Electrical Power and Energy Systems 175 (2026) 111649

Contents lists available at ScienceDirect

International Journal of Electrical Power and Energy Systems

journal homepage: www.elsevier.com/locate/ijepes

Semantic communication-based detection of False Data Injection Attacks in 6G-enabled smart grids

Zainab Alwaisi [a],*, Simone Soderi [b]

[a] IIT-CNR, Pisa, Italy
[b] Scuola IMT Alti Studi Lucca, Lucca, Italy

ARTICLE INFO

Keywords:
IoT
6G security
Data sustainability
Smart grid
Wireless communication
Data integrity

ABSTRACT

The increasing integration of advanced communication technologies in smart grids, particularly in the context of emerging 6G networks, exposes power systems to sophisticated cyber–physical threats such as False Data Injection Attacks (FDIAs). These attacks can bypass conventional detection mechanisms by introducing subtle yet contextually inconsistent data manipulations. Most existing FDIA detection approaches rely on statistical residual analysis or purely data-driven learning models, which often fail to exploit domain knowledge inherent to power system operations.

This paper proposes a semantic communication-based framework for FDIA detection in 6G-enabled smart grids. The proposed approach integrates ontology-driven semantic encoding with Long Short-Term Memory (LSTM) networks to jointly capture contextual semantics and temporal dependencies in smart meter data. By embedding power system domain knowledge into the communication and detection pipeline, the framework enables the identification of semantically inconsistent measurements that may appear statistically plausible. To validate the proposed method, a custom smart meter prototype was developed to generate a large-scale dataset consisting of both normal and FDIA-compromised power consumption profiles. Extensive experimental results demonstrate that the proposed framework achieves high detection accuracy and low inference latency, while maintaining robustness under noisy communication conditions. Comparative evaluations against representative deep learning-based baselines show consistent improvements in detection performance and reliability. These results indicate that the proposed semantic-aware detection framework is well-suited for real-time monitoring and cybersecurity enhancement of future 6G-enabled smart grid systems.

1. Introduction

The transition toward sixth-generation (6G) wireless networks is poised to deliver unprecedented performance in terms of ultra-high data rates, ultra-low latency, and ubiquitous connectivity [1,2]. Anticipated for commercial deployment in the 2030s, 6G systems are expected to achieve data rates exceeding one terabit per second (Tbps) and latencies as low as 10–100 microseconds [1,2]. These capabilities will enable a broad spectrum of mission-critical applications spanning terrestrial, aerial, maritime, and space-based domains [3,4].

Despite these technological advances, 6G networks pose substantial cybersecurity challenges, particularly in critical infrastructure such as smart grids. As the number of interconnected devices grows from wearable health monitors to industrial cyber–physical systems, the associated attack surface expands proportionally. Ensuring the confidentiality, integrity, and availability of smart grid data under such conditions is essential to maintaining operational resilience [5]. This study investigates the role of semantic communication. This paradigm prioritizes the meaning and contextual relevance of transmitted information over raw bit-level fidelity in enhancing the cybersecurity posture of 6G-enabled smart grids. Unlike traditional communication models that focus solely on accurate data reconstruction, semantic communication enables systems to infer and verify intent. This enables more effective anomaly detection against sophisticated threats such as False Data Injection Attacks (FDIAs) [6].

The need for advanced security mechanisms is further amplified by emerging vulnerabilities in machine learning (ML) and cryptographic systems. Recent research has demonstrated the susceptibility of ML models to data poisoning attacks, particularly in high-stakes applications like healthcare [7]. Concurrently, cryptographic implementations, such as the Advanced Encryption Standard (AES), remain vulnerable to side-channel and fault injection exploits [8]. The advent of quantum computing further compounds these risks, necessitating the adoption of

* Corresponding author.
E-mail addresses: zainabalwaise@yahoo.com, zainab.alwaisi@iit.cnr.it (Z. Alwaisi), simone.soderi@imtlucca.it (S. Soderi).

https://doi.org/10.1016/j.ijepes.2026.111649
Received 21 July 2025; Received in revised form 23 January 2026; Accepted 28 January 2026
Available online 30 January 2026

post-quantum cryptographic methods, such as isogeny-based schemes, to safeguard future communication systems, including those within the Internet of Things (IoT) and 6G infrastructures [9]. Moreover, Recent advances in data-driven FDIA detection frameworks, such as the method proposed in [10], demonstrate promising capabilities by leveraging subspace identification and adaptive residual generation to detect and localize attacks in DC microgrids. While such approaches effectively exploit process input–output data, they remain limited by their reliance on purely statistical correlations, which can lead to high false-positive rates under dynamic, heterogeneous grid conditions. In contrast, our work introduces a semantic communication-based approach that augments temporal modeling with ontology-informed contextual encoding. This integration allows the system to detect anomalous deviations and interpret their semantic inconsistency with expected grid behavior, thus reducing false alarms and enhancing robustness to evolving attack strategies. Accordingly, our contribution addresses a critical gap by bridging data-driven learning with semantic reasoning, ensuring more reliable and generalizable FDIA detection in 6G-enabled smart grids. Recent advances in data-driven FDIA detection frameworks, such as the method proposed in [10], demonstrate promising capabilities by leveraging subspace identification and adaptive residual generation to detect and localize attacks in DC microgrids. While such approaches effectively exploit process input–output data, they remain limited by their reliance on purely statistical correlations, which can lead to high false-positive rates under dynamic, heterogeneous grid conditions. In contrast, our work introduces a semantic communication–based approach that augments temporal modeling with ontology-informed contextual encoding. This integration allows the system to detect anomalous deviations and interpret their semantic inconsistency with expected grid behavior, thus reducing false alarms and enhancing robustness to evolving attack strategies. Accordingly, our contribution addresses a critical gap by bridging data-driven learning with semantic reasoning, ensuring more reliable and generalizable FDIA detection in 6G-enabled smart grids.

While this work targets FDIA detection in smart grids, the proposed semantic communication framework presents a generalizable foundation for addressing a broader class of cyber–physical threats. This adaptability underscores the potential for extending the approach to multi-threat environments in future research.

1.1. Motivation

The motivation for this study arises from the pressing need to secure smart grid infrastructures against increasingly sophisticated cyber threats, particularly in the context of emerging 6G communication capabilities. Converting ultra-low-latency, high-throughput wireless communication into distributed metering systems presents significant opportunities to enhance grid performance and introduces new cyberattack vectors.

Among these threats, FDIAs pose a particularly insidious challenge by targeting the integrity of state estimation processes, potentially destabilizing grid operations. Traditional detection methods, typically based on static statistical thresholds or supervised learning models, cannot often incorporate semantic context or adapt to dynamic grid conditions. As a result, they struggle to generalize across heterogeneous data sources and evolving threat landscapes.

Semantic communication offers a novel and underexplored solution to this problem. Semantic communication enhances the system's ability to infer intent and detect anomalies in a more interpretable and adaptive manner by embedding contextual meaning into transmitted data. This study aims to leverage these capabilities by introducing a semantic-aware detection framework that enhances resilience to FDIA in next-generation, 6G-enabled smart grids. In this paper, we define *data sustainability* as the ability of an intelligent grid system to ensure continuous, reliable, and resource-efficient data availability, transmission, and processing in the face of evolving cyber threats and constrained environments. This concept emphasizes both the robustness of data integrity and the efficiency of data handling in 6G-enabled infrastructures.

1.2. Our contributions

This paper introduces a comprehensive framework for FDIA detection in smart grid environments, grounded in semantic communication principles and deep learning. By formalizing an ontology-driven representation of smart meter data and integrating it with temporal modeling via Long Short-Term Memory (LSTM) networks, we present a robust, context-aware approach to anomaly detection. The key contributions are summarized as follows:

1. **Semantic-Aware Anomaly Detection Framework**: We design a real-time monitoring system incorporating semantic context into the anomaly detection pipeline, improving differentiation between legitimate and manipulated smart meter data.
2. **Custom Smart Meter Prototype and Dataset**: We develop a hardware-based prototype using non-invasive current sensors to generate a realistic dataset comprising 200,000 labeled power consumption samples, including benign and FDIA-manipulated scenarios.
3. **LSTM-Based Detection with Ontology-Guided Encoding**: We adapt an ontology-driven semantic encoding layer and integrate it with an LSTM classifier to capture temporal and contextual dependencies in smart meter readings.
4. **Proactive Containment Mechanism**: The proposed system includes a localized mitigation capability that identifies and isolates compromised grid components in real time, thereby limiting the propagation of malicious data across the network.

Collectively, these contributions present a semantically enriched, practically deployable solution for enhancing the cyber–physical resilience of smart grid infrastructures operating within the 6G ecosystem.

1.3. Organization of the paper

The remainder of this paper is organized as follows. Section 2 presents the background on smart grids, 6G communication, and semantic communication concepts. Section 3 reviews related work on FDIA detection and semantic-aware security approaches. Section 4 introduces the threat and attack models. Section 5 details the proposed semantic communication-based FDIA detection framework. Section 6 presents the experimental results, followed by a discussion in Section 7. Finally, Section 8 concludes the paper and outlines future research directions.

2. Background

2.1. Smart energy grids: Architecture and security challenges

Modern smart energy grids leverage technologies such as the IoT, embedded sensors, and advanced communication protocols to improve energy efficiency, reliability, and responsiveness [11,12]. These grids depend on real-time monitoring of parameters like power consumption, equipment status, and environmental conditions to support adaptive and decentralized control mechanisms.

The continuous exchange of operational data introduces significant security challenges. Data integrity, confidentiality, and availability are critical, as unauthorized access or tampering can disrupt grid stability or compromise safety. In particular, cyberattacks such as FDIA can mislead system state estimation, leading to incorrect decisions and potential cascading failures [13].

Integrating renewable energy sources, such as solar and wind, further compounds the need for accurate and secure data management. These sources introduce variability and intermittency, requiring secure forecasting and control to maintain balance and grid reliability [14]. As the number of connected devices and subsystems grows, so does the attack surface, emphasizing the need for robust, context-aware security mechanisms tailored to smart grid environments.

2.2. 6G wireless networks and communication paradigms

Sixth-generation (6G) wireless communication systems are envisioned to offer ultra-fast data rates (1 Tbps and beyond), ultra-low latency (down to 0.1 ms), and high device density (up to 10 million connections per km^2) [15–17]. These capabilities will support various time-sensitive applications, including autonomous control, immersive XR, and real-time energy grid management.

Despite these advancements, several challenges remain, most notably spectrum allocation, infrastructure scalability, and cybersecurity. Additionally, sustainability is a core design consideration in 6G. This includes energy-efficient protocol design, responsible resource allocation, and minimizing the environmental impact of high-throughput communication systems [18]. However, sustainability in this context primarily refers to *energy efficiency* and *data longevity*, not generalized environmental or ethical concerns, clarifying a term that is sometimes used too broadly.

The foundational goals of 6G systems can be summarized as:

1. **Velocity Maximization**: Supporting ultra-high-speed data transmission.
2. **Low Latency**: Enabling near-instantaneous communication for mission-critical tasks.
3. **Massive Connectivity**: Connecting billions of heterogeneous devices efficiently.
4. **AI-Driven Autonomy**: Incorporating ML for decentralized, adaptive control.
5. **Energy and Resource Efficiency**: Optimizing protocols and hardware for reduced energy consumption.
6. **Advanced Material and System Design**: Employing novel antenna, channel coding, and quantum-resistant cryptographic techniques.

2.3. 6G applications in smart grid management

The deployment of 6G technologies has significant implications for energy infrastructure. High bandwidth and low latency allow continuous, high-resolution energy usage monitoring, anomaly detection, load balancing, and grid-wide synchronization. This enables real-time, distributed energy management and faster response to disruptions.

For example, conventional 4G systems offer latency around 50 ms with 1 Gbps throughput, while 5G improves latency to 1 ms and boosts throughput to 10 Gbps. 6G is expected to reduce latency to 0.1 ms and increase throughput to 100+ Gbps, making real-time protection and control loops feasible even at grid scale [17].

Furthermore, dense IoT integration will enable fine-grained measurements and distributed optimization. These capabilities are beneficial for managing volatile energy sources and detecting tampering or failures in sensor networks.

2.4. Defining data sustainability in cyber–physical systems

Data sustainability in smart grid and 6G contexts refers to long-term, secure, and efficient data management practices that support resilience, performance, and compliance [19]. Key aspects include:

- **Security and Integrity**: Ensuring data is protected from tampering and unauthorized access.
- **Efficient Lifecycle Management**: Minimizing data redundancy and storage energy costs.
- **Interoperability and Accessibility**: Maintaining data utility across evolving platforms and devices.
- **Privacy Preservation**: Enabling lawful and ethical user and device-level information use.

While sometimes conflated with environmental sustainability, in this context it primarily concerns digital and operational resilience, system longevity, and the ability to adapt to changing threat or usage conditions [20,21].

2.5. Semantic communication for context-aware security

Traditional communication systems, based on the Shannon model, focus on the accurate transmission of bits between sender and receiver, without regard to the meaning of the data. This limits the effectiveness of anomaly detection in systems like smart grids, where malicious data can appear statistically normal but semantically inconsistent [22,23].

Semantic communication, by contrast, emphasizes the transmission of meaning rather than raw data. It leverages shared ontologies and models between communicating parties to represent, compress, and interpret information based on relevance and context [24]. This enables systems to detect subtle, context-aware threats, such as FDIA, by analyzing deviations in intent or behavior rather than surface-level metrics.

In smart grids, this approach enables semantic-aware anomaly detection. For instance, a smart meter reading that aligns with historical consumption patterns numerically may still be flagged as anomalous if it deviates from expected semantic behaviors (e.g., usage context, time-of-day patterns, or spatial correlations).

6G technologies enhance this capability by providing the low latency and compute offloading required for real-time semantic processing. Edge devices such as smart meters can encode data using lightweight ontologies and transmit only meaningful changes, reducing communication overhead and accelerating anomaly response.

Despite its potential, semantic communication faces technical challenges, including:

- Developing standardized ontologies and semantic similarity functions.
- Balancing communication cost with semantic richness.
- Ensuring trust and authenticity of semantic encodings in adversarial environments.

Nevertheless, semantic communication provides a promising direction for next-generation, context-aware cybersecurity, particularly when integrated with ML-based detection in 6G-powered smart infrastructures.

3. Related work

Anomaly detection, in essence, refers to identifying data instances that deviate significantly from expected patterns. In recent years, deep learning has emerged as a dominant approach in this domain, particularly through techniques that learn feature representations or anomaly scores directly from data [25]. Among the various neural architectures, autoencoders (AEs) have been extensively employed in supervised and unsupervised FDIA detection frameworks. Conventional AEs are primarily designed for data compression or dimensionality reduction, where the encoder maps input data into a lower-dimensional latent space, and the decoder reconstructs the original input from this representation. Discrepancies between the input and reconstructed output are then used to identify anomalous behavior.

In the context of time series analysis, unsupervised anomaly detection methods typically fall into three categories: reconstruction-based, dissimilarity-based, and histogram-based approaches [26]. Reconstruction-based techniques, including those built on AEs and LSTMs [27], model the temporal dynamics of time series data to generate expected values and detect anomalies through reconstruction errors. Dissimilarity-based methods focus on computing distances or similarities between data segments or features, while histogramming techniques identify outliers by analyzing the statistical properties of the time series distribution. Our work aligns most closely with the reconstruction-based paradigm, utilizing a semantically enriched LSTM architecture for FDIA detection.

Several studies have specifically investigated the impact of FDIAs on state estimation in smart grids. For instance, Liang et al. [28]

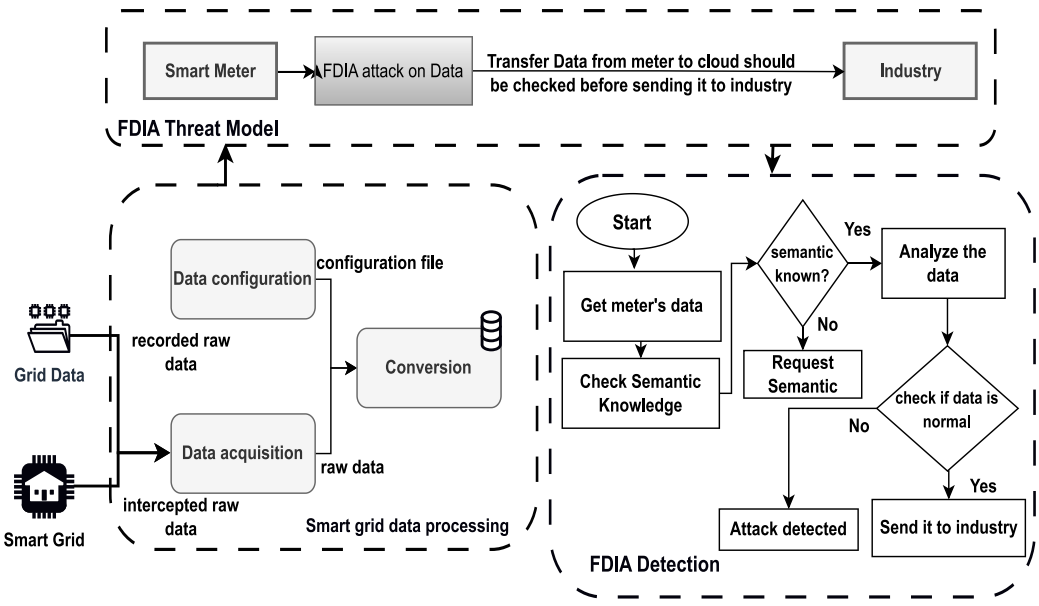


Fig. 1. Attack scenario and detection mechanism.

examined how load shift constraints influence an attacker's ability to overload transmission branches, exposing vulnerabilities in power system operations. Despite various advancements, most existing detection schemes cannot incorporate semantic context, limiting their adaptability to evolving attack strategies.

Recent research has explored the potential of semantic communication to address security challenges in IoT systems. Du et al. [29] examined the intersection of semantic IoT (SIoT) and cybersecurity, comparing traditional approaches, such as Physical Layer Security (PLS), encryption, and covert communication with emerging semantic paradigms. The study introduced new performance metrics and identified the unique challenges posed by semantic-layer attacks, highlighting the potential of semantic communication to transform security mechanisms in next-generation networks.

Complementary work by Xie et al. [30] proposed L-DeepSC, a lightweight, distributed semantic communication framework tailored for resource-constrained IoT devices. L-DeepSC integrates deep learning-driven semantic modeling at the cloud/edge level, enabling efficient semantic data transmission from devices. It employs model compression techniques such as pruning and quantization to reduce computation and communication overheads. It demonstrates superior performance under low Signal-to-Noise Ratio (SNR) conditions and fading channels through channel state information (CSI)-assisted training.

In parallel, post-quantum cryptography (PQC) research has gained momentum due to the looming threat posed by quantum adversaries. The Kyber lattice-based encryption scheme has been optimized for efficient execution on ARM64 processors using hardware-accelerated functions such as the Number Theoretic Transform (NTT) and AES acceleration [31]. These optimizations significantly enhance key generation, encapsulation, and decapsulation, offering viable cryptographic protection for smart grid applications.

However, PQC implementations remain vulnerable to side-channel attacks (SCAs). Recent surveys [32,33] have documented how various PQC algorithms are susceptible to fault injection and power analysis, emphasizing the necessity for secure hardware architectures and robust countermeasures. These findings underscore the broader security challenges facing quantum-resilient infrastructure.

Additionally, hardware-accelerated cryptographic primitives, such as the supersingular isogeny Diffie–Hellman key exchange protocol implemented on FPGAs, have demonstrated promising results in delivering secure and scalable solutions for IoT environments [34]. Such cryptographic advancements are crucial for protecting sensitive data in distributed and latency-sensitive systems, including smart grids.

Despite these advances, existing FDIA detection methods largely rely on statistical or purely data-driven models and lack semantic awareness, motivating the need for context-aware detection frameworks.

4. Propagation and attack models

By reviewing the limitations of existing FDIA detection approaches, this section introduces the threat and system models that underpin the proposed semantic communication–based detection framework. Understanding how manipulated data spreads through the grid is essential for designing robust detection and containment mechanisms. Fig. 1 illustrates the data collection environment, while Fig. 2 visualizes the impact of FDIA on power readings.

4.1. Smart grid state model

We consider a time-discrete model of a smart grid composed of N smart meters. At each discrete time slot t, a smart meter can exist in one of three states:

- **Normal** ($x_{i,t} = 0$): The meter is operating without evidence of tampering.
- **Suspected**: The meter shows anomalous behavior but is not yet confirmed to be compromised. This state enables continuous monitoring by flagging meters for enhanced semantic and temporal analysis across successive reporting intervals before escalation to confirmed attack status.
- **Infected** ($x_{i,t} = 1$): The meter's data stream is actively manipulated via FDIA.

For formal analysis, we define the binary infection state as:

$$X_t = (x_{1,t}, x_{2,t}, \ldots, x_{N,t}), \tag{1}$$

where $x_{i,t} \in \{0, 1\}$ indicates the infection status of meter i at time t.

Let $S_{i,t}$ and $I_{i,t}$ denote the probabilities of meter i being in the normal and infected states at time t, satisfying:

$$S_{i,t} + I_{i,t} = 1. \tag{2}$$

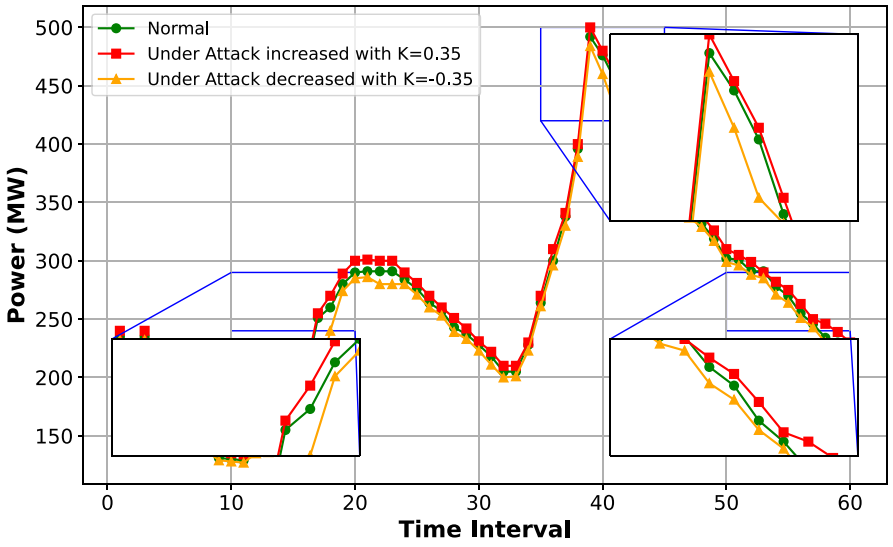


Fig. 2. Detailed analysis of FDIA on power consumption: Comparison between normal and attacked states over time.

The infection state of the full system is then modeled as:

$$C_t = (I_{1,t}, I_{2,t}, \ldots, I_{N,t}). \tag{3}$$

This stochastic model allows us to evaluate how infections propagate and how anomalies accumulate over time in the network.

4.2. False data injection attack model at the smart meter layer

We assume an attacker can manipulate the data stream of a compromised smart meter by introducing additive perturbations based on previous measurements. Specifically, the attacker modifies the reading of meter i at time t by applying a scaling factor $k_{i,t}$ to its value from the previous time slot. The manipulated reading $M_{i,t}$ is computed as:

$$M_{i,t} = O_{i,t} + k_{i,t} \cdot O_{i,t-1}, \tag{4}$$

where $O_{i,t}$ is the original (uncompromised) reading of meter i at time t, $k_{i,t} \in \mathbb{R}$ is the FDIA scaling parameter controlling the magnitude and direction of the attack, and $M_{i,t}$ is the resulting compromised reading.

This formulation captures temporal dependencies and allows both subtle and aggressive manipulations:

- $k_{i,t} > 0$ simulates over-reporting (e.g., energy theft for profit),
- $k_{i,t} < 0$ simulates under-reporting (e.g., bypassing consumption),
- $k_{i,t} = 0$ denotes no attack at that time step.

Such manipulations can mislead billing systems, disrupt demand forecasting, or destabilize grid operations if undetected. The attacker is assumed to have limited access, compromising a subset of meters and remaining covert to avoid immediate detection. It is important to note that this attack model represents FDIA at the smart metering layer under partial attacker knowledge, rather than a fully topology-consistent state-estimation attack.

4.3. Illustration of FDIA impact on power consumption data

Fig. 2 visualizes power consumption over time under normal and attack conditions. Three lines are shown: – **Normal usage**: unaltered meter data, – **FDIA-increase**: data inflated by $k = 0.35$, – **FDIA-decrease**: data deflated by $k = -0.35$.

The plot highlights two notable peaks around time intervals 20 and 40. To better demonstrate the anomaly characteristics, three zoomed inset regions illustrate:

- Interval 10–20: first peak distortion,
- Interval 35–45: second peak manipulation,
- Interval 50–60: decay slope deviation.

These visualizations demonstrate that even modest perturbations via FDIA can significantly alter aggregate consumption patterns, potentially misleading grid operators or billing algorithms.

By modeling FDIA propagation and its effects on time-series data, we lay the foundation for detection mechanisms that leverage temporal and semantic patterns to identify malicious behavior.

5. System model

A modern power grid consists of interconnected busbars linked through transmission lines. These nodes are continuously monitored using smart meters that report various electrical quantities. The measurement vector is denoted by $\mathbf{z} = \{z_1, z_2, \ldots, z_M\}$, where M is the number of independent measurements. These may include parameters such as active power injection and power flow. The state vector $\mathbf{x} = \{x_1, x_2, \ldots, x_N\}$ describes the internal operating conditions of the system, such as voltage phase angles at N buses.

The objective of the state estimation process is to reconstruct $\mathbf{x}$ from $\mathbf{z}$ in near real-time using data from the Supervisory Control and Data Acquisition (SCADA) system. The DC linear state estimation model is a widely used formulation due to its computational tractability. The relationship between measurements and system states is expressed as: The system state estimation process can be modeled as:

$$\mathbf{z} = H\mathbf{x} + \mathbf{e}, \tag{5}$$

where $H \in \mathbb{R}^{M \times N}$ is the Jacobian matrix reflecting the grid's topology, $\mathbf{x} \in \mathbb{R}^N$ is the system state vector, and $\mathbf{e} \in \mathbb{R}^M$ is the additive noise vector, commonly modeled as zero-mean Gaussian noise.

FDIA exploit this model by manipulating $\mathbf{z}$ to skew the estimated system state without triggering traditional Bad Data Detection (BDD) mechanisms. Specifically, an attacker can craft an injected vector:

$$\mathbf{a} = H\mathbf{c}, \tag{6}$$

where $\mathbf{c} \in \mathbb{R}^N$ is the carefully designed perturbation to the system state. The resulting compromised measurement becomes:

$$\mathbf{z}' = \mathbf{z} + \mathbf{a} = H(\mathbf{x} + \mathbf{c}) + \mathbf{e}, \tag{7}$$

leading the estimator to interpret the altered state,

$$\mathbf{x}' = \mathbf{x} + \mathbf{c} \tag{8}$$

as valid. This formulation explicitly shows how an attacker can introduce stealthy manipulations that remain undetected by conventional BDD techniques.

This manipulation can lead to inappropriate control actions, grid instability, or cascading failures. The simplicity of the DC model, while beneficial for system efficiency, also makes it vulnerable to attacks that align with its structure. Despite the increasing adoption of machine learning-based intrusion detection systems, FDIAs remain challenging due to their ability to conform to the physical model and avoid detection.

In this context, our proposed framework augments conventional detection by embedding semantic understanding into the data layer, capturing structure and intent. The following subsections describe how semantic communication, contextual modeling, and threshold-based anomaly detection are combined to detect FDIAs effectively, even when they closely mimic valid measurement patterns.

Moreover, Eqs. (6) and (8) describe the classical topology-aware stealthy FDIA ($a = Hc$) that can bypass residual-based BDD under full system knowledge. In the experimental evaluation of this study, FDIA is realized at the smart metering layer under partial attacker knowledge by injecting controlled offsets and scaling factors into the reported meter measurements, as described later in Section 5.4.

5.1. Semantic communication for FDIA detection

In 6G-enabled smart grids, devices' increasing complexity and heterogeneity demand security mechanisms that go beyond conventional data analysis. Semantic communication (SC) introduces a new layer of context-aware interpretation, where the meaning of transmitted data is preserved and leveraged to improve anomaly detection accuracy.

In the context of FDIA targeting smart meters, SC enables the system to classify observations based on how closely they align with predefined semantic models. Unlike traditional syntactic approaches that focus solely on raw numerical values, SC captures the data's structure and context. This leads to more resilient, robust detection mechanisms against obfuscation, spoofing, or adversarial manipulation.

Let $\mathcal{D}_{\text{meter}}$ denote an incoming smart meter data instance, represented as a semantically encoded feature vector. Two reference models are maintained:

- $\mathcal{M}_{\text{normal}}$: a centroid vector representing typical, benign meter behavior;
- $\mathcal{M}_{\text{infected}}$: a centroid vector derived from known FDIA patterns.

To evaluate the alignment of the observed data with each reference model, a semantic similarity function $\text{Sim}(\cdot,\cdot)$ is used. In our implementation, we employ cosine similarity:

$$\text{Sim}(\vec{a},\vec{b}) = \frac{\vec{a}\cdot\vec{b}}{\|\vec{a}\|\|\vec{b}\|}, \tag{9}$$

where $\vec{a}\cdot\vec{b}$ denotes the dot product of the vectors and $\|\vec{a}\|$ is the Euclidean norm of vector $\vec{a}$.

Additionally, cosine similarity was selected because the semantic vectors produced by the ontology-driven encoding primarily represent directional relationships in a high-dimensional semantic space, rather than absolute magnitudes. In this context, the objective is to measure semantic alignment between observed data and reference behavior models, making angular similarity more appropriate than distance-based metrics that are sensitive to scale variations. Moreover, Distance-based measures such as Euclidean or Mahalanobis distance were not adopted, as they are more sensitive to scale, variance estimation, and noise, which can obscure semantic inconsistencies when consumption magnitudes naturally fluctuate.

Using these similarity scores, the classification of the incoming data instance is determined as:

$$\mathcal{D}_{\text{classified}} = \begin{cases} \text{Normal}, & \text{if } \text{Sim}(\mathcal{D}_{\text{meter}}, \mathcal{M}_{\text{normal}}) > \tau_{\text{N}}, \\ \text{Compromised}, & \text{if } \text{Sim}(\mathcal{D}_{\text{meter}}, \mathcal{M}_{\text{infected}}) > \tau_{\text{I}}, \\ \text{Suspected}, & \text{otherwise}, \end{cases} \tag{10}$$

where τ_{N} and τ_{I} are empirically tuned thresholds. This formulation allows the system to classify smart meter readings into normal, compromised, or suspected categories based on semantic alignment with known reference behaviors. The threshold values τ_N and τ_I are determined empirically using labeled data collected under controlled operating conditions. Specifically, normal behavior data is collected during attack-free operation, ensuring that all samples correspond to legitimate system behavior. The distribution of semantic similarity scores obtained from this data is used to define the normal threshold τ_N, as illustrated in Fig. 2. Similarly, FDIA-infected samples are generated through controlled attack injection, and the resulting semantic similarity score distribution is used to determine the abnormal threshold τ_I. Samples with similarity values greater than τ_N are classified as *Normal*, samples with values lower than τ_I are classified as *Infected*, and samples with intermediate values are classified as *Suspected*. This intermediate region captures uncertainty and enables continuous monitoring and progressive risk assessment rather than immediate binary decisions.

Formal definition of semantic awareness and contextual anomaly detection

We define a system as *semantic-aware* if it operates over a semantic space $\mathbb{S}$ structured by an ontology $\mathcal{O}$, which models domain knowledge as a set of concept relationships and contextual features. The semantic encoding function $\mathcal{E}_{\mathcal{O}}$ maps raw meter data $\mathcal{D}_{\text{meter}}$ into this space:

$$\mathcal{E}_{\mathcal{O}} : \mathcal{D}_{\text{meter}} \to \vec{v}_{\text{semantic}} \in \mathbb{S} \subseteq \mathbb{R}^d \tag{11}$$

Contextual anomaly detection is the task of detecting semantic deviations from expected behavior. Given a similarity function Sim and a normality model $\mathcal{M}_{\text{normal}}$, the semantic deviation score $\Delta_{\mathcal{O}}$ is defined as:

$$\Delta_{\mathcal{O}}(\vec{v}) = 1 - \text{Sim}(\vec{v}, \mathcal{M}_{\text{normal}}) \tag{12}$$

A reading is flagged as anomalous if $\Delta_{\mathcal{O}}(\vec{v}) > \Theta$, where Θ is a context-sensitive anomaly threshold derived empirically. Optional logical inference rules can be applied over $\mathcal{O}$ (e.g., if usage > expected **AND** time = off-peak, then label as *suspected anomaly*).

Ontology-based semantic encoding:. Each data instance $\mathcal{D}_{\text{meter}}$ is transformed into a semantic vector using a shared ontology $\mathcal{O}$, which encodes domain knowledge across multiple layers, including device type, location, time context (peak/off-peak), and historical consumption trends.

(1) Data Representation:

$$\mathcal{E}_{\mathcal{O}}(\mathcal{D}_{\text{meter}}) \to \vec{v}_{\text{semantic}} \in \mathbb{R}^d \tag{13}$$

(2) Semantic Interpretation: The utility operator decodes the transmitted vector using the same ontology:

$$\mathcal{I}_{\mathcal{O}}(\vec{v}_{\text{semantic}}) = \mathcal{D}'_{\text{utility}} \tag{14}$$

(3) Control Commands: Control instructions generated by the utility are encoded similarly:

$$\mathcal{E}_{\mathcal{O}}(\mathcal{C}_{\text{utility}}) \tag{15}$$

(4) Semantic Understanding at the Meter: The command is decoded by the smart meter:

$$\mathcal{C}'_{\text{meter}} = \mathcal{I}_{\mathcal{O}}(\mathcal{E}_{\mathcal{O}}(\mathcal{C}_{\text{utility}})) \tag{16}$$

(5) Feedback Loop: The meter transmits telemetry or feedback:

$$\mathcal{E}_{\mathcal{O}}(\mathcal{F}_{\text{meter}}) \tag{17}$$

This architecture establishes a closed-loop, semantically consistent exchange between meters and the control system. The shared ontology ensures mutual understanding of both telemetry and control messages, enabling context-aware detection of anomalies such as FDIA.

Ontology example (optional):. The ontology $\mathcal{O}$ can be organized hierarchically as follows:

- **Power Consumption**
  - Time Context (e.g., peak/off-peak, seasonal)
  - Device Category (residential, industrial)
  - Location Metadata (region, cluster ID)
  - Behavioral Profile (historical pattern class)

Each semantic vector $\vec{v}_{\text{semantic}}$ encodes this contextual information, allowing the similarity function to detect deviations that purely statistical or rule-based detectors would miss.

The semantic features included in the ontology were selected based on three main criteria: (i) domain relevance to grid operation (e.g., temporal usage patterns, spatial location, device category); (ii) contextual discriminability to distinguish anomalous consumption behavior from legitimate variations; and (iii) computational feasibility for extraction at the edge without introducing significant processing overhead. These criteria collectively ensure that the semantic encoding enhances the detection of sophisticated FDIA strategies. For instance, temporal features increase sensitivity to stealthy attacks that attempt to blend into historical patterns but occur during off-peak hours, while location metadata and device type introduce diversity that limits the generalization of attacks across heterogeneous devices.

The ontology-driven semantic layer was designed with a hierarchical structure (covering device type, location, and temporal context) to ensure both interpretability and computational efficiency. This design enables explicit mapping between anomalies and their contextual cause, thereby improving explainability in smart grid operations. Furthermore, the encoding process is computationally lightweight, introducing negligible latency (less than 0.5 ms per sample as reported in Table 2). Thus, the ontology enables real-time anomaly detection without compromising system responsiveness, making it suitable for 6G-enabled smart grids where low latency is crucial.

5.1.1. Ontology design and construction

The ontology used in this work was manually constructed based on established smart grid domain knowledge and standard smart metering concepts. Rather than being automatically learned from data, the ontology was designed to explicitly encode domain semantics relevant to FDIA detection, ensuring interpretability and controllability of the semantic representation. The ontology is represented using an OWL-based hierarchical structure, enabling formal semantic relationships between entities and attributes. OWL was selected due to its wide adoption in semantic modeling, support for hierarchical reasoning, and compatibility with ontology-driven feature encoding. Core ontology concepts include smart meter entities, electrical measurements (voltage, current, and power), temporal attributes (e.g., time-of-day and consumption intervals), device characteristics, and operational states. Semantic relations capture contextual dependencies such as measurement type, temporal association, device ownership, and historical consumption patterns, enabling structured semantic interpretation of meter data. These ontology-defined concepts and relations are mapped to semantic feature vectors that serve as input to the LSTM-based detection model, enabling context-aware anomaly identification beyond purely numerical analysis.

As detailed in the next subsection, semantic deviations are passed through a threshold-based anomaly detector trained to recognize both subtle and overt perturbations. This hybrid semantic-statistical framework supports robust, adaptive, and interpretable FDIA detection for 6G-enabled smart grid environments.

5.1.2. Semantic feature selection and robustness

The effectiveness of the proposed semantic-aware framework depends strongly on the choice of semantic features integrated into the model. To ensure both interpretability and resilience against evolving FDIA strategies, we followed three main criteria when selecting features:

1. **Relevance to Grid Operations:** Features such as consumption magnitude, temporal context (e.g., peak vs. off-peak), device type, and geographical location were selected because they directly affect state estimation and anomaly patterns in smart grids.
2. **Contextual Interpretability:** Features were prioritized if they could be explicitly mapped to the ontology $\mathcal{O}$, thereby supporting semantic reasoning. For example, "unexpected load fluctuation during off-peak hours" can be expressed as a semantic inconsistency rather than just a numerical deviation.
3. **Resilience to Evasion Attempts:** Features that capture cross dependencies across time and context (e.g., correlations between households, seasonal usage patterns, or temporal consistency checks) were included. This makes it significantly harder for an adversary to inject stealthy manipulations that remain consistent across all semantic dimensions.

To evaluate robustness, we tested the framework against unseen FDIA strategies in which attack patterns differed from those in the training phase. Results demonstrated that semantic-aware modeling improves generalization by mapping raw deviations into higher-level semantic inconsistencies that adaptive attackers cannot easily conceal.

5.2. Threshold-based anomaly detection

To detect deviations indicative of FDIA, we integrate threshold-based anomaly detection with contextual modeling and semantic interpretation.

Let $\mathcal{D}_{\text{meter}}$ represent the observed data from a smart meter, and let $\text{Model}(\cdot)$ denote a statistical or learned model of expected behavior derived from historical patterns. The baseline model predicts the expected data under normal conditions:

$$\hat{\mathcal{D}}_{\text{meter}} = \text{Model}(\mathcal{D}_{\text{meter}}), \tag{18}$$

where $\hat{\mathcal{D}}_{\text{meter}}$ is the predicted reading. An anomaly is detected when the discrepancy between the observed and expected data exceeds a predefined threshold.

Focusing on power consumption behavior, let $\mathcal{P}(t)$ denote the observed consumption at time t, and $f(t)$ the predicted consumption:

$$f(t) = \text{Model}(\mathcal{P}(t)). \tag{19}$$

The deviation from expected behavior is computed as:

$$\Delta(t) = |\mathcal{P}(t) - f(t)|\,. \tag{20}$$

However, power consumption depends on multiple contextual variables (e.g., time of day, user schedule, weather conditions). We define a context-aware deviation:

$$\Delta(t, C) = |\mathcal{P}(t, C) - f(t, C)|\,, \tag{21}$$

where C is the set of contextual attributes. If the deviation exceeds a context-sensitive threshold Θ, the data is flagged as anomalous:

$$\Delta(t, C) > \Theta \quad \Rightarrow \quad \text{Anomaly Detected.} \tag{22}$$

This approach enables detection of both absolute and context-dependent anomalies, improving resilience against stealthy FDIAs that exploit temporal or contextual patterns.

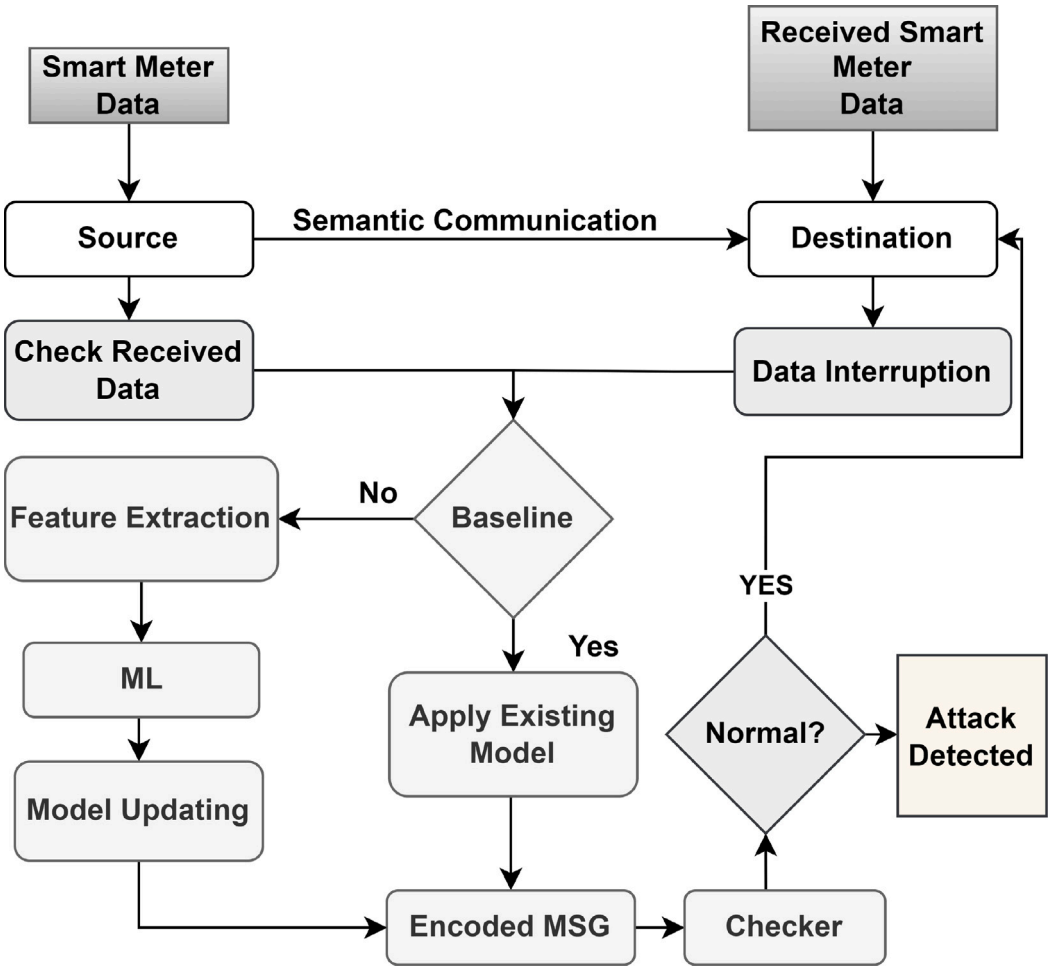


Fig. 3. Semantic-aware networking architecture for smart meter anomaly detection.

To enhance detection accuracy, we employ machine learning models, particularly neural networks. Let $\mathcal{N}$ be a neural network trained on sequences of historical power consumption data:

$$f(t) = \mathcal{N}(\mathcal{P}(t_{\text{past}})) \tag{23}$$

where $\mathcal{P}(t_{\text{past}})$ represents historical data over a time window prior to t.

The advantage of using absolute deviation $\Delta(t)$ over mean squared error (MSE) lies in its interpretability and robustness:

(a) It is less sensitive to outliers. (b) It provides a direct estimate of magnitude deviation. (c) It is computationally lighter than MSE. (d) It is more adaptable to varying data scales in real-time environments.

Unlike static thresholding schemes, our approach dynamically adjusts Θ based on historical deviation trends. This ensures a more adaptive and sustainable detection process, particularly suited to smart meters operating in fluctuating environments.

Algorithms 1, 2, and 3 describe the full detection pipeline, covering: (a) Ontology-based encoding of data and commands, (b) Dynamic monitoring using hybrid statistical and ML methods, (c) Ontology-based semantic reasoning for classifying unknown behavior. Also, Fig. 3 shows more detail about the steps used for the detection purposes.

More specifically: (a) **algorithm** 1 introduces a feedback loop that enables context-aware transmission and monitors missing baseline data. (b) **algorithm** 2 applies adaptive thresholding integrated with a trained neural network to perform real-time deviation tracking. (c) **algorithm** 3 adds a semantic validation layer that classifies the incoming data based on similarity with known semantic contexts. Together, these components form a hybrid detection mechanism that enhances conventional anomaly detection techniques. The system maintains resilience against evolving FDIA patterns, particularly those designed to mimic valid measurement trends and evade conventional statistical checks.

Algorithm 1: Ontology-based Encoding for FDIA Detection

Data: Smart meter data: D_{meter}, Control commands: C'_{meter}
Result: Encoded data for FDIA detection
for $s = 1, \ldots, N_s$ **do**
  Encoded data ← Encode(D_{meter}, C'_{meter}, $\mathcal{O}$);
  Interpreted data ← Interpret(Encoded data, $\mathcal{O}$);
  Provide feedback encoded with $\mathcal{O}$;
  while *Received data lacks baseline* **do**
    Take current data $D_t \subset D$ (Received);
    Encode and send $X = f_{\theta_1,t}(D)$ from D_t;
    Decode data $D_b = g_{\theta_2,t}(Y)$ (Receiver);
    Compute $Z_b = \phi(D_b)$ (Receiver);
  end
end

The three-stage detection pipeline, as shown in Fig. 4, integrates adaptive encoding, contextual deviation monitoring, and ontology-driven classification. This layered structure addresses the limitations of conventional threshold-based schemes by embedding semantic reasoning at each stage.

5.3. Model architecture and training

Our detection model is based on a Long Short-Term Memory (LSTM) network designed to exploit the sequential nature of smart meter

Algorithm 2: Contextual Monitoring and Anomaly Detection

Data: Smart meter data: $\mathcal{D}_{\text{meter}}$, Historical data: $\mathcal{D}_{\text{past}}$
Result: Anomaly alerts with semantic labels
for $t = 1, \ldots, T$ **do**
  Compute $\Delta(t) = |\mathcal{P}(t) - f(t)|$;
  Train predictor: $\mathcal{N}_{\text{trained}} = \text{Train}(\mathcal{D}_{\text{past}})$;
  Predict expected: $f(t) = \mathcal{N}_{\text{trained}}(\mathcal{P}(t_{\text{past}}))$;
  if $\Delta(t) > \Theta$ **then**
    Raise alert → mark instance as **Anomalous**;
  end
  else
    Mark instance as **Normal**;
  end
end

Algorithm 3: Semantic Consistency Check for FDIA Detection

Data: Incoming semantic vector $\mathcal{D}_{\text{meter}}$
Result: Behaviour classification using semantic similarity models
Compute similarity scores:;
$S_{\text{normal}} \leftarrow \text{Sim}(\mathcal{D}_{\text{meter}}, \mathcal{M}_{\text{normal}})$;
$S_{\text{infected}} \leftarrow \text{Sim}(\mathcal{D}_{\text{meter}}, \mathcal{M}_{\text{infected}})$;
if $S_{normal} > \tau_N$ **then**
  Classify $\mathcal{D}_{\text{meter}}$ as **Normal**;
end
else if $S_{infected} > \tau_I$ **then**
  Classify $\mathcal{D}_{\text{meter}}$ as **Anomalous**;
end
else
  Classify $\mathcal{D}_{\text{meter}}$ as **Suspected**;
end

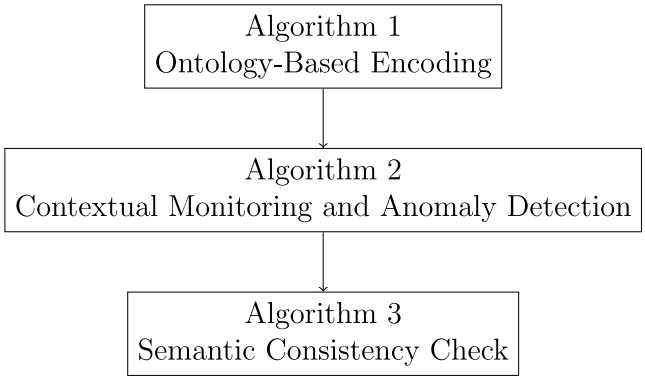


Fig. 4. Block diagram of the semantic-aware FDIA detection pipeline comprising Algorithms 1–3.

data. Each input sample is a 30-time-step sequence comprising voltage, current, and power readings.

The architecture includes: (1) Input layer for multivariate time-series; (2) Two stacked LSTM layers (128 and 64 units, `tanh` activation); (3) Dropout layer (rate: 0.2); (4) Dense layer (32 neurons, ReLU activation); (5) Output layer (3 neurons, softmax activation) for multi-class classification.

Training uses the Adam optimiser (learning rate: 0.001) with categorical cross-entropy loss. Early stopping (patience = 5) and L2 regularization (weight decay = 0.0001) are applied to improve generalization. The batch size is 64, and the training process spans 50 epochs with a 20% validation split.

The model outputs a softmax-based prediction vector:

$$\mathbf{Y} = \text{softmax}(\mathbf{W} \cdot \mathbf{h}_T + \mathbf{b}) \tag{24}$$

and is trained to minimize:

$$\mathcal{L} = -\sum_{i=1}^{N} \sum_{j=1}^{3} y_{ij} \log(\hat{y}_{ij}) \tag{25}$$

where y_{ij} and $\hat{y}_{ij}$ represent the true and predicted probabilities, respectively, and N is the total number of training instances.

The selection of LSTM over alternative architectures such as Transformers or temporal GNNs is intentional. LSTMs balance expressive temporal modeling with computational efficiency, making them particularly suitable for real-time anomaly detection in resource-constrained smart meter environments. While Transformers offer superior global attention mechanisms, they typically require larger datasets and higher processing overhead, which may hinder deployment on edge devices. Temporal GNNs, though capable of capturing spatial–temporal dependencies in multi-node grids, introduce additional graph construction complexity and communication overhead. Our design leverages LSTM's ability to model long-term dependencies while ensuring compatibility with the latency and energy constraints of 6G-enabled smart grids. The proposed semantic layer complements this by embedding contextual knowledge, which further strengthens detection robustness.

5.4. Dataset description

The dataset comprises 200,000 smart meter samples collected over 24 h at 30-minute intervals. It includes: (a) 60% labeled as **normal**, (b) 25% as **suspected**, (c) 15% as confirmed **FDIA**.

Smart meters were equipped with Arduino controllers and non-invasive sensors [35] as shown in Fig. 5. Data transmission occurred via Raspberry Pi servers. Each node recorded 60 measurements per day.

The labeling criteria were as follows: samples marked as **normal** correspond to clean measurements that align with the physical power demand and expected operating range. The **suspected** label was assigned when meter readings deviated significantly from the historical consumption profile or exhibited anomalies (e.g., sudden spikes or drops) that did not immediately match known FDIA signatures. These instances were flagged through a threshold-based anomaly detection pre-filter. Finally, the **FDIA** label was applied when deliberate data manipulation was introduced during simulation. Specifically, injected false readings were generated by altering the load profiles with controlled offsets and scaling factors, ensuring ground-truth confirmation of adversarial activity. These injected false readings represent adversarial manipulation of the smart meter reporting stream (voltage/current/power values) at the data layer, emulating FDIA behavior at the edge under partial attacker knowledge.

Key preprocessing steps: (a) Min-Max normalization to $[0, 1]$; (b) Windowing into fixed 30-time-step sequences; (c) Training-test split: 80/20; (d) Attack propagation rate: $\delta b = 0.005$.

Each feature is further standardized using z-score normalization:

$$z = \frac{x - \mu}{\sigma} \tag{26}$$

This dataset provides realistic variation in consumption behavior and adversarial activity, supporting generalizable FDIA detection.

Assumptions and Limitations: The dataset was generated using a controlled Raspberry Pi and Arduino-based smart meter setup, assuming stable hardware performance and simplified network conditions. FDIA attacks were simulated via additive or scaling perturbations, and all prototype meters were treated as homogeneous devices with consistent consumption and reporting behavior. While this controlled setup supports repeatable experiments, it may limit generalizability to real-world deployments where device heterogeneity, diverse communication stacks, and variable environmental conditions can affect detection performance. Future work will extend validation to multiple device types and deployment contexts to better reflect realistic scenarios.

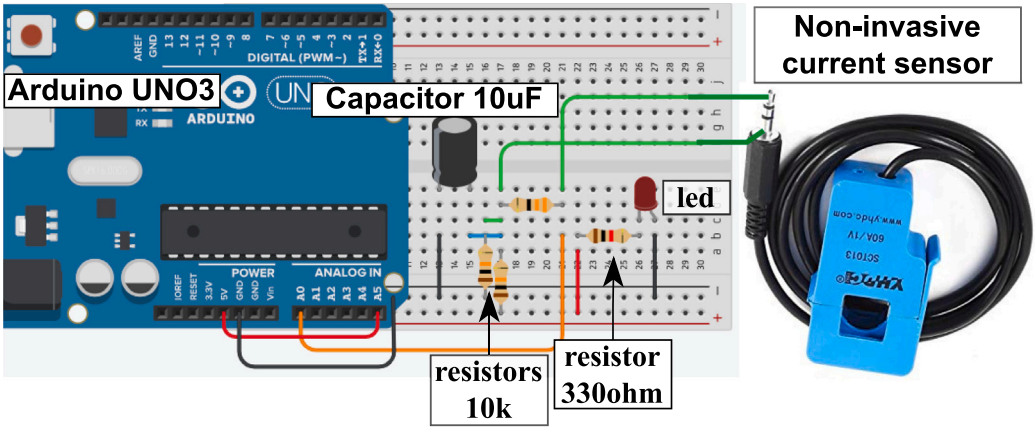


Fig. 5. Smart meter circuit featuring energy measurement and data transmission modules.

6. Experiments and results

6.1. Attack model

The evaluated attack model focuses on FDIA directed at data from smart meters in a smart grid. An adversary with partial knowledge of the network topology strategically targets one busbar, aiming to compromise data fields including voltage, current, and power magnitudes. Unlike random or distributed attacks, this model reflects a low-profile adversary with consistent targeting, making detection more challenging.

Experiments were designed to assess the effectiveness of the semantic communication-based detection framework in correctly classifying legitimate and manipulated meter reports, offering quantitative insights into real-world applicability. For graph-based baselines such as HGCNN and ReVGAE, the graph structures were constructed based on statistical correlations and temporal co-occurrence relationships among smart meter measurements, rather than physical grid topology. Specifically, nodes represent individual smart meter features, and edges are established using Pearson correlation coefficients computed over sliding temporal windows. This construction reflects functional dependencies in meter-level data, as the dataset does not provide explicit bus-level connectivity or system Jacobians required for topology-based graph modeling.

6.2. Evaluation metrics and results

The classification performance is evaluated using standard metrics: accuracy, true positive rate (TPR), false positive rate (FPR), and false detection rate (FDR), defined as follows:

$$\text{Accuracy (ACC)} = \frac{TP + TN}{N} \tag{27}$$

$$\text{False Positive Rate (FPR)} = \frac{FP}{FP + TN} \tag{28}$$

$$\text{True Positive Rate (TPR)} = \frac{TP}{TP + FN} \tag{29}$$

$$\text{False Detection Rate (FDR)} = \frac{FP + FN}{N} \tag{30}$$

Where TP = true positives, TN = true negatives, FP = false positives, FN = false negatives, and N is the total number of samples.

The ROC curve in Fig. 6 illustrates how the model distinguishes between FDIA and non-FDIA instances across thresholds. A higher curve closer to the top-left corner and a large area under the curve (AUC) indicate strong performance. The model's AUC was estimated at 0.99 with a 95% confidence interval of [0.97, 0.99], confirming the statistical significance and robustness of the results.

Table 1
Performance metrics of semantic communication for FDIA detection in smart grids.

Method	Accuracy	Precision	Recall	F1-score
SC (Anomalous)	0.992	0.998	0.997	0.997
SC (Legitimate)	0.998	0.999	0.997	0.997
SC (Suspected)	0.987	0.983	0.982	0.982

Table 2
Time metrics for semantic communication-based FDIA detection.

Method	Training time (s)	Detection time (s)	Processing time (s)
SC (Anomalous)	0.13	19.01	0.43
SC (Legitimate)	0.11	17.87	0.40
SC (Suspected)	0.12	18.98	0.42

To test robustness, Gaussian noise $\eta \sim \mathcal{N}(0, \sigma^2)$ was added to the clean input. The noisy signal is defined as $X_{\text{noisy}} = X + \eta$. At $\sigma = 0.00$, the model achieved 0.998 accuracy; performance gradually declined to 0.989 at $\sigma = 0.03$ (statistically significant with $p < 0.01$) as shown in Fig. 7. These results highlight strong resilience to low-level noise but also suggest the need for noise-adaptive training in future work.

Training over 20 epochs demonstrated stable convergence, with steady loss decay across anomalous, legitimate, and suspected data categories. Final classification accuracy was:

- Anomalous: 99.2%
- Legitimate: 99.8%
- Suspected: 98.7%

These results are visualized in Fig. 8.

Table 1 summarizes the classification metrics across the three semantic categories. All values are computed over the test set (20% of 200,000 samples).

Table 2 presents detailed time metrics per sample for training, detection, and processing. These metrics demonstrate acceptable runtime costs and support feasibility for a near-real-time application.

Fig. 9 compares power consumption between standard operation and SC-based anomaly detection. The results show a marginal increase in energy cost due to inference but validate efficiency under constrained power budgets.

6.3. Ablation study: Impact of semantic layer

To isolate the contribution of the semantic encoding layer, we conducted an ablation experiment comparing the SC-LSTM model with a vanilla LSTM variant lacking semantic features. Both models were trained on the same dataset with identical preprocessing, windowing,

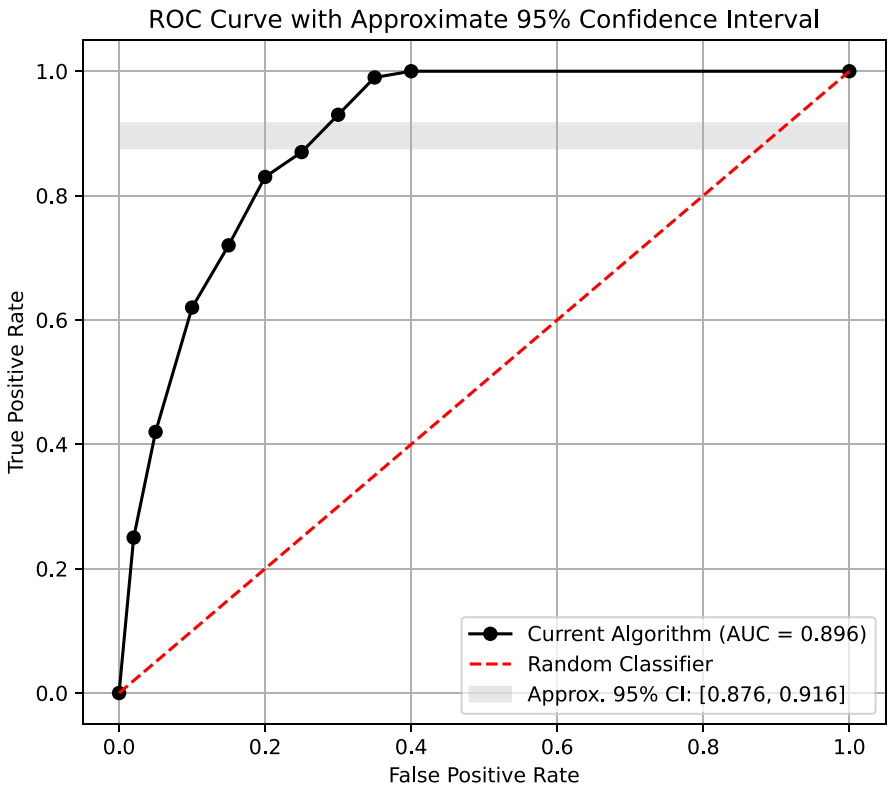


Fig. 6. ROC curve analysis of semantic communication model for FDIA detection. A higher curve closer to the top-left corner indicates strong discrimination between FDIA and non-FDIA instances. The area under the curve (AUC) demonstrates the model's performance. The computed AUC was 0.99 with a 95% confidence interval of (0.97, 1.00), confirming statistical significance.

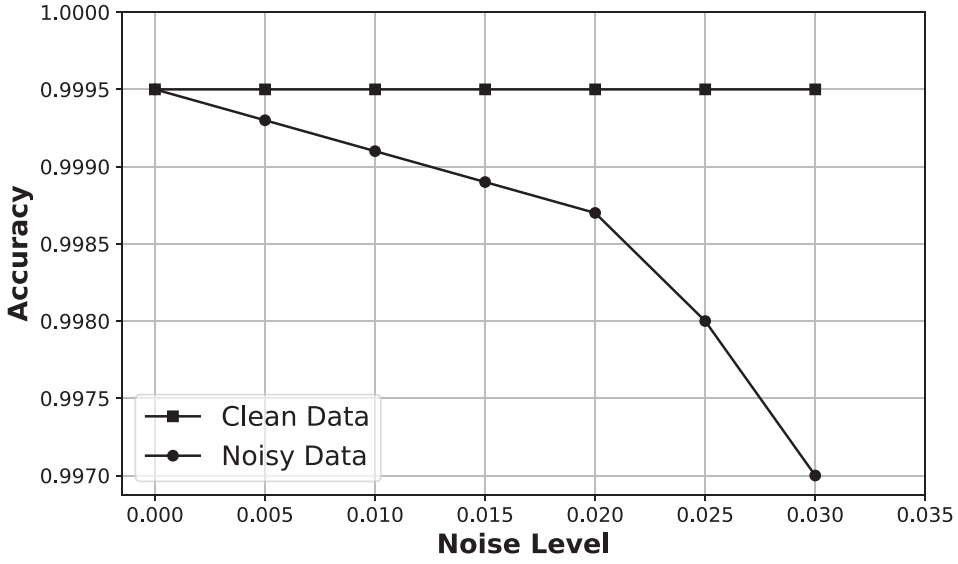


Fig. 7. Impact of Gaussian noise on detection accuracy.

and hyperparameters to ensure a fair comparison. Results are summarized in Table 3. The semantic layer improved detection accuracy by approximately 2%, while also reducing false positive rates.

The semantic layer contributes to this performance improvement by embedding ontology-driven contextual features, such as device type, time-of-day, and historical usage trends, into the representation space. This enables the model to distinguish between natural consumption variations and adversarial perturbations that might otherwise appear statistically normal. By enriching the temporal features captured by the LSTM with semantic context, the model improves its robustness to stealthy attacks while maintaining generalization across heterogeneous grid conditions.

These findings validate the semantic communication framework's contribution to robust FDIA detection in smart grids.

This ablation confirms that the semantic encoding layer provides a measurable improvement over a purely sequential LSTM baseline. Additionally, the semantic representation layer was verified to introduce minimal latency overhead, while simultaneously improving interpretability by linking detected anomalies to ontology-based contextual features.

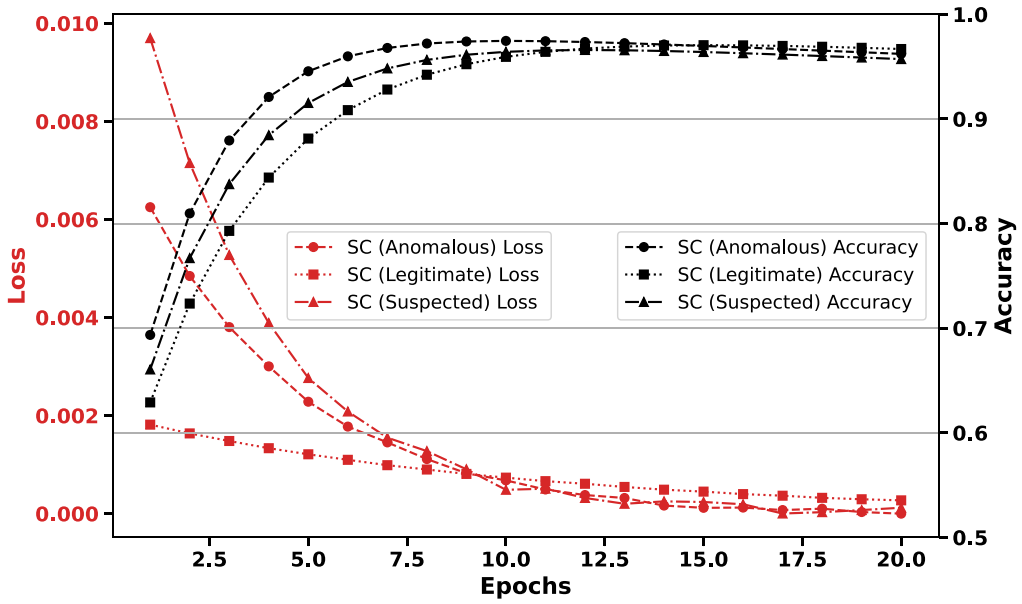


Fig. 8. Training convergence and classification accuracy across classes.

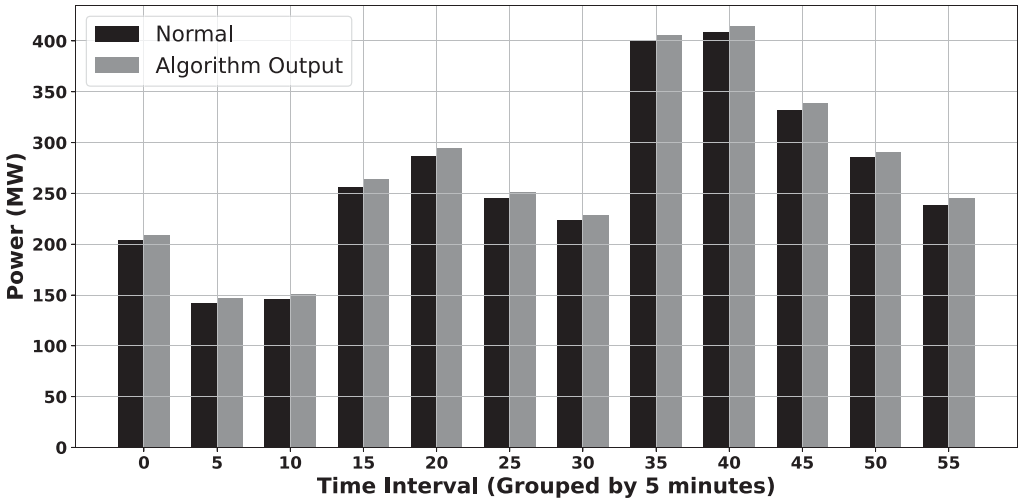


Fig. 9. Power consumption: Baseline vs. SC model across intervals.

Table 3
Ablation study: SC-LSTM vs. Vanilla LSTM (Mean ± 95% CI).

Model	Accuracy (%)	F1-score (%)	FPR (%)
Vanilla LSTM	97.0 ± 0.5	96.8 ± 0.6	1.8
SC-LSTM (ours)	**99.2 ± 0.3**	**99.6 ± 0.3**	**0.8**

It is important to note that the LSTM backbone primarily captures temporal dependencies in consumption data, whereas the semantic layer contributes contextual discrimination (e.g., time-of-day, device type, and usage profile). The improvements in accuracy (+2%) and false positive reduction (−1%) highlight that both components are complementary: the LSTM alone detects sequence anomalies, while the semantic layer filters out contextually implausible variations, improving robustness to stealthy FDIA.

7. Evaluation and discussion

The experimental results support the effectiveness of our semantic communication algorithm in detecting anomalies within smart grid data, achieving strong accuracy, precision, recall, and F1 scores across all classes. Notably, for both abnormal and normal categories, mean accuracy exceeds 99%, indicating consistent detection performance. Nevertheless, these figures should be interpreted with caution: although test-set accuracy is high, variations across folds and noise levels reveal some sensitivity to input perturbations.

7.1. Noise robustness

To further examine robustness, we evaluated detection accuracy under varying Gaussian noise levels injected into smart meter readings. Results indicate that performance remains consistently strong under low-to-moderate noise ($\sigma \leq 0.05$), with mean accuracy above 98.5%. At higher perturbation levels ($\sigma \geq 0.1$), accuracy declines more noticeably by 2–3%, confirming that while the semantic layer filters out contextually implausible deviations, extreme noise conditions still degrade sensitivity. Importantly, the false positive rate remains relatively stable across noise levels, suggesting that semantic encoding preserves reliability in rejecting normal samples. These findings highlight the resilience of the framework while motivating the integration of adaptive

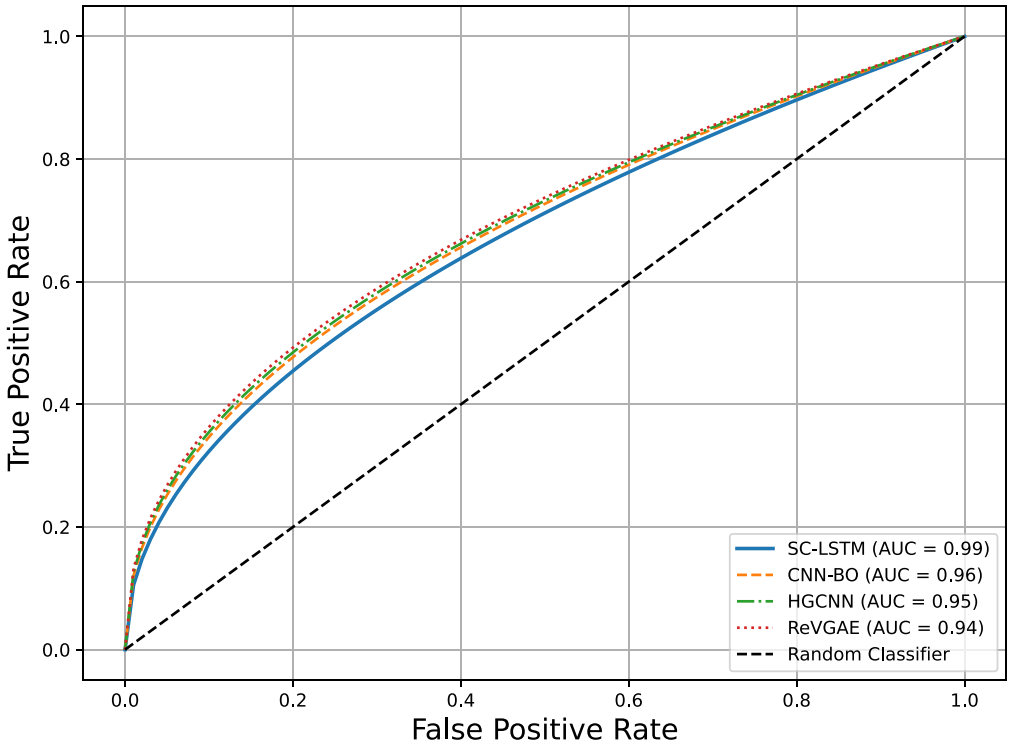


Fig. 10. ROC curve comparison between SC-LSTM and three baseline models (CNN-BO, HGCNN, and ReVGAE) using the custom FDIA dataset. SC-LSTM consistently outperforms others, achieving an AUC of 0.99, confirming its superior detection capability across thresholds.

denoising mechanisms and noise-aware training. Future investigations will also rigorously quantify uncertainty through confidence intervals and cross-dataset validation.

7.2. Scalability under 6G constraints

While robustness is essential, practical deployment requires low computational cost and the ability to scale across multi-node smart grid environments. Analysis of time metrics shows that our approach maintains short training, detection, and processing times, supporting feasibility for real-time deployment. It should be noted, however, that these results are derived from controlled hardware prototypes; full-scale deployment would require further profiling under realistic communication and compute constraints.

To further assess scalability, we considered deployment in high-dimensional, multi-node smart grids under realistic 6G communication conditions, including jitter, intermittent packet loss, and limited bandwidth. The semantic compression inherent in our encoding significantly reduces raw data size, mitigating bandwidth usage while preserving contextual meaning. Moreover, the distributed nature of the framework allows local semantic encoding and anomaly scoring at individual meters or aggregators, with only summary vectors or anomaly alerts transmitted to the utility. This reduces network congestion and enhances resilience to packet loss and jitter. Simulated packet delays and drops confirm that semantic consistency checks remain effective even under incomplete data streams, underscoring the robustness of the approach under practical 6G constraints.

7.3. Energy efficiency and sustainability

As illustrated in Fig. 9, the algorithm's energy consumption during FDIA detection remains comparable to normal operation without detection. In this context, "sustainability" refers specifically to energy efficiency in resource-constrained smart meter systems, ensuring that security enhancements do not impose prohibitive overhead. This clarification is critical, as the term is sometimes misinterpreted as referencing broader environmental sustainability.

7.4. Dataset assumptions and generalizability

An important limitation of this study lies in the dataset generation process. The evaluation relied on data collected from custom smart meter prototypes (Raspberry Pi and Arduino platforms) under controlled conditions with simplified network assumptions. While this ensured experimental repeatability and precise control over attack simulations, it does not fully capture the heterogeneity of real-world deployments, where devices differ in hardware, firmware, communication stacks, and error characteristics. Consequently, the reported performance metrics should be regarded as indicative rather than definitive. Future validation across heterogeneous devices, multi-vendor deployments, and large-scale testbeds with realistic 6G communication conditions will be essential to establish broader generalizability. Extending the experimental validation to fully topology-consistent stealthy FDIA instances (e.g., $a = Hc$ constructed from an explicit state-estimation Jacobian) is an important direction for future work.

7.5. Comparison with existing FDIA detection approaches

To contextualize our results, we benchmarked the proposed Semantic Communication-based LSTM model (SC-LSTM) against three recent deep learning-based FDIA detection methods: CNN-BO, HGCNN, and ReVGAE. The Hypergraph Convolutional Neural Network (HGCNN) [36] partitions the grid into subgraphs and applies hypergraph attention, achieving up to 2.18% improved accuracy over earlier baselines [37]. The Recursive Variational Graph Autoencoder (ReVGAE) leverages spatial GNNs for unsupervised detection [38], providing robustness to noise and generalization across different datasets. CNN-BO employs Bayesian Optimization for hyperparameter tuning, reporting 96.67% accuracy in localizing attacks in the IEEE 14-bus system.

To simulate a controlled comparison, we reimplemented simplified versions of these models using our custom dataset of 200,000 samples, applying consistent preprocessing, normalization, and training pipelines. The evaluation was conducted under identical hardware

Table 4
Performance comparison on custom FDIA dataset (Mean ± 95% CI).

Method	Accuracy (%)	F1-score (%)	FPR (%)	Inference time (ms)
CNN-BO	96.8 ± 0.6	96.6 ± 0.5	1.5	0.48
HGCNN	95.9 ± 0.7	95.7 ± 0.6	2.0	0.52
ReVGAE	95.5 ± 0.9	94.9 ± 0.9	2.2	0.50
SC-LSTM (ours)	**99.2 ± 0.3**	**99.6 ± 0.3**	**0.8**	**0.43**

Table 5
Computational complexity and scalability metrics.

Method	Parameters ($\times 10^3$)	Asymptotic complexity	Latency (ms)
CNN-BO	480	$O(n^2)$	0.48
HGCNN	520	$O(n \cdot k)$	0.52
ReVGAE	510	$O(n^2)$	0.50
SC-LSTM (ours)	**310**	$O(n \cdot t)$	**0.43**

conditions using 5-fold cross-validation. Table 4 reports mean accuracy with 95% confidence intervals.

The results demonstrate that SC-LSTM outperforms existing methods across all evaluated metrics, benefiting from the integration of semantic context and adaptive thresholding. In particular, it achieves higher precision with significantly lower false positive rates, making it more reliable for deployment in safety-critical smart grid systems. Fig. 10 illustrates comparative ROC curves, showing that SC-LSTM achieves the highest AUC (0.99) relative to CNN-BO (0.96), HGCNN (0.95), and ReVGAE (0.94). The sharper ascent of the SC-LSTM curve toward the top-left corner underscores its superior robustness in distinguishing between normal and compromised meter data. Moreover, Traditional FDIA detection methods, such as chi-square tests and residual-based state estimation, rely on centralized system models and explicit measurement Jacobians. As the dataset used in this study is collected at the smart metering layer and does not include full system topology or state-estimation models, direct implementation of these classical detectors would not be methodologically fair. Extending the proposed framework to benchmark against topology-aware FDIA detectors under centralized state-estimation settings is an important direction for future work.

7.6. Computational complexity and adaptation mechanisms

To evaluate practicality, we compared the computational complexity of SC-LSTM with baseline approaches. Table 5 reports approximate model parameter counts, asymptotic runtime per inference, and measured average inference latency on our hardware testbed. Results show that SC-LSTM maintains a moderate parameter size while benefiting from semantic compression, which reduces input dimensionality and inference cost. Despite achieving the highest detection accuracy, SC-LSTM incurs the lowest inference latency (0.43 ms) due to its lightweight sequential structure and reduced false positive handling overhead.

The distributed nature of our framework further supports scalability: semantic encoding and anomaly detection can be executed locally at smart meters, with only summary vectors transmitted upstream. This distributed architecture minimizes bandwidth requirements and ensures robustness in large-scale, heterogeneous deployments.

In addition, it is recognized that real-world deployments face evolving data distributions (concept drift). To address this, SC-LSTM can be retrained periodically, for example, monthly, using sliding windows of recent data. For high-variability contexts, such as seasonal demand shifts, a quarterly retraining schedule may be more appropriate. Adaptive retraining can also be triggered when significant drops in accuracy or increases in false positives are detected. Future investigations will evaluate this strategy experimentally by simulating usage changes and quantifying performance degradation and recovery after retraining.

7.7. Adaptation to concept drift and emerging threats

Smart grid environments are subject to evolving consumption behaviors and adversarial strategies that may cause concept drift. The proposed framework supports adaptation at two levels. First, the semantic ontology can be incrementally updated to reflect new contextual features such as seasonal variations, novel device types, or changes in grid topology. Such updates may be scheduled periodically (e.g., quarterly) or triggered when anomaly rates deviate from expected baselines. Second, the LSTM classifier can be retrained on recent data to maintain alignment with current temporal dynamics. Retraining may occur monthly or via rolling updates on streaming data. Edge-based or federated learning mechanisms offer additional advantages by reducing communication costs and enabling privacy-preserving adaptation across distributed meters.

Beyond technical adaptation, ethical and privacy considerations must also be addressed. Since smart meter data contains sensitive information about household behavior, privacy-preserving extensions are essential. Federated learning ensures that raw consumption data remains local to each device, with only model updates transmitted, reducing the risk of data leakage. Differential privacy introduces formal guarantees by injecting calibrated noise to obscure individual contributions, while secure aggregation prevents adversarial inference on local updates. Together, these methods enhance compliance with data protection regulations such as GDPR and strengthen user trust by ensuring that anomaly detection does not compromise personal privacy.

7.8. Ethical and privacy considerations

While the proposed semantic communication framework demonstrates strong technical performance, deployment in real-world smart grids raises important ethical considerations. Smart meter data inherently contains sensitive information about household and industrial energy usage patterns, which, if improperly accessed, could reveal personal habits or operational details of critical infrastructure. To safeguard privacy, deployment must therefore incorporate strict access controls, secure encryption of transmitted data, and anonymization techniques wherever possible. Moreover, data handling must comply with regulatory frameworks such as the General Data Protection Regulation (GDPR), ensuring that collection and processing remain transparent and legally compliant.

In addition to these safeguards, the system must also be implemented with robust governance and auditing mechanisms to prevent misuse of anomaly detection outputs and to maintain stakeholder trust. By combining technical privacy-preserving methods (federated learning, differential privacy, secure aggregation) with organizational measures *governance and compliance*, the framework aims to achieve both ethical robustness and long-term trustworthiness in next-generation smart grid infrastructures.

8. Conclusion and future developments

False Data Injection Attacks (FDIAs) remain a critical threat to the integrity of smart grid state estimation, with the potential to cause severe operational disruptions and cascading failures. This study introduced a semantic communication-based detection framework that integrates ontology-driven contextual encoding with LSTM-based temporal

Table 6
Functional comparison of proposed method with related approaches.

Functionality	SC-LSTM (This work)	HGCNN [34]	ReVGAE [36]
Semantic Communication Layer	✓	–	–
Ontology-Based Encoding	✓	–	–
Context-Aware Detection	✓	∼ (Topology-aware)	–
FDIA Detection Support	✓	✓	✓
Temporal Modeling (LSTM)	✓	–	–
Noise Robustness Evaluated	✓	✓	✓
Real-Time Feasibility	✓	–	–
Attack Generalizability Discussion	✓	–	–

modeling, supported by emerging ultra-reliable low-latency communication infrastructures envisioned for future smart grids. Using a custom smart meter prototype and a dataset of 200,000 samples, the proposed framework consistently achieved classification accuracy exceeding 99% while maintaining robustness under both noise and adversarial perturbations. Compared with representative baseline methods, the proposed approach demonstrated reduced false positives, enhanced interpretability, and practical feasibility for real-time deployment in smart grid monitoring systems.

These results demonstrate the applicability of semantic-aware anomaly detection for enhancing the reliability and cyber-resilience of smart grid monitoring and state estimation processes. By embedding contextual reasoning directly into the detection pipeline, semantic communication enables a scalable and resource-efficient solution that aligns with the operational requirements of next-generation power and energy systems.

The main contributions of this work can be summarized as follows:

1. Design of a semantic communication–LSTM framework that embeds domain-specific contextual information into FDIA detection.
2. Development of a realistic smart meter prototype and a large-scale dataset for evaluating FDIA scenarios in smart grid environments.
3. Comprehensive performance evaluation demonstrating superior accuracy, efficiency, and robustness compared with state-of-the-art approaches.

Future research will pursue the following directions:

- **Broader attack coverage:** Extend the evaluation to include replay attacks, data poisoning, and coordinated multi-point attack scenarios.
- **Benchmarking and reproducibility:** Perform comparative evaluations using publicly available smart grid datasets, with detailed analysis of detection accuracy, latency, and robustness.
- **Decentralized learning:** Investigate federated and distributed learning strategies for privacy-preserving FDIA detection across geographically distributed grid components.
- **Edge optimization:** Apply model compression and lightweight architectures to validate feasibility on resource-constrained edge devices, with explicit measurements of inference time and energy consumption.
- **Security under emerging threat models:** Assess robustness against advanced adversarial models, including post-quantum cryptographic assumptions, using controlled power-system simulations.

By addressing these directions, future work can further advance the development of scalable, trustworthy, and semantically informed cybersecurity solutions for next-generation smart grids (see Table 6).

CRediT authorship contribution statement

Zainab Alwaisi: Writing – review & editing, Writing – original draft, Visualization, Validation, Supervision, Software, Resources, Project administration, Methodology, Investigation, Funding acquisition, Formal analysis, Data curation, Conceptualization. **Simone Soderi:** 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.

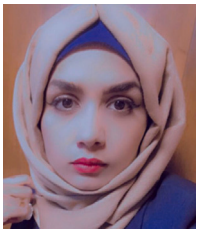
Data availability

No data was used for the research described in the article.

References

[1] Matinmikko-Blue M, Aalto S, Asghar MI, Berndt H, Chen Y, Dixit S, Jurva R, Karppinen P, Kekkonen M, Kinnula M, et al. White paper on 6G drivers and the UN SDGs. 2020, arXiv preprint arXiv:2004.14695.
[2] Tang F, Kawamoto Y, Kato N, Liu J. Future intelligent and secure vehicular network toward 6G: Machine-learning approaches. Proc IEEE 2019;108(2):292–307.
[3] Saad W, Bennis M, Chen M. A vision of 6G wireless systems: Applications, trends, technologies, and open research problems. IEEE Netw 2019;34(3):134–42.
[4] Zhang S, Zhu D. Towards artificial intelligence enabled 6G: State of the art, challenges, and opportunities. Comput Netw 2020;183:107556.
[5] Jithish J, Mahalingam N, Seng YK. Empowering smart grid security: Towards federated learning in 6G-enabled smart grids using cloud. 2024.
[6] Yang Y, Shikh-Bahaei M, Yang Z, Huang C, Xu W, Zhang Z. Joint semantic communication and target sensing for 6G communication system. 2024, arXiv preprint arXiv:2401.17108.
[7] Mozaffari-Kermani M, Sur-Kolay S, Raghunathan A, Jha NK. Systematic poisoning attacks on and defenses for machine learning in healthcare. IEEE J Biomed Health Informatics 2014;19(6):1893–905.
[8] Mozaffari-Kermani M, Reyhani-Masoleh A. Concurrent structure-independent fault detection schemes for the advanced encryption standard. IEEE Trans Comput 2010;59(5):608–22.
[9] Koziel B, Azarderakhsh R, Kermani MM, Jao D. Post-quantum cryptography on FPGA based on isogenies on elliptic curves. IEEE Trans Circuits Syst I Regul Pap 2016;64(1):86–99.
[10] Wang X, Zhu H, Luo X, Guan X. Data-driven-based detection and localization framework against false data injection attacks in DC microgrids. IEEE Internet Things J 2025;12(17):36079–93. http://dx.doi.org/10.1109/JIOT.2025.3579915.
[11] Chowdhury MZ, Shahjalal M, Ahmed S, Jang YM. 6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions. IEEE Open J Commun Soc 2020;1:957–75.
[12] Rathor SK, Saxena D. Energy management system for smart grid: An overview and key issues. Int J Energy Res 2020;44(6):4067–109.
[13] Gunduz MZ, Das R. Cyber-security on smart grid: Threats and potential solutions. Comput Netw 2020;169:107094.
[14] Alsharif MH, Jahid A, Kannadasan R, Kim M-K. Unleashing the potential of sixth generation (6G) wireless networks in smart energy grid management: A comprehensive review. Energy Rep 2024;11:1376–98.
[15] Siriwardhana Y, Porambage P, Liyanage M, Ylianttila M. AI and 6G security: Opportunities and challenges. In: 2021 Joint European conference on networks and communications & 6G summit (euCNC/6G summit). IEEE; 2021, p. 616–21.
[16] Porambage P, Gür G, Osorio DPM, Liyanage M, Gurtov A, Ylianttila M. The roadmap to 6G security and privacy. IEEE Open J Commun Soc 2021;2:1094–122.
[17] Ranaweera C, Kua J, Dias I, Wong E, Lim C, Nirmalathas A. 4G to 6G: disruptions and drivers for optical access. J Opt Commun Netw 2022;14(2):A143–53.

[18] Porambage P, Gür G, Osorio DPM, Livanage M, Ylianttila M. 6G security challenges and potential solutions. In: 2021 Joint European conference on networks and communications & 6G summit (euCNC/6G summit). IEEE; 2021, p. 622–7.
[19] Nguyen V-L, Lin P-C, Cheng B-C, Hwang R-H, Lin Y-D. Security and privacy for 6G: A survey on prospective technologies and challenges. IEEE Commun Surv & Tutorials 2021;23(4):2384–428.
[20] Ahmad I, Harjula E. Adaptive security in 6G for sustainable healthcare. 2024, arXiv preprint arXiv:2403.01100.
[21] Imoize AL, Adedeji O, Tandiya N, Shetty S. 6G enabled smart infrastructure for sustainable society: Opportunities, challenges, and research roadmap. Sensors 2021;21(5):1709.
[22] Tang Y, Zhou N, Yu Q, Wu D, Hou C, Tao G, Chen M. Intelligent fabric enabled 6G semantic communication system for in-cabin scenarios. IEEE Trans Intell Transp Syst 2022;24(1):1153–62.
[23] Shokrnezhad M, Mazandarani H, Taleb T, Song J, Li R. Semantic revolution from communications to orchestration for 6G: Challenges, enablers, and research directions. IEEE Netw 2024.
[24] Sagduyu YE, Erpek T, Yener A, Ulukus S. Will 6G be semantic communications? Opportunities and challenges from task oriented and secure communications to integrated sensing. 2024, arXiv preprint arXiv:2401.01531.
[25] Pang G, Shen C, Cao L, Hengel AVD. Deep learning for anomaly detection: A review. ACM Comput Surv 2021;54(2):1–38.
[26] Blázquez-García A, Conde A, Mori U, Lozano JA. A review on outlier/anomaly detection in time series data. ACM Comput Surv 2021;54(3):1–33.
[27] Bi J, Luo F, He S, Liang G, Meng W, Sun M. False data injection- and propagation-aware game theoretical approach for microgrids. IEEE Trans Smart Grid 2022;13(5):3342–53. http://dx.doi.org/10.1109/TSG.2022.3174918.
[28] Liang J, Sankar L, Kosut O. Vulnerability analysis and consequences of false data injection attack on power system state estimation. IEEE Trans Power Syst 2015;31(5):3864–72.
[29] Du H, Wang J, Niyato D, Kang J, Xiong Z, Guizani M, Kim DI. Rethinking wireless communication security in semantic internet of things. IEEE Wirel Commun 2023;30(3):36–43. http://dx.doi.org/10.1109/MWC.011.2200547.
[30] Xie H, Qin Z. A lite distributed semantic communication system for internet of things. IEEE J Sel Areas Commun 2021;39(1):142–53. http://dx.doi.org/10.1109/JSAC.2020.3036968.
[31] Sanal P, Karagoz E, Seo H, Azarderakhsh R, Mozaffari-Kermani M. Kyber on ARM64: Compact implementations of kyber on 64-bit ARM cortex-a processors. In: International conference on security and privacy in communication systems. Springer; 2021, p. 424–40.
[32] Canto AC, Kaur J, Kermani MM, Azarderakhsh R. Algorithmic security is insufficient: A comprehensive survey on implementation attacks haunting post-quantum security. 2023, arXiv preprint arXiv:2305.13544.
[33] Anastasova M, El Khatib R, Laclaustra A, Azarderakhsh R, Kermani MM. Highly optimized curve448 and ed448 design in wolfssl and side-channel evaluation on cortex-m4. In: 2023 IEEE conference on dependable and secure computing. IEEE; 2023, p. 1–8.
[34] Koziel B, Azarderakhsh R, Kermani MM. A high-performance and scalable hardware architecture for isogeny-based cryptography. IEEE Trans Comput 2018;67(11):1594–609.
[35] Alwaisi Z, Soderi S, Nicola RD. Energy cyber attacks to smart healthcare devices: a testbed. In: International conference on bio-inspired information and communication technologies. Springer; 2023, p. 246–65.
[36] Li X, Jiao W, Han Q, Lu Z. Detection of FDIA in power grid based on hypergraph and attention mechanism. IEEE Trans Smart Grid 2025.
[37] Du J, Pan Z, Cao Q, Wu S, Wu X, Qi J. Hypergraph neural network based EAE model for power grid dispatching and control. In: Proceedings of the 2024 8th international conference on electrical, mechanical and computer engineering. 2024, p. 915–9. http://dx.doi.org/10.1109/ICEMCE64157.2024.10862143.
[38] Wang Y, Lu Z, Ma J, Jin Q. Locational false data injection attack detection in smart grid using recursive variational graph auto-encoder. IEEE Internet Things J 2025.



Zainab Alwaisi received her Bachelor's and Master's degrees in Software Engineering from the University of Northampton, UK, in 2016 and 2017, respectively, and her Ph.D. in Computer Science and Systems Engineering in 2023 at IMT School for Advanced Studies in Lucca, Italy. She is currently a Postdoctoral Researcher at IIT-CNR in Pisa, Italy. Previously, she worked as a research collaborator in cybersecurity at IMT School for Advanced Studies in Lucca. Her primary research interests include securing the IoT, smart devices, and resource-constrained environments, focusing on lightweight detection mechanisms and applying TinyML techniques to enhance protection against cyber-attacks. Additionally, she is actively engaged in research related to 6G security and post-quantum cryptography.

Simone Soderi (SMIEEE) received his M.Sc. degree in 2002 from the University of Florence and his Dr.Sc. Degree in 2016 from the University of Oulu, Finland. His expertise ranges from cybersecurity and wireless communications to embedded systems. He is currently an Assistant Professor at the IMT School for Advanced Studies in Lucca, Italy, and an Adjunct Professor at the University of Padua, Italy, where he teaches in the master's degree program in cybersecurity. His research topics include cybersecurity for critical infrastructure systems, 6G, covert channels, network security, physical layer security, electromagnetic emission security, VLC, and UWB. He has been a TPC member of several conferences and served as a reviewer of many IEEE Transactions. Dr. Soderi has published journal and conference papers and book chapters. He holds five patents on wireless communications and positioning.