Scilight

Smart Energy Systems

https://www.sciltp.com/journals/ses

Article

Electricity Theft Detection and Protection in a Power Distribution System: A Modeling and Analysis Approach

Sajid Hussain [1,2], Umar Jamil [3], Nabeeha Qayyum [4] and Anzar Mahmood [1,*]

[1] Department of Electrical Engineering, Mirpur University of Science and Technology, Mirpur 10250, Pakistan
[2] Larsen & Toubro Limited, Riyadh 295020, Saudi Arabia
[3] Department of Electrical Engineering, University of Texas at San Antonio, San Antonio, TX 78249, USA
[4] Department of Electrical and Computer Engineering, COMSATS University, Islamabad 45550, Pakistan
* Correspondence: anzar.pe@must.edu.pk

How To Cite: Hussain, S.; Jamil, U.; Qayyum, N.; et al. Electricity Theft Detection and Protection in a Power Distribution System: A Modeling and Analysis Approach. *Smart Energy Systems* **2026**, *1*(1), 5.

Received: 26 November 2025
Revised: 15 June 2026
Accepted: 15 June 2026
Published: 24 June 2026

Abstract: Electrical energy theft is a critical concern with significant implications for the economic, reliable, and stable operation of power systems, especially in less developed countries. While technical losses occur during power transmission and distribution, non-technical losses, including electricity theft, pose a greater challenge to system stability by introducing unpredictability. This research presents an integrated Power Line Communication (PLC) with Advanced Metering Infrastructure (AMI) based technique, supported by high-frequency signal communication, to detect, monitor, and control energy theft. In the proposed scheme, high-frequency, low-amplitude signals are transmitted through the power system, and variations in the amplitude of both high- and low-frequency signals are analyzed to detect illegal energy consumption. As a result, the distribution system can be automatically disconnected from the rest of the power system in the event of a fault or theft occurrence. The MATLAB® (R2024a (v 24.1)) Simulink tool is used to design and analyze the proposed theft detection and protection model. The results demonstrate that the hybrid PLC–AMI technique efficiently detects different types of electricity theft loads and system faults.

Keywords: electricity theft; non-technical loss; frequency signal-based communication; fault detection; power system

1. Introduction

Electricity demand is steadily rising across all sectors due to the rapid advancement and widespread adoption of electrical appliances [1]. At the same time, building new conventional power plants is becoming increasingly difficult because of environmental concerns and strict government policies on pollution control [2]. This situation has placed greater emphasis on efficient electricity consumption planning, where the goal is not only to optimize available generation capacity but also to minimize losses within the existing infrastructure. Electricity generated at power stations is delivered to consumers through an extensive network of transmission and distribution lines, transformers, poles, and associated equipment. However, the energy received by end-users is often lower than the energy produced at the source, and this discrepancy is referred to as power system losses. Among these, the distribution network is the most vulnerable segment, accounting for the majority of the overall losses, while the transmission system contributes a relatively smaller portion [3,4], highlighting the potential for reducing losses and improving overall grid efficiency.

Power system losses are broadly classified into technical and non-technical categories. Technical losses occur naturally as electricity flows through conductors, transformers, and meters, and although these can be minimized through better equipment and design, they cannot be eliminated. They result from factors such as conductor

resistance (I^2R losses), dielectric heating, magnetic effects, load imbalances, undersized equipment, and poor maintenance practices. In contrast, non-technical losses (NTL) are external in nature and arise from human actions or operational inefficiencies. These include electricity theft or meter tampering, illegal connections, billing errors, inaccurate meter readings, meter malfunctions, and unpaid bills [5,6]. Among these, electricity theft is the most significant contributor, particularly in least developed countries such as Congo [7,8], and in developing countries such as Brazil, Nigeria, Ghana, Pakistan, India, and Bangladesh etc. [9–14], where weak enforcement, lack of advanced monitoring infrastructure, and limited financial resources exacerbate the problem. Unlike technical losses, NTLs are difficult to quantify due to irregular patterns and inadequate records, which further complicates detection and prevention.

Figure 1 shows traditional electricity theft method which includes direct hooking, drilling holes in meters, and meter tempering. In less developed or developing countries, where electricity theft is widespread and resources are limited, Power Line Communication (PLC) combined with Advanced Metering Infrastructure (AMI) is considered the most effective method, as it enables real-time, bidirectional communication, accurate theft detection, and precise localization, critical advantages in areas with high theft rates and limited manpower. Compared to Global System for Mobile Communications (GSM)-based systems, manual inspections, wireless ZigBee modules, Arduino based system, and other techniques [15–18], PLC combined with AMI offers superior scalability, automation, and long-term cost savings, while also encompassing the benefits provided by the aforementioned methods [19]. PLC technology combines the strengths of wired fiber-optic and wireless communication by offering secure, high-speed data transfer. It is particularly effective in delivering elevated data transmission rates within smaller network environments [20].

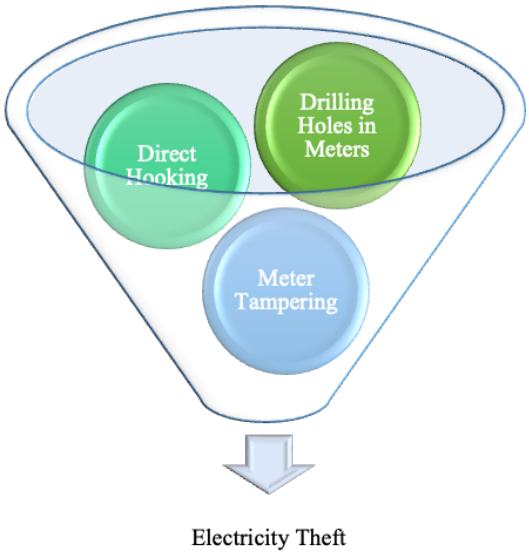


Figure 1. Electricity theft methods.

Electricity theft and ground faults cause significant losses and threaten grid reliability. Table 1 shows comparison of proposed method for electricity theft detection with existing methods.

Table 1. Comparison between different electricity theft detection techniques.

Method	Communication/System	Accuracy	Response Time	Deployment Cost	Communication Overhead	Scalability
GSM-based systems	Cellular network	Moderate	High (seconds–minutes)	High (SIM + module cost)	High	Limited
ZigBee-based systems	Wireless sensor network	Moderate	Medium	Medium	Medium	Moderate
Arduino-based systems	Embedded standalone	Moderate	Medium	Low	Low-Medium	Low
AI/ML-based	Software-based classification	High	Medium	Medium–High	Low	High
Proposed method	Power Line Communication + Smart Metering Infrastructure	High	Very Low (real-time)	Low (uses existing grid)	Low	Very High

While developed countries have increasingly focused on adopting intelligent techniques such as state estimation and artificial intelligence-based approaches for electricity theft detection [21,22], recent studies have further advanced this direction. In [23], the authors proposed Kalman filter-based energy theft detection algorithms for smart grids, including a privacy-preserving framework that identifies energy theft while protecting users' load profile privacy through parallel filtering and privacy analysis. Building on privacy-aware theft detection, the authors introduced a stochastic Petri Net-based framework for electricity theft detection and localization in grid-tied microgrids with bi-directional power flow [24]. The method utilizes smart meter resistance disturbances and singular value decomposition to accurately identify theft locations and estimate technical and non-technical losses while preserving customer privacy through low-rate data transmission. Similarly, another study [25] proposed a privacy-preserving energy theft detection scheme that combines state estimation-based recursive filtering with lightweight encryption to detect abnormal energy consumption while reducing communication and computational costs in smart grid systems. Furthermore, the authors in [26] proposed a state estimation–based framework to detect NTLs caused by partial meter bypass, enabling theft localization, timing identification, and loss estimation with low false-positive rates, while demonstrating robustness against network variations and irregular consumption behavior.

In [27], classical machine learning ensembles such as logistic regression and random forest regression were introduced to address class imbalance in electricity theft detection, improving minority-class learning and overall classification performance. Similarly, ref. [28] extend this direction by evaluating multiple machine learning models (including Naive Bayes, Support vector machine, Adaptive Boosting, decision tree, and random forest), where random forest achieved the best results with 95% accuracy and balanced evaluation metrics, particularly in non-smart grid environments. Building on these traditional machine learning approaches, ref. [29] shifts toward deep learning model that integrates temporal convolutional networks with Bayesian optimization to enhance feature extraction and automate hyperparameter tuning for time-series-based theft detection in smart grids. Further advancing robustness, ref. [30] propose a tensor decomposition–driven contrastive distillation and semi-supervised multitask learning framework to handle high-dimensional, incomplete spatio-temporal data, significantly improving performance under real-world uncertainty and missing information.

Extending beyond single-model improvements, ref. [31] introduce a multi-objective evolutionary hybrid deep learning framework that simultaneously optimizes detection accuracy, reduces false positives, and captures periodic consumption patterns, improving overall decision robustness. Another study, ref. [32] address practical deployment constraints by proposing a deep compression–based split computing framework, enabling efficient execution of deep learning models in resource-constrained internet of things and smart grid environments, thereby bridging the gap between high-performance detection models and real-world implementation feasibility.

Overall, the literature demonstrates a clear shift toward more intelligent, accurate, and deployable electricity theft detection systems. However, despite these advancements, existing approaches still face several challenges, including high computational complexity, limited interpretability of deep learning models, and reduced generalization performance due to dataset dependency and evolving attack behaviors in smart grid environments. Furthermore, in many developing and least developed countries, the adoption of advanced electricity theft detection techniques remains constrained by limited financial resources, weak regulatory enforcement, a shortage of skilled workforce, inadequate infrastructure, and low penetration of advanced metering systems. As a result, utilities in these regions continue to rely primarily on conventional or manual theft detection approaches [33,34].

Although prior studies have explored PLC-based techniques for detecting resistive-inductive (RL) and resistive (R) theft loads [35,36], these methods remain limited in scope, as they do not address multiple theft load characteristics, fault detection, or integrated theft protection capabilities. In addition, most previous studies have primarily focused on theft detection rather than simultaneously incorporating system protection mechanisms. To address these limitations, integrating PLC with AMI offers a promising solution by enabling real-time monitoring, secure communication, and enhanced detection of both theft and fault conditions.

Motivated by these challenges and research gaps, this study proposes a unique hybrid PLC-AMI framework for electricity theft detection and protection in power distribution systems to improve grid security, reduce non-technical losses, and support sustainable grid operations. In the proposed approach, different theft load types, together with ground fault circuits, are incorporated into a base-case system (without theft/fault) to analyze variations in carrier signal voltage, power signal frequency, and protection device (circuit breaker) current, which are subsequently compared with normal operating conditions to identify abnormal behavior.

2. Methods

2.1. Power System Flow

Figure 2 illustrates the complete power system flow, starting from generation and extending through transmission and distribution to the load. The sequence includes generators, high-voltage transmission lines with transmission towers, substations, distribution transformers, distribution feeders, energy storage units, PLC couplers, service lines to customers, smart meters, protection devices, AMI, and other components.

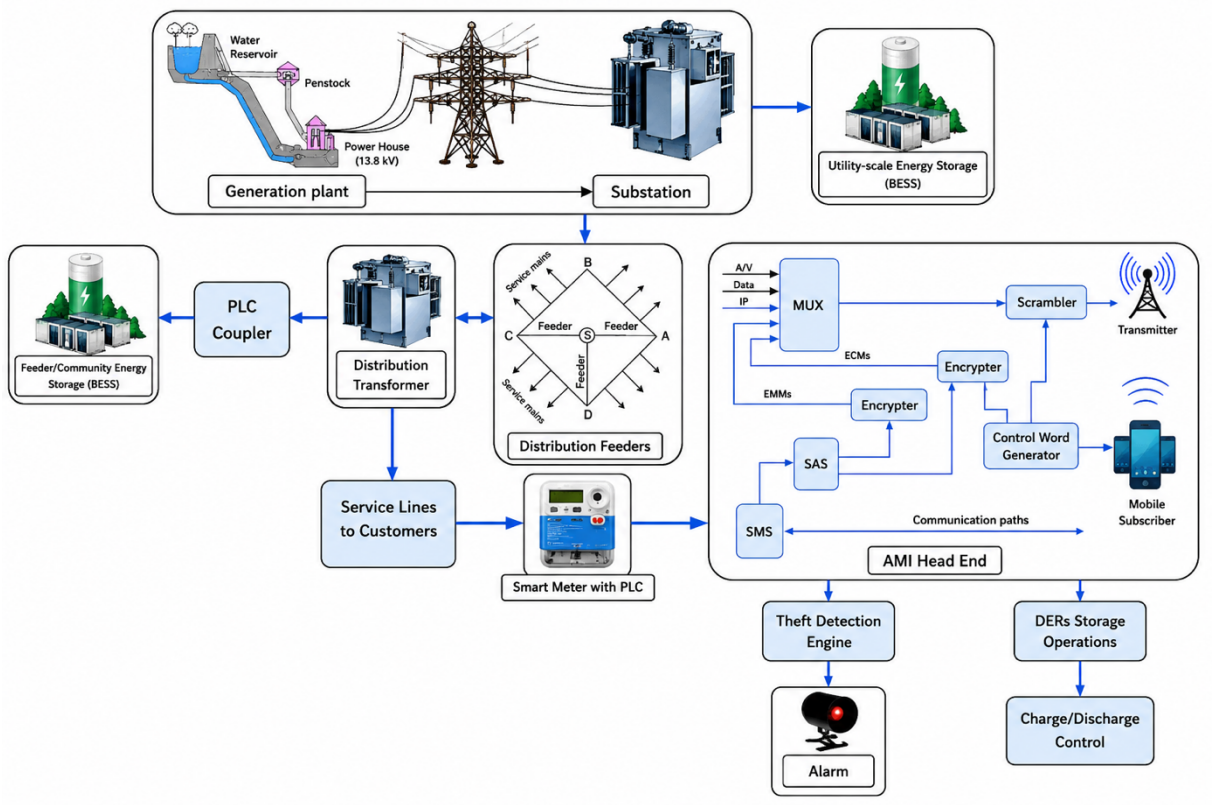


Figure 2. Power system flow from generation through transmission and distribution to load.

In the current power system, variations in the connected load cause small voltage drops and frequency fluctuations at the load end. These fluctuations are typically short-lived, as capacitor banks and other equipment work to stabilize the system.

2.2. Integrated PLC with AMI

In the proposed system, two signals are injected into the transmission line: a 50 Hz, 230 V power signal and a 150 kHz, 20 V high-frequency carrier signal. The carrier signal is injected through a high-frequency coupling circuit providing galvanic isolation while allowing propagation along the power line. Series capacitors and high-impedance inductors are used to separate the low-frequency (50/60 Hz) and high-frequency components, ensuring safe operation and minimizing interference with normal loads. Additionally, band-pass and notch filters are employed to suppress noise, harmonics, and other unauthentic components, thereby preserving the integrity of the carrier signal.

Since the carrier signal is not compensated within the power system, variations in load conditions affect its amplitude. Therefore, monitoring the carrier amplitude enables detection of electricity theft through the AMI. The proposed scheme can also identify fault conditions and frequency variations in the power signal. In integration with AMI, the PLC-based system continuously monitors voltage and current characteristics and initiates disconnection when abnormal conditions are detected, as illustrated in Figure 3.

In principle, when high-frequency and low-frequency signals coexist in the power line, inductive elements impede high-frequency components while allowing low-frequency power flow, whereas capacitive elements block low-frequency signals and permit high-frequency carrier propagation. This frequency-selective behavior enables independent monitoring of both signals for detecting load variations, faults, and potential electricity theft in the distribution network.

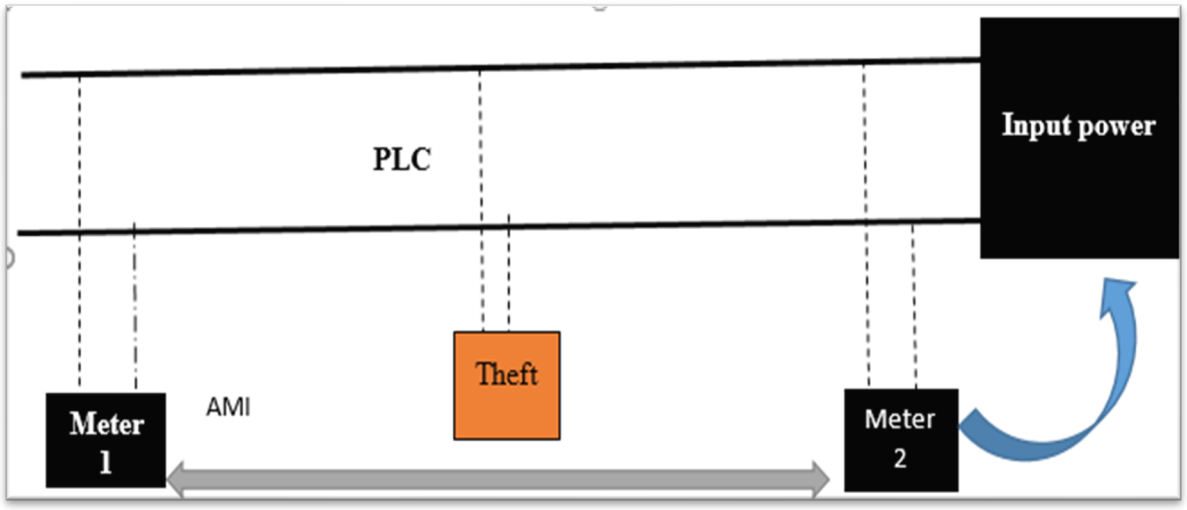


Figure 3. Integration of AMI with PLC.

Security of PLC-AMI system is a critical requirement to prevent energy theft, spoofing, and malicious control actions. In the proposed system, data exchange between smart meters and the data concentrator unit (DCU) is assumed to be protected using symmetric encryption (e.g., AES-128/256) to ensure confidentiality. Mutual authentication mechanisms are considered so that both the meter and the DCU verify each other's identity before data transmission. Message integrity codes (MICs) and sequence counters are used in standard PLC-AMI security frameworks to prevent replay and message injection attacks. To mitigate carrier signal spoofing or jamming, the system considers signal validation techniques such as frequency consistency checks, modulation pattern verification, and anomaly detection at the head-end. In addition, redundancy in data reporting and event logging can help detect abnormal communication behavior. Physical bypass attempts are addressed through tamper detection features within the smart meter, including voltage imbalance monitoring and neutral disturbance detection. Any abnormal condition is reported to the utility for further investigation.

2.3. Proposed Model

In this research work, the MATLAB Simulink tool is used to design the proposed model, which consists of various detection and protection devices such as circuit breakers, relays, pi-section lines, inductive, capacitive, and resistive components, as well as power and voltage sources, as shown in Figure 4. In an inductive component, voltage is opposed by a back electromotive force (EMF), which is proportional to the rate of change of current. At higher AC frequencies, the rate of change of current increases at the peak of the sine wave, leading to a greater back EMF that opposes current flow. A capacitor blocks DC signals but allows AC signals, provided the AC frequency is not too low. At very low frequencies, the capacitor cannot charge and discharge quickly enough due to frequency limitations, thus effectively blocking the low-frequency signal. The resistive component limits the flow of current, and its impedance depends on the frequency of the signal. The impedances of these three components are shown in Equation (1).

$$Z = \begin{cases} 2\pi fL, & for\ inductive\ component \\ {}^{1}/_{2\pi fC}, & for\ capacitive\ component \\ R, & for\ resistive\ component \end{cases} \quad (1)$$

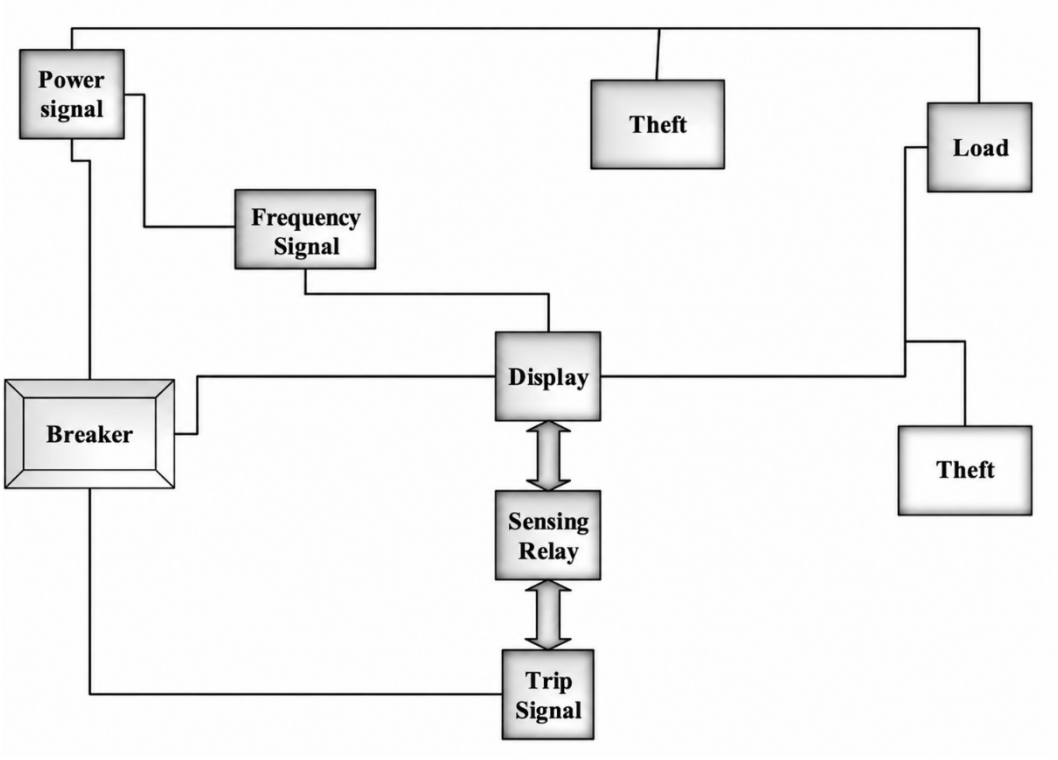


Figure 4. Block diagram of proposed system.

Three main model parameters, representing theft loads, are considered: RL, RC, and R Load, as presented in Table 2. In the proposed model, pi-section lines are integrated with different theft loads and a ground fault circuit sequentially, as indicated in Figure 5, to analyze the behavior of theft/fault cases compared to the no-theft/no-fault case. The parameters of the pi-section lines, breaker, and source/components are shown in Table 3. The power distribution system is disconnected from the transmission system whenever any hazard, such as a fault or theft, occurs. The breaker current output serves as an indicator to identify the type of theft or fault. The MTALAB Simulink model for electricity theft detection and protection system is shown in Figure 6. The workflow of the proposed Electricity Theft Detection approach is presented in Algorithm 1.

Table 2. Mathematical representation of theft load types and associated voltage deviation characteristics.

Theft Load Types	Theft Load Impedance (Ω)	Voltage Drop across Theft Load (V)	Voltage Deviation (V)
RL Load	$Z_{RL} = R_t + j\omega L_t$	$V_{RL}(t) = I_{RL}(t)\, Z_{RL}$	$\Delta V_{RL}(t) = V_{base}\,(t) - V_{RL}(t)$
RC Load	$Z_{RC} = R_t - {}^{j}/_{\omega C_t}$	$V_{RC}(t) = I_{RC}(t)\, Z_{RC}$	$\Delta V_{RC}(t) = V_{base}\,(t) - V_{RC}(t)$
R Load	$Z_R = R_t$	$V_R(t) = I_R(t)\, R_t$	$\Delta V_R(t) = V_{base}\,(t) - V_R(t)$

$V_{base}\,(t)$: base voltage with no theft.

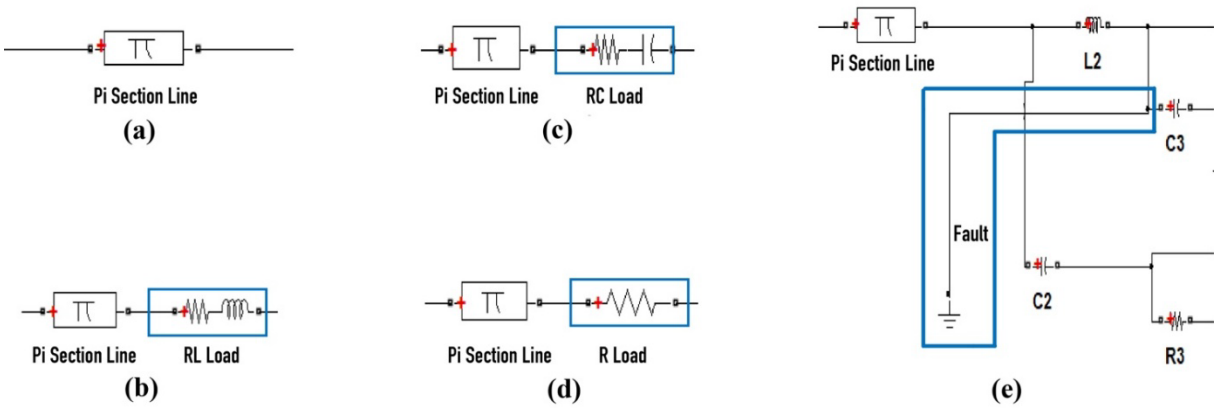


Figure 5. Pi Section lines with: (**a**) No Theft Load case (**b**) RC Theft Load case (**c**) RL Theft Load case (**d**) R Theft Load case (**e**) Ground Fault case.

Table 3. Model parameters.

Pi-Section Line Parameters	Value	Circuit Breaker Parameters	Value	Source/Component	Value
Number of Phases & Pi sections	1	Initial status	1 (closed)	AC Voltage Source	230 V peak/50 Hz
Line Length	100 km	Breaker resistance	0.1 mΩ	High Frequency Signal	20 V peak/150 kHz
Frequency used for RLC specification (Hz)	50 Hz	Snubber resistance	1 MΩ	L1	10 µH
Resistance per unit length	0.01273 Ω/km	Snubber capacitance	0 F (disabled)	L2	1 µH
Inductance per unit length	0.9337 mH/km	Breaker control Time	[0 1.5/60 3/60] s	C1, C2, C3	1 µF
Capacitance per unit length	12.74 nF/km	Amplitude	[1 0 1]	R1, R2, R3	200 Ω

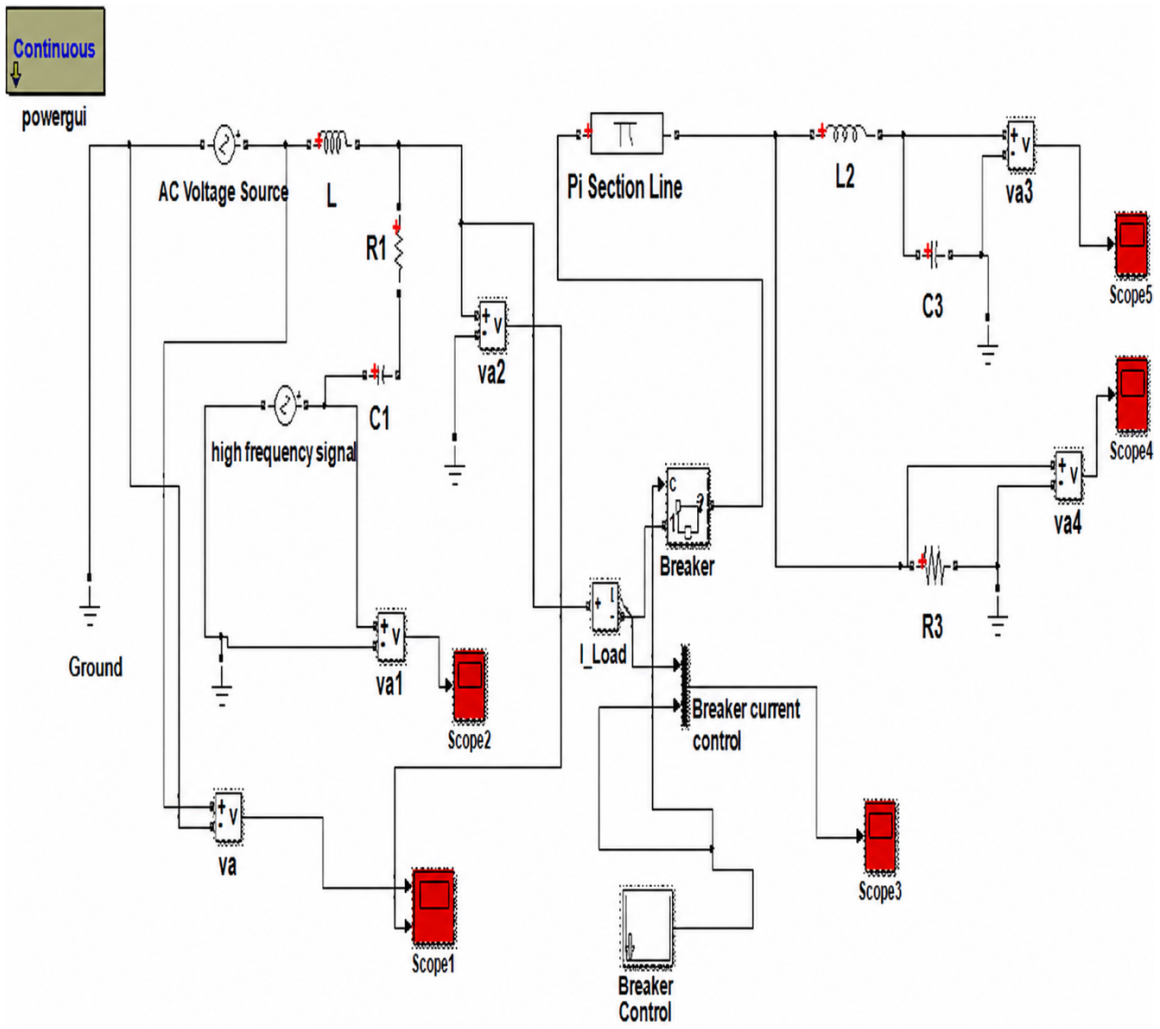


Figure 6. Simulink model of electricity theft detection and protection system.

The proposed method is a deterministic physics-based detection approach; therefore, evaluation focuses on waveform-level separability and feature discrimination rather than statistical classification metrics. The proposed system is designed with cost-effectiveness in mind by leveraging existing power line infrastructure for communication through PLC, thereby reducing the need for additional dedicated communication networks. In addition, the hardware requirements are minimal, as the detection mechanism relies primarily on signal injection and measurement rather than expensive sensing or metering infrastructure. While a detailed economic analysis is beyond the scope of this study, these design considerations suggest that the proposed approach has the potential to reduce deployment and operational costs compared to standalone communication-based theft detection systems.

Algorithm 1. Electricity Theft Detection

Step 1: Measure carrier signal volage V(t)

Step 2: Compute positive peak:

V_{peak} = max (V(t))

Step 3: Set threshold:

$V_{th} = 17\ V$

Step 4: Decision logic:

IF $V_{peak} \geq V_{th}$

→ Normal Operation

Else IF $V_{peak} < V_{th}$

→ Suspicious Condition

Step 5: Persistence check:

IF $V_{peak} < V_{th}$ persist for N $\geq$ 3 or more cycles

→ Theft Detected

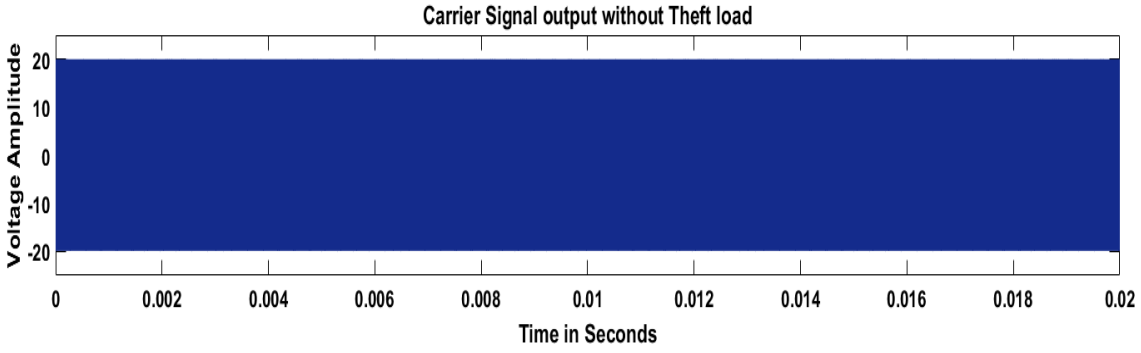
3. Results and Discussions

This section discusses following cases with results.

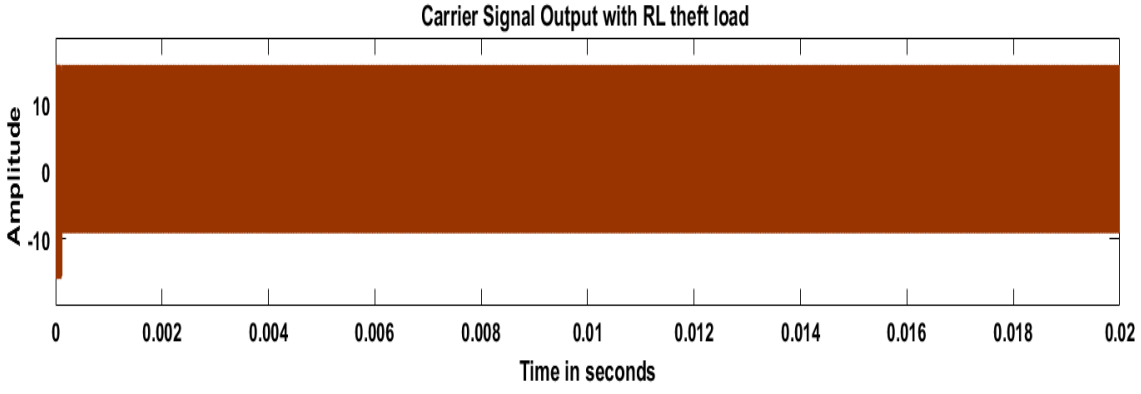
(a) Impact of theft loads and ground faults on the output of carrier voltage signal
(b) Impact of power signal frequency on the output of carrier voltage signal
(c) Impact of theft load and ground faults on the output of breaker current signal
(d) Comparative analysis against existing relevant methods

3.1. Impacts of Theft Loads and Ground Faults on the Output of Career Signal

In the case of no theft condition, the carrier signal output voltage lies within the amplitude range of –20 V to 20 V, as depicted in Figure 7a. This represents the normal operating condition, where the carrier signal maintains its full symmetrical swing.



(**a**)



(**b**)

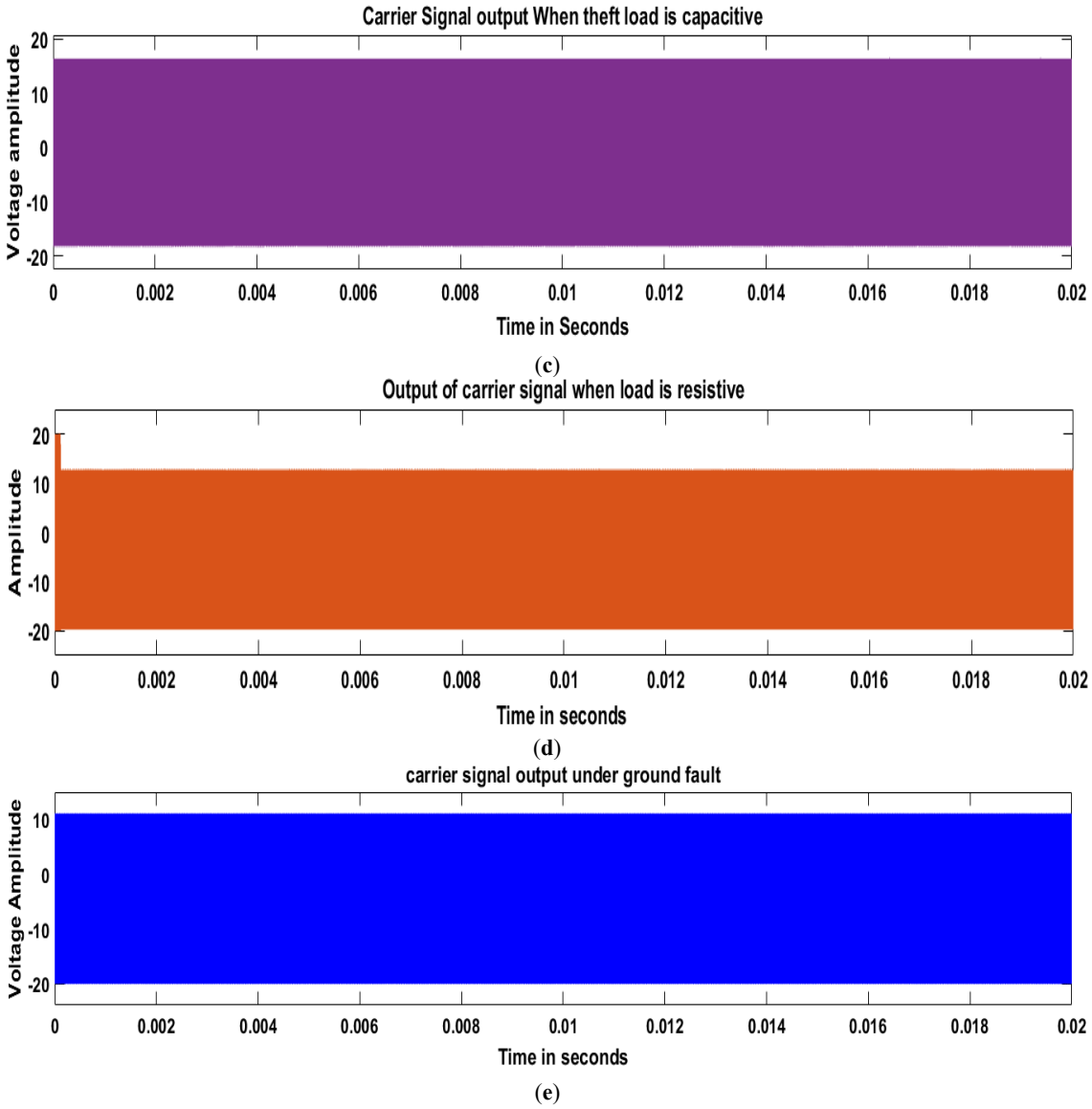


Figure 7. Analysis of voltage amplitude for different case (**a**) No Theft Load (**b**) RL Theft Load (**c**) RC Theft Load (**d**) R Theft Load (**e**) Ground Fault.

Under different theft conditions, the amplitude range of the carrier signal becomes distorted. For RL theft load, the amplitude is reduced to between –9 V and 15 V, as shown in Figure 7b. This indicates that the RL load causes a shift and compression of the carrier signal. For RC theft load, the carrier signal varies between –18 V and 16 V (Figure 7c), showing that the capacitive-resistive load slightly reduces the negative swing while maintaining near-symmetric behavior on the positive side. For R theft load, the carrier signal amplitude decreases further to the range of –19.5 V to 11 V (Figure 7d), which reflects that a purely resistive theft load mainly suppresses the positive amplitude.

In the case of a ground fault in the absence of theft load, the carrier signal output voltage magnitude is limited to the range of –20 V to 10.5 V, as illustrated in Figure 7e. This result suggests that the fault condition primarily reduces the positive half-cycle of the signal while leaving the negative half-cycle almost unaffected. The Table 4 shows career signal output voltage across time for different system states.

Table 4. Career signal output voltage for different system states.

System State	Overall Range of Career Signal Output Voltage (V)
No Theft/Fault	[−20, 20]
RL Theft Load	[−9, 15]
RC Theft Load	[−18, 16]
R Theft Load	[−19.5, 11]
Ground Fault	[−20, 10.5]

3.2. Impacts of Power Signal Frequency on the Output Carrier Voltage Signal

The effect of supply frequency on the carrier signal is shown in Figure 8a,b. At a frequency of 60 Hz, the carrier signal output voltage varies within the range of –17 V to 16 V, whereas at the nominal 50 Hz frequency, the range extends to –19 V to 19 V. This comparison highlights that increasing the supply frequency slightly reduces the overall amplitude swing of the carrier signal. The narrower range observed at 60 Hz indicates a reduction in signal sensitivity, which may affect the ability to clearly distinguish abnormal operating conditions. In contrast, the wider and more symmetric range at 50 Hz reflects stable system behavior under normal frequency conditions.

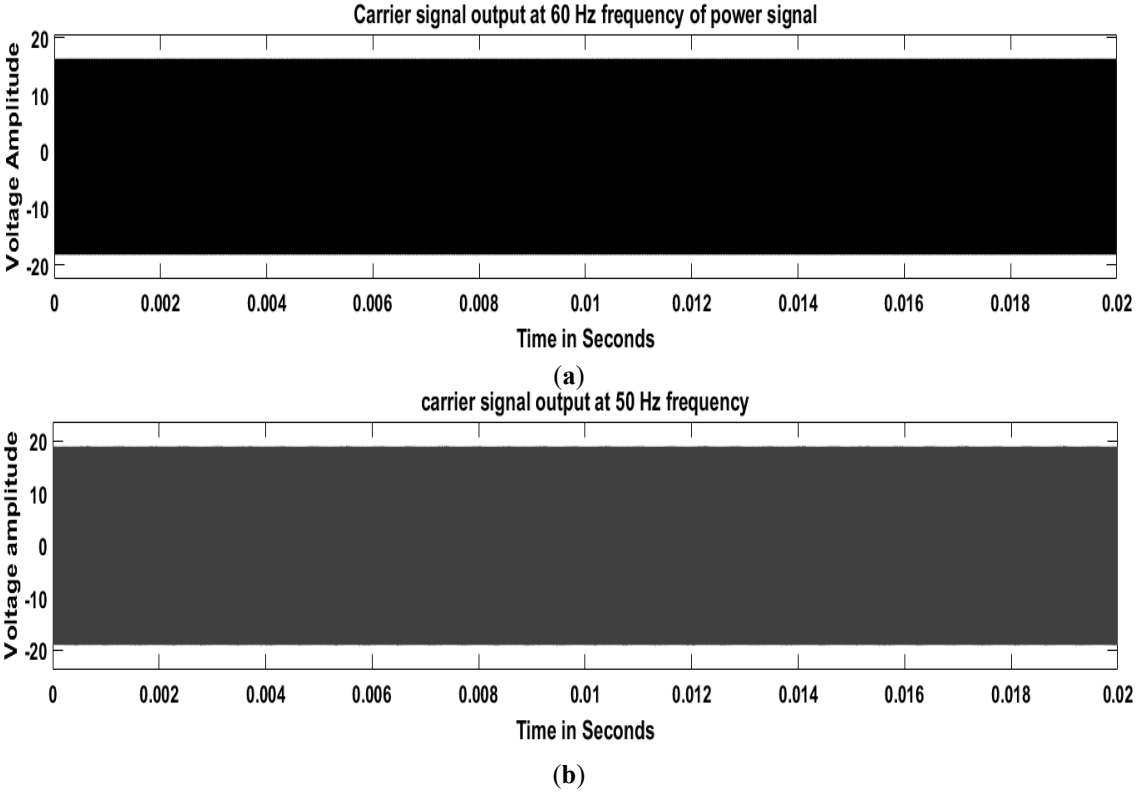
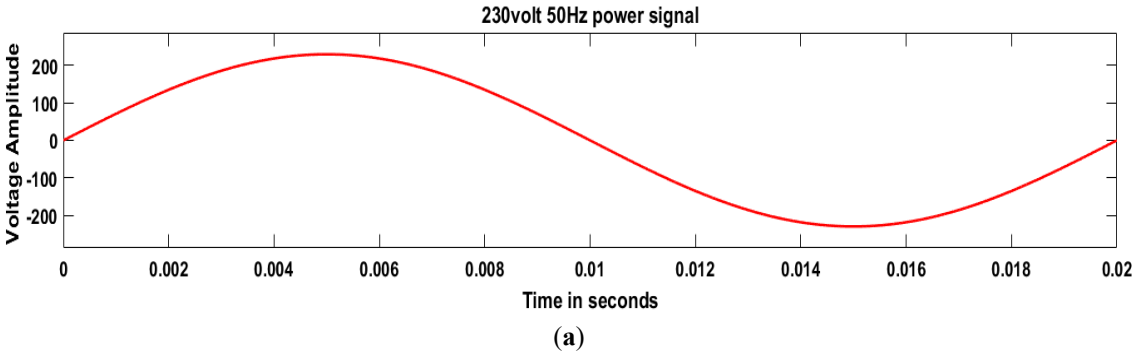
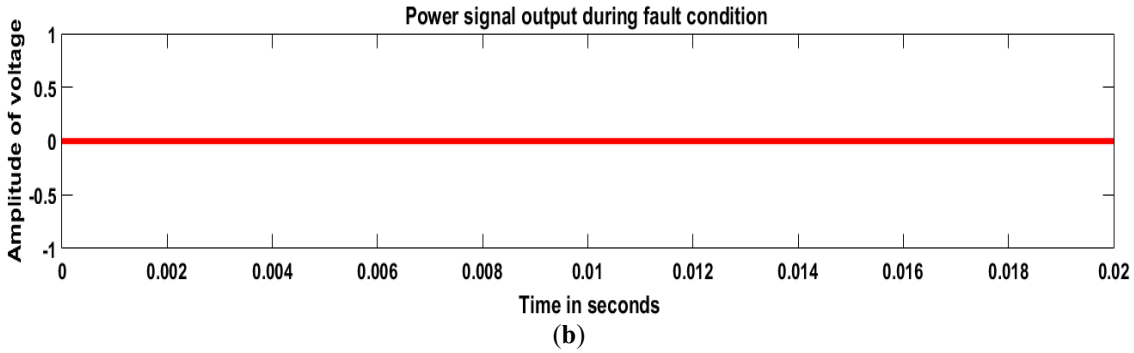


Figure 8. Analysis of career signal output voltage at different frequency of power signal (**a**) at 60 Hz, (**b**) at 50 Hz.

The power signal at 230 V and 50 Hz, which appears as a sinusoidal waveform with a maximum amplitude of approximately 230 V, is observed in the time range of 0–0.02 s during no-fault condition, as shown in Figure 9a. In a single line-to-ground fault, the fault current remains very small due to the capacitive nature of the earth. Conventional overcurrent-based detection systems are generally unable to detect such minor imbalances in a single phase. However, the proposed system demonstrates the capability to identify these subtle fault conditions in the power network. Under fault conditions, the output of the power signal is observed as a straight line, as depicted in Figure 9b, which illustrates both the output of the power signal at the distribution end and the corresponding fault detection circuit.





(**b**)

Figure 9. Analysis of power signal output on distribution side (**a**) No Fault Condition (**b**) Fault Condition.

The carrier signal in the proposed system operates at a significantly higher frequency (150 kHz) compared to the fundamental grid frequency (50/60 Hz). Therefore, small grid frequency variations such as ±1–2 Hz (e.g., 49–51 Hz or 59–61 Hz) primarily affect only the low-frequency component of the power signal and do not directly overlap with the high-frequency carrier band. In the proposed design, coupling and band-pass filtering stages are assumed to suppress low-frequency variations and their harmonics, thereby limiting their influence on the carrier signal.

3.3. Impacts of Theft Load and Ground Faults on the Output of Circuit Breaker Current Signal

The breaker current threshold $I_{th} = 1.5$ A is defined based on the maximum normal operating current (±1.25 A) with a 20% safety margin, in the context of the simulation-scale PLC-AMI model.

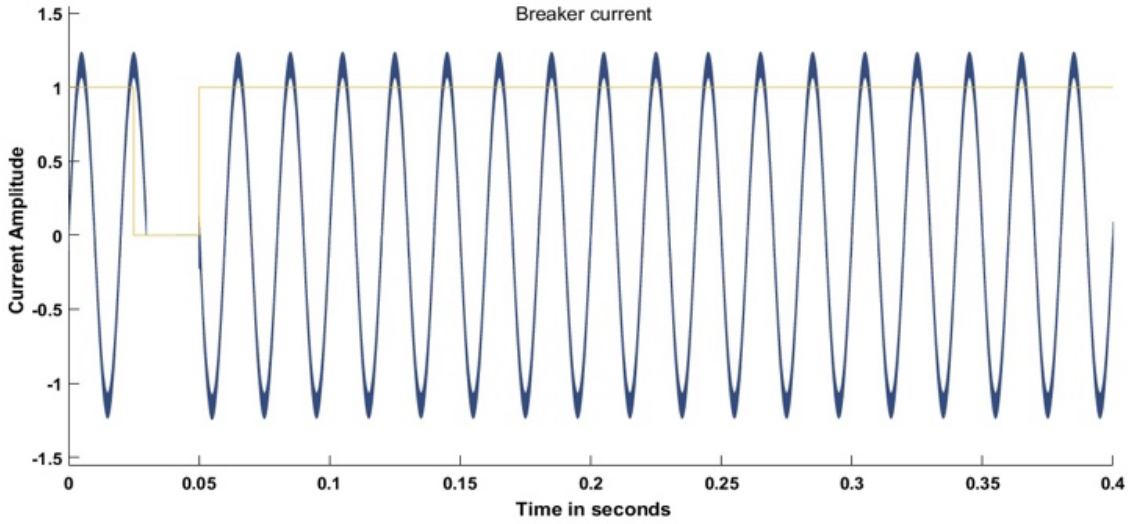
The protection action is triggered when the measured current exceeds I_{th} for a sustained duration beyond transient disturbances. Under normal operating conditions, the system current remains below this threshold, whereas abnormal conditions such as electricity theft result in deviations that exceed the defined operating range.

For different consumer categories, the threshold can be adapted proportionally to the maximum load demand. In general, the adaptive threshold can be expressed by (2):

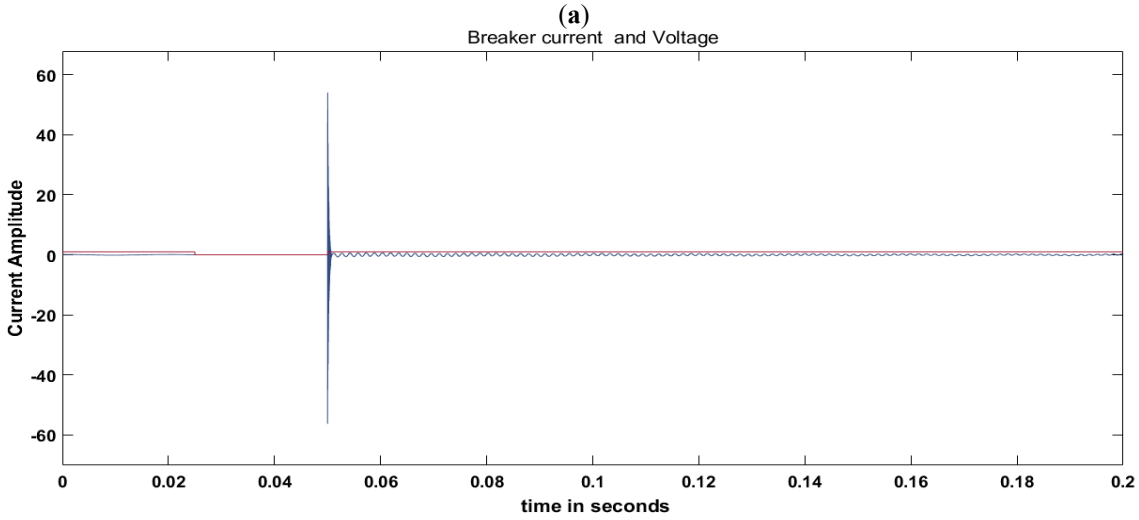
$$I_{th} = k.I_{max} \tag{2}$$

where I_{max} is the maximum expected load current of the consumer, and k is a safety factor ($1.1 \leq k \leq 1.3$) depending on the desired protection sensitivity.

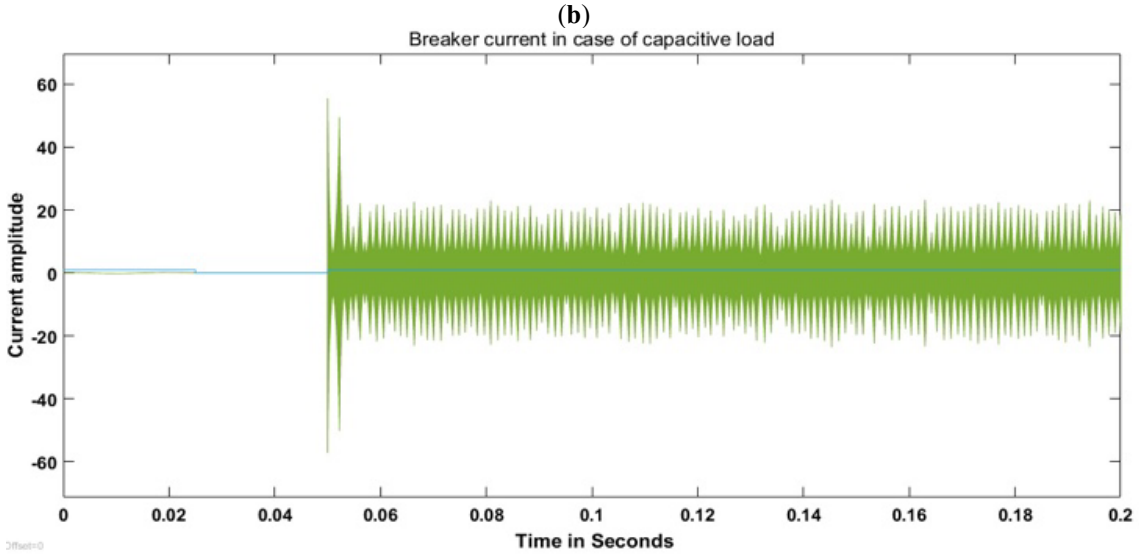
In general, circuit breakers are current-sensing devices, and voltage cannot be accurately measured through them. Since circuit breakers are designed for different current ratings, in the proposed system the breaker current threshold is set according to the maximum load requirement of consumers. The breaker current response clearly reflects the electrical characteristics of the connected load or fault condition. Under normal operating conditions, the current remains stable within a narrow range of approximately [−1.25, 1.25] A, representing balanced operation with minimal distortions, as shown in Figure 10a. When inductive theft loads are connected, the current shifts to about [−1, 1] A, as indicated in Figure 10b, where the phase lag between voltage and current produces additional magnetic flux and increases the system's energy demand. In the case of capacitive theft loads, the current exhibits the widest excursion of approximately [−20, 20] A, caused by harmonics and waveform distortion as current leads the voltage, indicating system instability, as shown in Figure 10c.


Breaker current
Current Amplitude
Time in seconds
1.5
1
0.5
0
-0.5
-1
-1.5
0
0.05
0.1
0.15
0.2
0.25
0.3
0.35
0.4

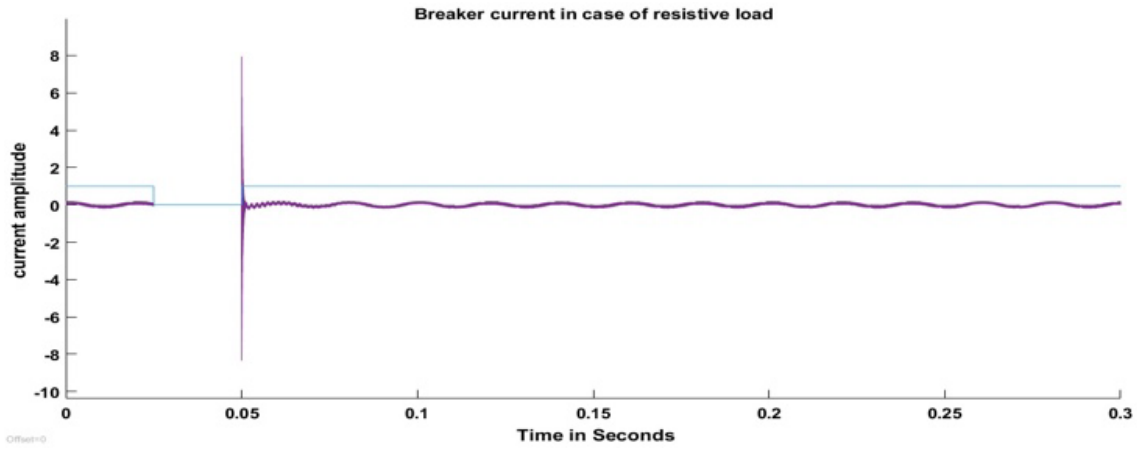
(**a**)


Breaker current and Voltage
Current Amplitude
time in seconds
60
40
20
0
-20
-40
-60
0
0.02
0.04
0.06
0.08
0.1
0.12
0.14
0.16
0.18
0.2

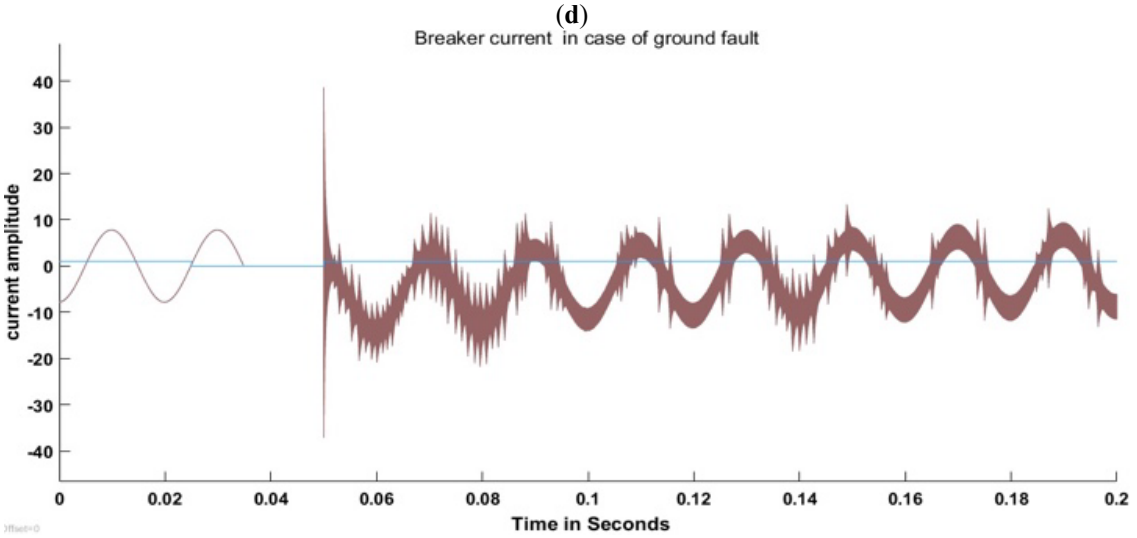
(**b**)


Breaker current in case of capacitive load
Current amplitude
Time in Seconds
60
40
20
0
-20
-40
-60
0
0.02
0.04
0.06
0.08
0.1
0.12
0.14
0.16
0.18
0.2

(**c**)



(**d**)



(**e**)

Figure 10. Analysis of Circuit Breaker's current amplitude for different case (**a**) No Theft Load (**b**) RL Theft Load (**c**) RC Theft Load (**d**) R Theft Load (**e**) Ground Fault.

Resistive theft loads yield the lowest current amplitude within [−0.4, 0.4] A, since the power factor remains unity and voltage and current are in phase, with only transient inrush current observed at the instant of connection, as shown in Figure 10d. For ground fault conditions, the breaker current ranges between [−16, 10] A and displays distinct sinusoidal behavior dominated by the snubber resistance and capacitance, with large excursions that reflect fault severity, as shown in Figure 10e. These results confirm that each load or fault condition produces a unique breaker current signature, which can be effectively utilized for reliable detection and classification of electricity theft and faults in the distribution system. The Table 5 shows circuit breaker's current output across time for different system states.

Table 5. Range of breaker current output for different system states.

System State	Overall Range of Breaker Current Output (A)
No Theft/Fault	[−1.25, 1.25]
RL Theft Load	[−1, 1]
RC Theft Load	[−20, 20]
R Theft Load	[−0.4, 0.4]
Ground Fault	[−16, 10]

In this work, a single-scale residential-type model is considered for study purposes, while adaptive multi-class thresholding (residential, commercial, and industrial loads) is identified as a potential extension of the proposed framework.

3.4. Comparative Analysis against Existing Relevant Methods

As compared to previous work, this study presents a comparative analysis of the proposed detection and protection scheme by incorporating different main load types, as indicated in Table 6.

Table 6. Comparison with existing PLC-based electricity theft detection approaches.

Ref.	Year	Normal Power Signal	High Frequency Carrier Signal	Objective	Career Signal Output (V)	Breaker Current Output (A)
[35]	2014	230 V, 50 Hz	20 V, 150 kHz	Electric Theft Detection	No Theft load: [−7, 7] RL Theft Load: [−3, 3] R Theft Load: [−5, 5]	N/A
[36]	2022	230 V, 50 Hz	20 V, 150 kHz	Electric Theft Detection	No Theft load: [−20, 20] RL Theft Load: [−15, 20]	N/A
This work	2026	230 V, 50 Hz	20 V, 150 kHz	Electric Theft and Ground Fault Detection, and Protection Systems	No Theft load: [−20, 20] RL Theft Load: [−9, 15] RC Theft Load: [−18, 16] R Theft Load: [−19.5, 11] Ground Fault: [−20, 10.5]	No Theft load: [−1.25, 1.25] RL Theft Load: [−1, 1] RC Theft Load: [−20, 20] R Theft Load: [−0.4, 0.4] Ground Fault: [−16, 10]

4. Limitations

The proposed method is performed under controlled simulation conditions and therefore represents an idealized operating environment. In practical deployment, several factors may affect its performance. These include measurement noise, variations in load characteristics, signal attenuation along distribution lines, and non-ideal grid operating conditions. In addition, the current study does not explicitly evaluate sensitivity under extreme operating scenarios or highly dynamic disturbances.

Furthermore, the analysis does not consider hardware imperfections, communication delays, or environmental interference that may arise in real-world PLC-AMI based implementations. The method's robustness under large-scale deployment with heterogeneous network configurations also remains untested. These limitations highlight that the present work focuses on conceptual validation, and further experimental and field-based studies are required to fully assess practical applicability.

Although the proposed model is developed on a single-phase 100 km distribution network for conceptual demonstration, the underlying principle can be extended to three-phase distribution systems. In a practical three-phase network, the same carrier signal injection and measurement concept can be applied to each phase independently or through phase-wise multiplexing techniques. However, extending the proposed approach to three-phase systems introduces additional challenges. These include inter-phase coupling effects, increased noise levels, unbalanced loading conditions, and more complex signal propagation behavior. Furthermore, variations in network topology such as radial, ring, and meshed configurations, along with long-distance signal attenuation, may impact carrier signal integrity and detection reliability. To address these challenges, practical implementations may require phase-wise signal separation strategies, adaptive filtering techniques, and the use of localized data concentrators for improved signal processing and scalability.

5. Impact of Distributed Generation Penetration

In modern distribution networks, the increasing penetration of user-side distributed generation (e.g., rooftop photovoltaic (PV) systems and small-scale energy storage units) significantly alters the voltage and current characteristics of the grid. These resources introduce bidirectional power flow, increased variability, and dynamic changes in load profiles, which may affect conventional power system measurements.

With the proposed PLC-AMI based electricity theft detection framework, such distributed generation may primarily influence the low-frequency operating conditions of the network. However, the detection mechanism relies on the behavior of a high-frequency carrier signal, which is largely decoupled from fundamental frequency variations. Therefore, the direct impact of PV and energy storage integration on carrier signal propagation is expected to be limited.

Nevertheless, high penetration of distributed energy resources may introduce additional variability and noise in practical deployment environments, which could affect overall system robustness.

6. Conclusions

This work presents a simple yet realistic technique for detecting, monitoring, and mitigating electricity theft using a PLC-AMI integrated approach. High-frequency, low-amplitude signals are transmitted through the power network to detect theft and protect against system faults, while also analyzing load variations, consumer load types, and frequency deviations. In normal conditions, the carrier signal remains symmetric (–20 V to 20 V), whereas different theft loads (RL, RC, R) and ground faults distort its amplitude, mainly suppressing the positive swing. At 50 Hz, the carrier signal shows a wider symmetric range (–19 V to 19 V), indicating stable operation, while at 60 Hz the narrower range (–17 V to 16 V) reduces sensitivity for abnormality detection.

Protection devices, such as circuit breakers, current analysis further confirms distinct patterns for each case: stable under normal operation, shifted for RL loads, widely distorted for RC loads, minimal for resistive loads, and showing large excursions ground faults. These distinctive patterns enable reliable detection and classification of electricity theft and faults. The results show the effectiveness, practicality, and potential of the proposed PLC-AMI based framework for secure and sustainable distribution system operation.

In future, the integration of energy storage systems can be explored to enhance the resilience of electricity theft detection and protection schemes. Although this study does not model or experimentally evaluate energy storage, future work may investigate how storage units can support critical legitimate loads after theft or fault events, particularly when supply is intentionally disconnected. Such analysis would enable a deeper understanding of how coordinated control between detection mechanisms and storage resources can maintain service continuity, improve operational stability, and strengthen overall distribution system reliability. More realistic theft scenarios, including dynamic load profiles and advanced bypass methods, will be investigated in future work to further evaluate the robustness of the proposed approach.

Author Contributions

Conceptualization, S.H. and A.M.; methodology, S.H., U.J., N.Q. and A.M.; software, S.H. and U.J.; analysis, S.H. and U.J.; investigation, S.H., U.J., N.Q. and. A.M.; writing—original draft preparation, S.H., U.J. and. A.M.; writing—review and editing, S.H., U.J. and A.M.; supervision, A.M. All authors have read and agreed to the published version of the manuscript.

Funding

This research received no external funding.

Institutional Review Board Statement

Not applicable.

Informed Consent Statement

Not applicable.

Data Availability Statement

The data supporting the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare no conflict of interest.

Use of AI and AI-Assisted Technologies

During the preparation of this work, the author(s) used ChatGPT to improve the flow of the manuscript. After using this tool, the author(s) reviewed and edited the content as needed and take(s) full responsibility for the content of the published article.

References

1. IEA. *Electricity Mid-Year Update 2025*; IEA: Paris, France, 2025. Available online: https://www.iea.org/reports/electricity-mid-year-update-2025 (accessed on 1 November 2025).
2. Tian, G.; Khan, I. Impact of Energy End-Uses and Efficiency Indicators on the Environmental Policy Stringency Index. *Energy* **2025**, *326*, 136232.
3. Sadiq, E.H.; Antar, R.K. Minimizing Power Losses in Distribution Networks: A Comprehensive Review. *Chin. J. Electr. Eng.* **2024**, *10*, 20–36.
4. Jamil, U.; Amin, A.; Mahmood, A. A Comparative Study of Control Techniques for Power Loss Minimization in a Distribution Network. In Proceedings of the 2018 1st International Conference on Power, Energy and Smart Grid (ICPESG), Mirpur Azad Kashmir, Pakistan, 9–10 April 2018; pp. 1–5.
5. Díaz, S.; Moreno Rocha, C.M.; Berdugo Sarmiento, K.M.; et al. Electric Power Losses in Distribution Networks. *Turk. J. Comput. Math. Educ.* **2021**, *12*, 581–591.
6. Niste, D.F.; Tîrnovan, R.; Pavel, S.; et al. Electricity Losses in Focus: Detection and Reduction Strategies—State of the Art. *Appl. Sci.* **2025**, *15*, 7.
7. Kankonde, P.; Bokoro, P. Bridging the Energy Divide: An Analysis of the Socioeconomic and Technical Factors Influencing Electricity Theft in Kinshasa, DR Congo. *Energies* **2025**, *18*, 3566.
8. Kasumba, D.; Nkulu, G.; Diambomba, H.; et al. Electricity Theft and Its Impact on Quality of Service in Lubumbashi, DR Congo. *Energy Eng.* **2025**, *122*, 2401.
9. Resende, D.; Richter, G.; Castello Branco Sant'Anna, M.; et al. Pricing and Informality: Evidence from Energy Theft in Brazil. 2025. Available online: https://ssrn.com/abstract=5126274 (accessed on 20 May 2026).
10. Ndulaka, J.S.; Nwele, E.O.; Olubiwe, M.; et al. Anti-Electricity Theft Model for Sustainable Economic Development in Nigeria. *Int. J. Electr. Energy Power Syst. Eng.* **2025**, *8*, 128–141.
11. Yakubu, O.; Babu, N.; Adjei, O. Electricity Theft: Analysis of the Underlying Contributory Factors in Ghana. *Energy Policy* **2018**, *123*, 611–618.
12. Mushtaq, I.; Mirza, F.M. The Impact of Services Quality on Electricity Theft Reduction: An Empirical Analysis of Electricity Distribution Utilities in Pakistan. *Lahore J. Econ.* **2023**, *28*, 88–114.
13. Gupta, A.K.; Routray, A.; Naikan, V.A. Detection of Power Theft in Low Voltage Distribution Systems: A Review from the Indian Perspective. *IETE J. Res.* **2022**, *68*, 4180–4197.
14. Saiam, M.; Salimullah, S.M.; Akther, M.S.; et al. Reducing Electricity Theft by Low Frequency Control Scheme in Bangladesh. In Proceedings of the 2020 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI), Dhaka, Bangladesh, 19–20 December 2020; pp. 1–4.
15. Asfu, W.T. Automatic Power Theft Detection and Protection on Distribution Line. *Glob. Sci. J.* **2020**, *8*, 7.
16. Thangalakshmi, S. Power Theft Prevention in Distribution System Using Smart Devices. *Int. J. Appl. Eng. Res.* **2015**, *10*, 30841–30845.
17. Jiyane-Tshikomba, S. Technical Analysis Mitigation of Electricity Theft for Domestic and Commercial End Users. Ph.D. Thesis, Durban University of Technology, Durban, South Africa, 2019.
18. Vani, A.V.; Yasaswini, V.; Boppa, J.S.G.; Prakash, S.R. Power Theft Detection in Distribution Lines. *Int. J. Innov. Res. Eng.* **2025**, *6*, 9–12.
19. Ercan, S.U. Power Line Communication: Revolutionizing Data Transfer over Electrical Distribution Networks. *Eng. Sci. Technol. Int. J.* **2024**, *52*, 101680.
20. Casella, I.R.; Anpalagan, A. *Power Line Communication Systems for Smart Grids*; IET: London, UK, 2024.
21. Kim, S.; Sun, Y., Lee, S.; et al. Data-Driven Approaches for Energy Theft Detection: A Comprehensive Review. *Energies* **2024**, *17*, 3057.
22. Xia, X.; Xiao, Y.; Liang, W.; et al. Detection Methods in Smart Meters for Electricity Thefts: A Survey. *Proc. IEEE* **2022**, *110*, 273–319.
23. Salinas, S.A.; Li, P. Privacy-Preserving Energy Theft Detection in Microgrids: A State Estimation Approach. *IEEE Trans. Power Syst.* **2015**, *31*, 883–894.
24. Tariq, M.; Poor, H.V. Electricity Theft Detection and Localization in Grid-Tied Microgrids. *IEEE Trans. Smart Grid* **2016**, *9*, 1920–1929.
25. Wen, M.; Yao, D.; Li, B.; et al. State Estimation Based Energy Theft Detection Scheme with Privacy Preservation in Smart Grid. In Proceedings of the 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018; pp. 1–6.
26. Wong, H.L.; Tan, C.K.; Tan, W.-N.; et al. Energy Theft Identification: A State Estimation Model for Partial Meter Bypass. *IEEE Access* **2025**, *13*, 121412–121431.

27. Saqib, S.M.; Mazhar, T.; Iqbal, M.; et al. Utilizing Machine Learning Ensembles for Effective Electricity Theft Detection. *Energy Explor. Exploit.* **2026**, *44*, 526–553.
28. Saqib, S.M.; Mazhar, T.; Iqbal, M.; et al. Enhancing Electricity Theft Detection with ADASYN-Enhanced Machine Learning Models. *Electr. Eng.* **2025**, *107*, 10525–10542.
29. Yang, L.; Feng, C.; Shen, T.; et al. Application of a Novel Deep Learning Method for Electricity Theft Detection Based on Explainable Artificial Intelligence. *AIP Adv.* **2026**, *16*, 1.
30. Qin, W.; Ding, Y.; Luo, X. A Robust Approach to Electricity Theft Detection via Tensor Representation-Driven Contrastive Distillation. *IEEE Trans. Ind. Inform.* **2026**, *22*, 4561–4570.
31. Tursunboev, J.; Palakonda, V.; Kang, J.-M. Multi-Objective Evolutionary Hybrid Deep Learning for Energy Theft Detection. *Appl. Energy* **2024**, *363*, 122847.
32. Sung, M.; Palakonda, V.; Kim, I.-M.; et al. Deco-mesc: Deep Compression-Based Memory-Constrained Split Computing Framework for Cooperative Inference of Neural Network. *IEEE Trans. Veh. Technol.* **2025**, *74*, 13319–13324.
33. Wong, J.C.Y.; Blankenship, B.; Urpelainen, J.; et al. Perceptions and Acceptability of Electricity Theft: Towards Better Public Service Provision. *World Dev.* **2021**, *140*, 105301.
34. Ali, S.; Yongzhi, M.; Ali, W. Prevention and Detection of Electricity Theft of Distribution Network. *Sustainability* **2023**, *15*, 4868.
35. Christopher, A.V.; Swaminathan, G.; Subramanian, M.; et al. Distribution Line Monitoring System for the Detection of Power Theft Using Power Line Communication. In Proceedings of the 2014 IEEE Conference on Energy Conversion (CENCON), Johor Bahru, Malaysia, 13–14 October 2014; pp. 55–60.
36. Awasthi, M.; Kumar, A.; Kumar, D.; et al. Electric Power System Monitoring and Theft Detection Using Power Line Communication. *Int. J. Eng. Sci. Inf. Technol.* **2022**, *2*, 79–85.