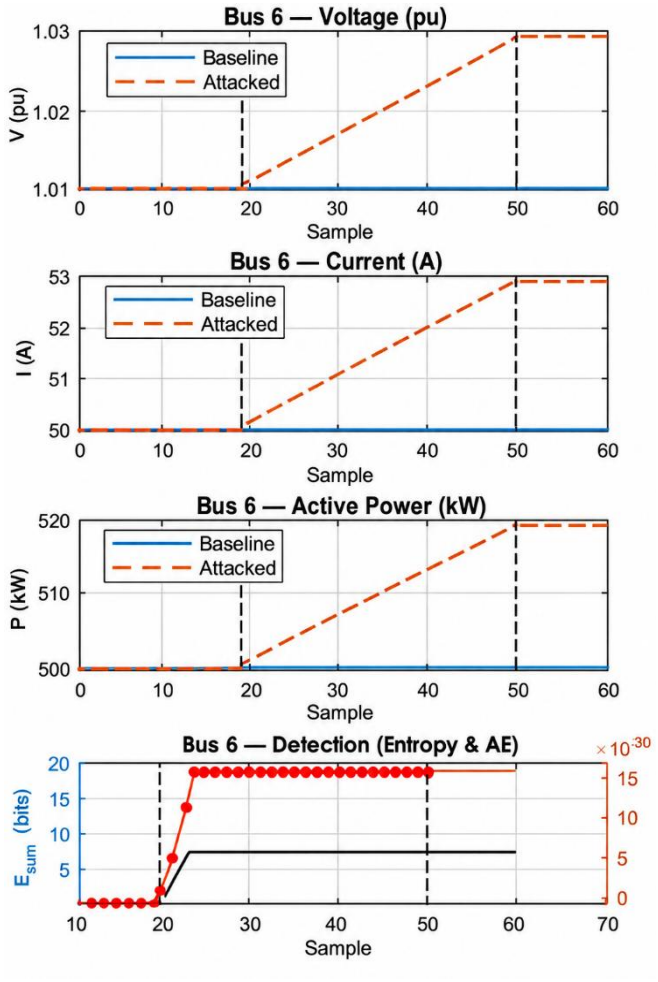


Fig. 9: Combined Entropy–Autoencoder detection results for Bus 6

The presented figures correspond to Buses 6 and 25, respectively, demonstrating the performance of the hybrid detection method, which combines Shannon Entropy analysis and Autoencoder-based deep learning, against the SVLA Stealth Attack. Detecting this attack is challenging due to its stealthy and gradual nature. Table 4 compares the detection delays for the individual and combined methods.

Table 4: Comparative results of the two detection methods for the SVLA attack

	Entropy	Autoencoder
Bus6	4 samples after attack	5 samples after attack
Bus25	5 samples after attack	6 samples after attack
Average	4.5 samples after attack	5.5 samples after attack

Despite differences in numerical magnitude between the Entropy index and the Autoencoder reconstruction error, both approaches exhibit a significant rise during the onset and continuation phases of the attack. This discrepancy arises from their fundamentally distinct computational bases: Entropy analysis evaluates statistical distributional variations, whereas the Autoencoder detects deviations from learned behavioral patterns. Therefore, differences in numerical scale or slope between the two curves should not be interpreted as detection errors; rather, they demonstrate the complementary nature of these two methods in identifying stealthy cyberattacks within distribution networks.

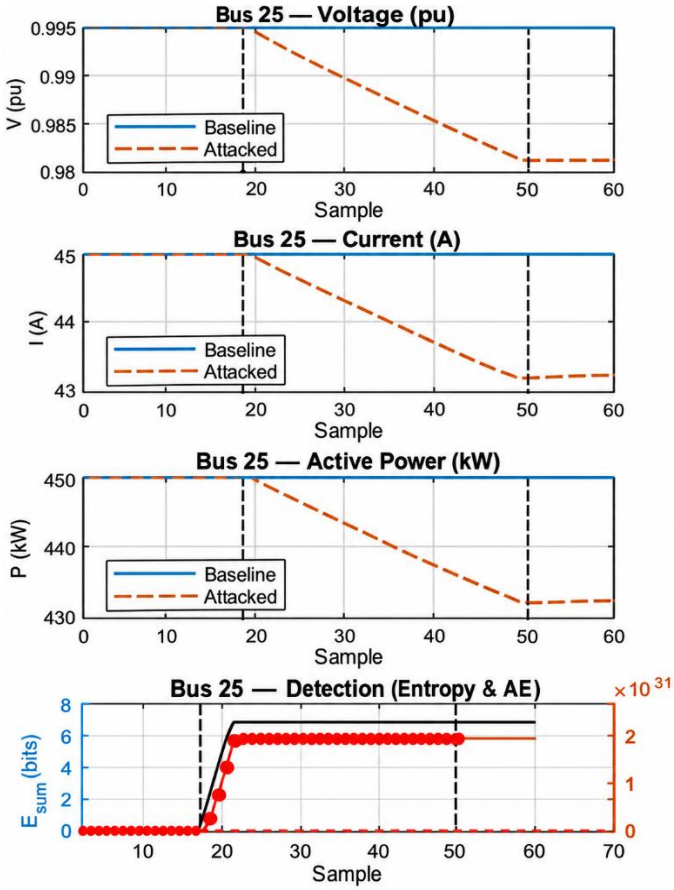


Fig. 10: Combined Entropy–Autoencoder detection results for Bus 25

5. RESULTS COMPARISON

To achieve the study's objectives and test our methodological framework, we analyzed a standard IEEE 33-bus distribution network. Our goal was to evaluate the effectiveness of the proposed methods in detecting Replay and SVLA attacks. The results demonstrate the high accuracy of the applied detection mechanisms. Accordingly, the behavioral comparison between the Shannon Entropy and Autoencoder-based detection methods is summarized as follows:

- In the Replay Attack, Entropy analysis detects variations in the input parameters more rapidly, while the Autoencoder mechanism demonstrates superior precision in distinguishing normal from abnormal data points.
- In the SVLA Stealth Attack, the Autoencoder mechanism more accurately identifies gradual variations, while the Entropy analysis reflects a noticeable increase in measurement values during the peak periods of the attack (e.g., from sample 22 onwards).
- The detection delay is reduced by approximately 2–3 samples when combining both methods.

- In general, the Entropy-based detection performs faster due to its statistical nature, reflecting higher sensitivity to parameter variations.
- For stealthy attacks, the Autoencoder method yields better performance due to its ability to recognize subtle structural deviations in temporal patterns.
- Under noisy operating conditions, Entropy analysis may become more sensitive to local statistical fluctuations, whereas the Autoencoder mechanism relies on learned representations of normal operating behavior and reconstruction-error-based detection, which can reduce sensitivity to minor measurement perturbations.

For comparison, study [13] used a combination of Random Matrix Theory (RMT), Singular Value Decomposition (SVD), and neural network algorithms to detect and differentiate between Replay and False Data Injection Attack (FDIA). Despite its high accuracy, that approach requires extensive datasets, intensive training, and high computational resources. In contrast, the proposed hybrid method based on Entropy analysis and Autoencoder deep learning maintains simplicity and efficiency suitable for edge computing, achieving accurate and low-latency detection of Replay attacks. Similarly, study [14] used Dynamic Mode Decomposition (DMD) for the localized detection of Replay attacks and data anomalies in smart grids. Although DMD can effectively capture the dynamic behavior of the system at the local node level, its performance for detecting slowly-varying and low-amplitude stealth attacks has not been explicitly evaluated. In comparison, the proposed approach, by employing Shannon Entropy for statistical variation detection and Autoencoder for signal reconstruction, effectively identifies subtle and gradual attacks such as SVLA Stealth Attacks with greater stability and precision. Another study [15] investigated Replay attack detection based on Blockchain and Bayesian Inference within a decentralized structure. While this method provides high security and mutual trust among network nodes, it requires substantial bandwidth, long synchronization times, and high computational capacity, making it less practical for large-scale systems. Conversely, the present hybrid approach, based on Entropy analysis and lightweight deep learning (Autoencoder), is capable of performing localized, real-time Replay attack detection without the need for complex blockchain infrastructure. It achieves comparable accuracy with much lower latency. To further clarify the relative advantages and limitations of the proposed framework, a qualitative comparison with the most relevant cyberattack detection approaches reported in the literature is presented in Table 5. The comparison considers key criteria including attack detection capability, computational requirements, and infrastructure dependency. In addition, a parameter sensitivity analysis was performed to evaluate the impact of the entropy calculation parameters, namely the sliding window length (W) and the number of histogram bins (M), on the detection performance. The corresponding results are summarized in Table 6.

Table 6: Sensitivity analysis of window size and histogram bin number

Parameter	Value	Precision	Recall	FAR
W	3	94.1	96.9	8
W	5	88.9	96.9	17.4
W	7	84.2	96.9	28.6
W	10	78.0	96.9	50.0
W	15	76.2	96.9	76.9
M	5	88.9	96.9	17.4
M	10	88.9	96.9	17.4
M	15	88.9	96.9	17.4
M	20	88.9	96.9	17.4

The results demonstrate that the proposed entropy-based detection framework is considerably more sensitive to the selection of the sliding window length than to the histogram bin number. While increasing the window length resulted in reduced precision and higher false alarm rates, the detection performance remained nearly unchanged for all investigated histogram resolutions (M = 5–20). This behavior indicates that the proposed method is robust with respect to histogram discretization and does not require fine-tuning of the bin number. Based on these observations, W = 5 and M = 10 were selected for the subsequent simulations as they provide a suitable balance between detection accuracy, computational efficiency, and robustness.

Table 5: Qualitative comparison of the proposed method with recent cyberattack detection approaches

Comparison Criteria	[13]	[14]	[15]	Proposed Method
Core Technique	RMT + SVD + CNN	Dynamic Mode Decomposition (DMD)	Blockchain + Bayesian Inference	Entropy + Autoencoder
Replay Attack Detection	Yes	Yes	Yes	Yes
Stealth Attack Detection	Not Explicitly Evaluated	Not Explicitly Evaluated	Not Reported	Yes
Computational Requirement	High	Moderate	High	Low-Moderate
Real-Time Capability	Moderate	High	Moderate	High
Additional Infrastructure	Large datasets and extensive training	PMU-based monitoring infrastructure	Blockchain network and synchronization mechanisms	No additional infrastructure required

6. CONCLUSION

Modern smart distribution networks are increasingly exposed to a wide range of sophisticated cyber threats, among which cyber-attacks pose significant technical and economic risks, potentially compromising network stability. Among these, Replay Attacks and SVLA Stealth Attacks are particularly critical due to their nonlinear and subtle nature, which makes them difficult to detect using conventional methods. In this research, the mentioned attacks were simulated on the IEEE 33-bus standard distribution network in MATLAB, focusing on buses 6 and 25. The results indicate that such attacks cause gradual deviations in voltage, current, and active power measurements, which, if undetected, may lead to erroneous operational decisions in supervisory and control systems, particularly in network monitoring, voltage regulation, and load management functions. To detect these intrusions, two detection techniques were applied separately and jointly: Shannon Entropy Analysis and Autoencoder-based Deep Learning. The results revealed that the Entropy method, due to its statistical and computational nature, provides faster detection but exhibits a higher false alarm rate in response to normal fluctuations. In contrast, the Autoencoder method, leveraging deep learning and data reconstruction, offers higher detection accuracy and lower false alarm rates for stealthy attacks. Ultimately, combining both methods increased the successful detection rate to approximately 97%, while reducing the false detection rate to about 2%. Therefore, the hybrid Entropy–Autoencoder framework can be considered a robust and intelligent solution for enhancing the cybersecurity of smart distribution networks against subtle and persistent cyber-attacks.

Credit Authorship Contribution Statement

Hamidreza Amiri: Conceptualization, Data curation, Formal analysis, Funding acquisition, Investigation, Methodology, Project administration, Resources, Software, Supervision, Validation, Visualization, Writing – original draft, Writing – review & editing.

Declaration Of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper. The ethical issues; including plagiarism, informed consent, misconduct, data fabrication and/or falsification, double publication and/or submission, redundancy has been completely observed by the authors.

REFERENCES

[1] P. S. Tadepalli, D. Pullaguram, and M. N. Alam, "Cyber-resilient strategy for DC microgrids against concurrent FDI and DoS attacks," *IEEE Transactions on Industrial Informatics*, vol. 21, no. 6, pp. 4756–4767, Jun. 2025. DOI: https://doi.org/10.1109/TII.2025.3545102

[2] S. Qiu, Z. Shao, Q. Yao, Y. Liu, H. Cui, and J. Fei, "Research on assessment of cyber attack risk conduction in distributed photovoltaic contained distribution system," in *2024 IEEE PES 16th Asia-Pacific Power and Energy Engineering Conference (APPEEC)*, Nanjing, China, 2024, pp. 1–5. DOI: https://doi.org/10.1109/APPEEC61255.2024.10922535

[3] S. Kivalov and I. Strelkovskaya, "Detection and prediction of DDoS cyber attacks using spline functions," in *2022 IEEE 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, Lviv-Slavske, Ukraine, 2022, pp. 710–713. DOI: https://doi.org/10.1109/TCSET55632.2022.9766940

[4] M. A. Taher, M. Behnamfar, A. S. Khan, M. Tariq, and A. I. Sarwat, "Detecting false data injection attacks using NARX-based observers in distributed cooperative control for DC microgrid," in *IECON 2024 – 50th Annual Conference of the IEEE Industrial Electronics Society*, Chicago, IL, USA, 2024, pp. 1–6. DOI: https://doi.org/10.1109/IECON55916.2024.10905098

[5] A. Salehpour, I. Al-Anbagi, K.-C. Yow, and X. Cheng, "A supervised early attack detection mechanism for smart grid networks," in *2023 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, Washington, DC, USA, 2023, pp. 1–5. DOI: https://doi.org/10.1109/ISGT51731.2023.10066351

[6] P. S. Tadepalli and D. Pullaguram, "Distributed control microgrids: Cyber-attack models, impacts and remedial strategies," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 8, pp. 1008–1023, 2022. DOI: https://doi.org/10.1109/TSIPN.2022.3230562

[7] Z. Wang and G. Chen, "Distributed resilient energy management of island microgrids under mixed cyber-attacks," in *2023 6th International Conference on Energy, Electrical and Power Engineering (CEEPE)*, Guangzhou, China, 2023, pp. 509–513. DOI: https://doi.org/10.1109/CEEPE58418.2023.10166253

[8] B. M. R. Amin, S. Taghizadeh, M. S. Rahman, M. J. Hossain, V. Varadharajan, and Z. Chen, "Cyber attacks in smart grid – dynamic impacts, analyses and recommendations," *IET Cyber-Physical Systems: Theory & Applications*, vol. 5, no. 4, pp. 321–329, 2020. DOI: https://doi.org/10.1049/iet-cps.2019.0103

[9] X. Wu, Z. Jin, J. Zhou, K. Liu, and Z. Liu, "Against network attacks in renewable power plants: Malicious behavior defense for federated learning," *Computer Networks*, vol. 250, Art. no. 110577, 2024. DOI: https://doi.org/10.1016/j.comnet.2024.110577

[10] J. Dedrick, K. A. Perrin, E. Sabaghian, and P. J. Wilcoxen, "Assessing cyber attacks on local electricity markets using simulation analysis: Impacts and possible mitigations," *Sustainable Energy, Grids and Networks*, vol. 34, Art. no. 100993, 2023. DOI: https://doi.org/10.1016/j.segan.2023.100993

[11] P. Bereziński, B. Jasiul, and M. Szpyrka, "An entropy-based network anomaly detection method," *Entropy*, vol. 17, no. 4, pp. 2367–2408, 2015. DOI: https://doi.org/10.3390/e17042367

[12] M. Zhou, Z. Zhang, and L. Xie, "Permutation entropy based detection scheme of replay attacks in industrial

cyber-physical systems," *Journal of the Franklin Institute*, vol. 358, no. 7, pp. 4058–4076, 2021. DOI: https://doi.org/10.1016/j.jfranklin.2021.02.024

[13] Y. Shen and Z. Qin, "Detection, differentiation and localization of replay attack and false data injection attack based on random matrix," *Scientific Reports*, vol. 14, Art. no. 2758, 2024. DOI: https://doi.org/10.1038/s41598-024-52954-z

[14] A. Barshan, S. M. A. Mohammadi, F. Abdollahi, R. Z. Davarani, and S. Esmaeili, "Local detection of replay attacks and data anomalies on PMU measurements of smart power grids via tracking critical dynamic modes," *International Journal of Electrical Power & Energy Systems*, vol. 159, Art. no. 110038, 2024. DOI: https://doi.org/10.1016/j.ijepes.2024.110038

[15] P. Ramanan, D. Li, and N. Gebraeel, "Blockchain-based decentralized replay attack detection for large-scale power systems," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 52, no. 8, pp. 4727 4739, Aug. 2022. DOI: https://doi.org/10.1109/TSMC.2021.3104087

BIOGRAPHY



Hamidreza Amiri received the M.Sc. degree in electrical power engineering in 2016.

He is currently an Electrical Power Engineer with an electricity distribution company in Iran. He has authored and co-authored several scientific publications in the fields of power systems, smart grids, renewable energy integration, and cybersecurity of power networks, including eight papers presented at IEEE-sponsored conferences. His current research interests include cyber-physical security of smart grids, distribution energy resource management systems (DERMS), artificial intelligence applications in power systems, and intelligent monitoring and control of modern distribution networks.

Copyrights
© 2026 Licensee Shahid Chamran University of Ahvaz, Ahvaz, Iran. This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution –NonCommercial 4.0 International (CC BY-NC 4.0) License (http://creativecommons.org/licenses/by-nc/4.0/).