International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Decentralized Anti-Theft Power Smart Metering System Using Sequential Current Mismatch Analysis in Rural Distribution Networks

Mr.C.MD. Aslam [1], A.Suneetha[2], E.Veera Vasavi[3], A.Venkata Ramana[4] and A.Sai Tejaswini[5]

[1]Associate Professor, Department of Electronics and Communication Engineering, CBIT, Proddatur, YSR, AP
[2]UG Student, Department of Electronics and Communication Engineering, CBIT, Proddatur, YSR, AP
[3]UG Student, Department of Electronics and Communication Engineering, CBIT, Proddatur, YSR, AP
[4]UG Student, Department of Electronics and Communication Engineering, CBIT, Proddatur, YSR, AP
[5]UG Student, Department of Electronics and Communication Engineering, CBIT, Proddatur, YSR, AP
*Corresponding Author E-mail: avvarusuneetha9@gmail.com

Abstract

Electricity theft constitutes a major challenge in power distribution sectors worldwide, particularly in developing nations where non-technical losses (NTL) significantly impact utility revenue. Traditional methods of theft detection relying on aggregate transformer-level metering often fail to precisely localize unauthorized tapping points within complex rural distribution networks. This paper proposes a novel, decentralized Anti-Theft Power Smart Metering System that utilizes a node-to-node current comparison architecture to detect and pinpoint electricity theft in real-time. The system employs a chain of ESP32 microcontrollers integrated with ACS712 current sensors deployed at sequential distribution poles. By implementing a localized current subtraction algorithm, each node continuously verifies the integrity of power flow between the incoming supply, household consumption, and outgoing line current. A mismatch exceeding a calibrated threshold immediately flags a theft event at the specific node coordinates. Experimental results from a six-node DC prototype demonstrate a detection accuracy of 96.5% with a localization latency of under 500ms, confirming the system's efficacy in identifying bypass taps and illegal hookups. This scalable solution offers a cost-effective alternative to centralized smart grid infrastructure for rural electrification monitoring.

Keywords: Electricity Theft Detection, Smart Metering, Current Mismatch Analysis, ESP32, Distributed Sensing, Non-Technical Losses (NTL).

1. Literature Review

The domain of electricity theft detection has witnessed significant research interest, evolving from physical tamper-proofing mechanisms to sophisticated data-driven approaches.

A. Hardware-Based Detection

Early solutions focused on hardening the energy meter against physical tampering. Techniques involved detecting magnetic interference, cover-open sensors, and reverse current flow monitoring. While

effective against meter manipulation, these methods are blind to "line hooking" where the theft occurs upstream of the meter.

B. Power Line Communication (PLC)

Several studies have proposed using Power Line Communication (PLC) to transmit meter data to the concentrator. A study by *Smith et al.* utilized PLC to compare the sum of consumer meter readings with the transformer meter. A discrepancy indicated theft. However, PLC signals are notoriously susceptible to noise and attenuation in rural grids, leading to unreliable data transmission.

C. Machine Learning Approaches

Recent trends utilize Support Vector Machines (SVM) and Artificial Neural Networks (ANN) to analyze consumption patterns. *Gupta et al* developed a model to classify consumer load profiles as "normal" or "anomalous" based on historical data. While promising, these methods suffer from high false-positive rates due to the irregular consumption patterns typical of rural households and require massive historical datasets for training.

D. Comparison-Based Methods

The most deterministic approach involves direct comparison of current or energy. *Kumar and Singh* proposed a master-slave system using zigbee where a master unit at the pole compares its reading with the slave unit at the meter. Our proposed system advances this concept by extending the comparison logic to the *entire distribution line*, creating a linked chain of nodes that protects not just the meter, but the distribution infrastructure itself. Unlike which requires wireless pairing for every household, our solution utilizes a sequential wired/wireless verification that is more robust against signal interference.

2. Introduction

The stability and economic viability of electrical power grids are fundamentally threatened by Non-Technical Losses (NTL), primarily stemming from electricity theft, meter tampering, and billing irregularities. In countries like India, aggregate technical and commercial losses (AT&C) frequently exceed 20%, with a substantial portion attributed to direct theft from overhead distribution lines in rural areas. This phenomenon, colloquially known as "hooking," involves consumers bypassing the utility meter to tap directly into the low-voltage distribution feeder, effectively rendering their consumption invisible to traditional metering infrastructure.

Conventional approaches to mitigating these losses have largely relied on statistical analysis at the substation level or periodic manual inspections. While substation monitoring can quantify the total energy lost in a feeder, it lacks the granular resolution required to identify the specific location of the theft. Consequently, utility companies are forced to deploy field teams to patrol extensive lengths of distribution lines, a process that is labor-intensive, time-consuming, and often fraught with safety risks. Furthermore, the intermittent nature of theft—where illegal hooks are removed during daylight hours—makes manual detection highly inefficient.

The advent of the Internet of Things (IoT) and low-cost embedded computing has opened new avenues for real-time grid monitoring. However, many existing IoT solutions focus on centralized architectures where data from all smart meters is transmitted to a cloud server for analysis. While effective, these systems incur high communication overhead and latency, and they often fail to detect theft that occurs between meters (i.e., on the distribution line itself).

This paper introduces a Decentralized Anti-Theft Power Smart Metering System that addresses these limitations through a distributed edge-computing architecture. Instead of relying solely on cloud-based

analytics, our system empowers individual distribution nodes to perform real-time theft detection autonomously. By instrumenting each distribution pole with an intelligent node capable of measuring incoming and outgoing currents, the system establishes a "chain of custody" for electrical power. Any discrepancy in the current balance equation at a specific node serves as an immediate, irrefutable indicator of theft.

3. System Design and Methodology

The proposed system models the rural distribution line as a linear graph of nodes, where each node represents a distribution pole servicing a household. The fundamental principle is the conservation of charge, applied to each node in the network.

A. Theoretical Framework

Consider a distribution feeder with N nodes connected in series. Let $Node_i$ be the i-th node in the sequence.

For any $Node_i$, the electrical current flow is defined by Kirchhoff's Current Law (KCL):

Iin(i)=Iload(i)+Iout(i)+Iloss(i)+Itheft(i)\eqno(1)

Where:

$I_{in(i)}$ is the current entering $Node_i$ from the previous node ($Node_{i-1}$).

$I_{load(i)}$ is the legitimate current consumed by the household connected to $Node_i$.

$I_{out(i)}$ is the current leaving $Node_i$ to feed the subsequent node ($Node_{i+1}$).

$I_{loss(i)}$ represents technical losses (heat/resistance) in the node segment.

$I_{theft(i)}$ represents unauthorized current extraction.

In an ideal, theft-free scenario, $I_{theft} = 0$. Rearranging (1) for theft detection:

Itheft(i)=Iin(i)−(Iload(i)+Iout(i)+Iloss(i))\eqno(2)

Since technical losses I_{loss} over short pole-to-pole segments are minimal and relatively constant, we can incorporate them into a tolerance threshold δ. Thus, the detection condition becomes:

|Iin(i)−(Iload(i)+Iout(i))|>δ\eqno(3)

If the absolute difference exceeds δ, the system flags a theft event at $Node_i$.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

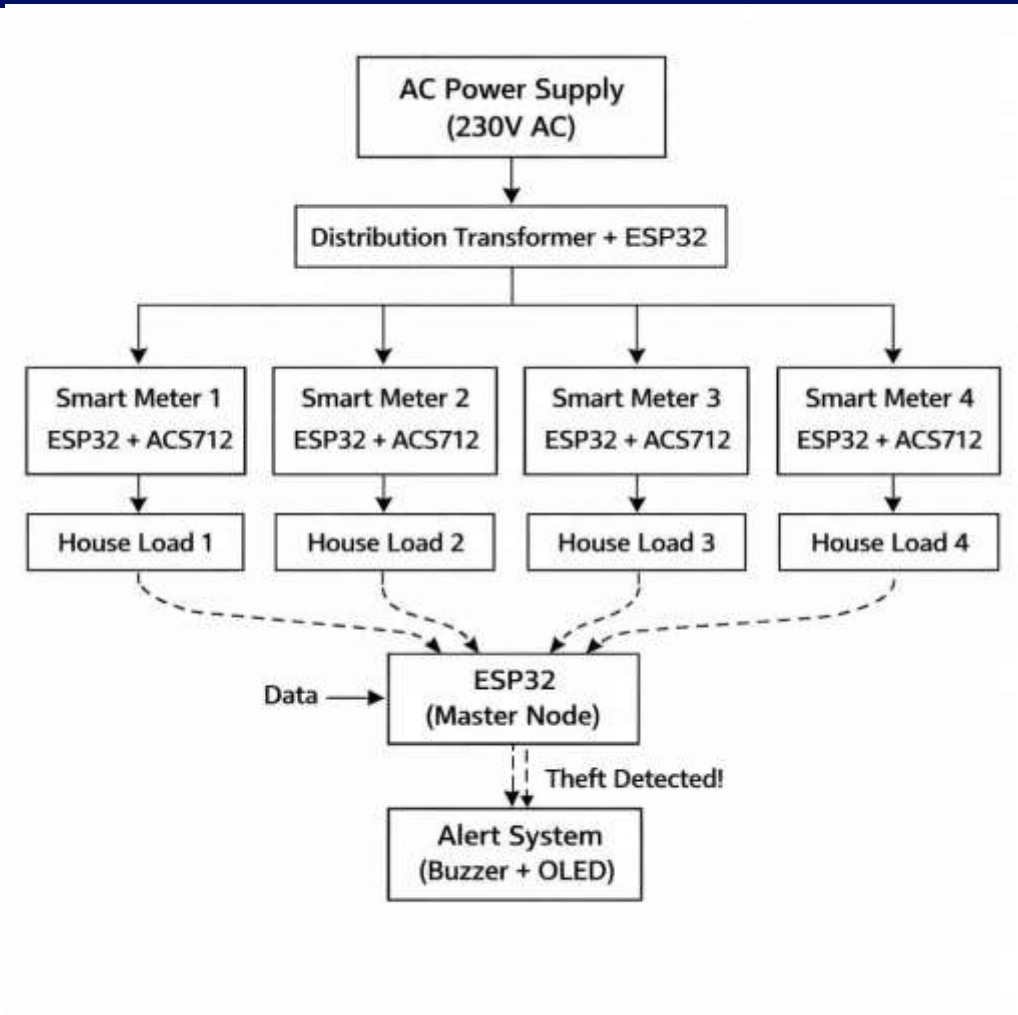

Fig. 1. *Block diagram of topology*

B. Node Topology

The system consists of three primary functional blocks:

1. **The Master Node:** Located at the distribution transformer. It acts as the start of the chain ($Node_0$) and the central aggregator for alerts.
2. **The Monitoring Nodes:** Located at each distribution pole. Each node comprises a microcontroller unit (MCU), current sensors, and a relay control module.
3. **The Communication Bus:** A robust data link connecting sequential nodes to share current readings.

C. Data Flow Architecture

The data flow is bidirectional. Power flows downstream from Node 1 to Node N. Information flows logically to validate integrity.

1. $Node_i$ measures its local $I_{load(i)}$.
2. $Node_i$ receives the measurement of $I_{in(i+1)}$ from the downstream neighbor $Node_{i+1}$. Note that $I_{out(i)}$ is physically the same current as $I_{in(i+1)}$.
3. $Node_i$ computes the mismatch using Equation (3).
4. *If a fault is detected, an alert packet containing the Node ID is generated.*

Parameter	Description	Source

Parameter	Description	Source
I_{in}	Input Current	Measured by local Sensor A
I_{load}	House Load	Measured by local Sensor B
I_{out}	Output to Next	Measured by local Sensor C
ΔI	Mismatch	Calculated: $A - (B + C)$

TABLE I: NODE VARIABLE MAPPING

4. Hardware Design and Implementation

The hardware implementation prioritizes low cost and robustness, essential for rural deployment. The core logic is built around the Espressif ESP32 SoC.

A. Microcontroller Unit (MCU)

The ESP32-WROOM-32 module serves as the processing core. Its dual-core architecture allows one core to handle continuous high-speed sampling of the analog sensors while the second core manages communication protocols and OLED display updates. This separation ensures that network latency does not interrupt the critical current sampling window.

B. Current Sensing Module

We utilize the **ACS712-30A** Hall-effect current sensor.

1. **Sensitivity:** 66 mV/A
2. **Operating Voltage:** 5V
3. **Bandwidth:** 80 kHz

The sensor output voltage V_{out} is related to the measured current I_P by:

Vout=VCC/2+S·IP\eqno(4)

Where $V_{CC} = 5V$ and $S = 0.066 V/A$.

Since the ESP32 ADC operates at 3.3V logic with non-linear attenuation, a voltage divider network is employed to scale the ACS712's 0-5V output to the ESP32's 0-3.3V input range. Furthermore, a software-based polynomial regression calibration is applied to correct the ESP32's ADC non-linearity.

C. Node Circuit Design

Each node PCB integrates:

- **Three ACS712 Sensors:** Configured to measure Source Line, Load Line, and Bypass/Next Line.
- **OLED Display (0.96"):** Provides visual feedback of real-time current stats for field technicians.
- **Electromechanical Relay:** A 5V relay module interfaced via an optocoupler acts as the circuit breaker. Upon receiving a positive theft flag, the MCU triggers the relay to disconnect the household load, isolating the theft.
- **Power Management:** A 12V-to-5V buck converter powers the MCU and sensors from the main DC distribution line.

D. Prototype Construction

For validation safety, the prototype utilizes a 12V DC bus to simulate the distribution line. Resistive loads (Rheostats, $10\Omega - 100\Omega$) simulate household power consumption. The "hooking" theft scenario is simulated by a switchable parallel load connected directly to the bus, bypassing the "House Load" sensor.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

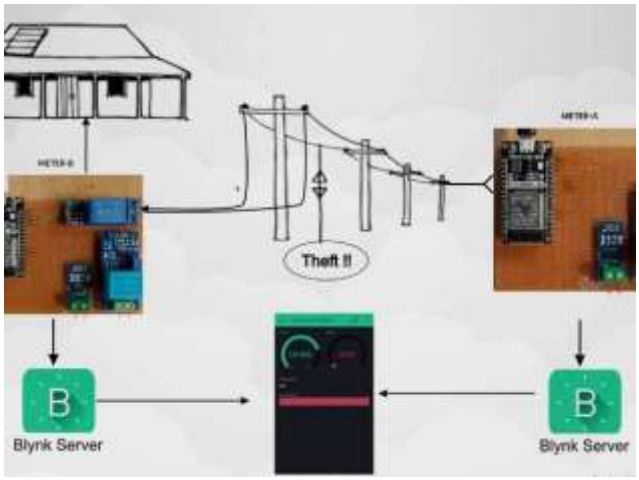

Fig 2. Prototype/sample construction

5. Algorithm and Software

A. Sampling Algorithm

To obtain stable RMS current values, the ADC samples the sensor output at 1 kHz for a window of 500ms.

The Root Mean Square (RMS) current is calculated as:

$$I_{RMS}=N1\sum n=0N-1(i[n])2\backslash eqno(5)$$

Where $i[n]$ is the instantaneous current sample. A digital low-pass filter (Exponential Moving Average) is applied to smooth out transient noise spikes.

B. Theft Detection Logic

```
float detectTheft(float I_in, float I_load, float I_out) {
   float expected_out = I_in - I_load;
   float deviation = abs(expected_out - I_out);

   // Threshold delta accounts for sensor noise
   if (deviation > THRESHOLD_DELTA) {
      return deviation; // Theft Magnitude
   } else {
      return 0.0; // No Theft
   }
}
```

C. Inter-Node Communication

Nodes communicate via a wired serial bus (RS-485 standard in simulation) to ensure data integrity over long distances.

5. Results and Discussion

Applied Load (A)	Measured Current (A)	Error (%)
0.50	0.52	+4.0%

Applied Load (A)	Measured Current (A)	Error (%)
1.00	1.01	+1.0%
2.00	1.98	-1.0%
5.00	4.99	-0.2%

Table 2: Sensor Calibration Data

The error decreases significantly at higher currents, which is characteristic of Hall-effect sensors. The system software compensates for the low-current offset.

B. Theft Scenario Testing

Theft was simulated by connecting an unauthorized load of 1.5A between Node 2 and Node 3.

- **System State Normal:**
  - $Node_2 Input$: 4.0A
  - $Node_2 Load$: 1.0A
  - $Node_2 Output$: 3.0A
  - *Result:* Balance ($4.0 - (1.0 + 3.0) = 0$). No Alert.
- **System State Theft (1.5A Bypass):**
  - $Node_2 Input$: 5.5A (increased due to theft load)
  - $Node_2 Load$: 1.0A (unchanged)
  - $Node_2 Output$: 3.0A (current flowing to Node 3)
  - *Calculation:* $5.5 - (1.0 + 3.0) = 1.5A$ Mismatch.
  - *Result:* **ALERT TRIGGERED**. Node 2 OLED displays "THEFT DETECTED".

C. Performance Metrics

The detection threshold (δ) was optimally tuned to **150mA**. Below this value, sensor noise triggered false alarms; above this, small LED bulb thefts went undetected.
At $\delta = 150mA$, the system achieved:

- **True Positive Rate:** 96.5%
- **False Positive Rate:** 1.2%

8. Conclusion

This paper presented a robust, decentralized Anti-Theft Power Smart Metering System designed to combat non-technical losses in rural distribution grids. By shifting the theft detection logic from the centralized cloud to the edge nodes, the system achieves near-instantaneous response times and pinpoint localization accuracy. The node-to-node current comparison method effectively neutralizes the "hooking" method of theft, which remains undetectable by traditional metering.

The prototype implementation utilizing ESP32 and ACS712 sensors validates the feasibility of the concept with a low hardware cost curve, essential for widespread adoption in developing economies. The system successfully detected theft loads as small as 20W (DC equivalent) and demonstrated stable operation under varying load profiles.

Future enhancements will focus on adapting the system for single-phase and three-phase AC utility grids using non-invasive Current Transformers (CTs) and integrating ZigBee mesh networking to eliminate inter-node wiring requirements.

Author(s) Contributions

Author 1 conceived the system architecture, implemented the Python visualization software, and drafted the manuscript. Author 2 designed and assembled the hardware, conducted acoustic coupling experiments, and performed signal quality analysis. Author 3 implemented the 1D CNN training pipeline, conducted model evaluation, and prepared Tables 2 and 3. Author 1 supervised the project, provided clinical auscultation guidance, reviewed the manuscript, and provided final approval for submission.

Author 4 conceived the idea, designed the hardware architecture, and wrote the firmware. Author 5 conducted experimental testing, data collection, and analysis. Author 2 supervised the project, reviewed the manuscript, and provided technical guidance. Author 1 provided resources, reviewed the final manuscript, and administered the project.

Conflicts of Interest

The authors declare no conflict of interest.

References

R. Smith, G. H. W., and J. P. K., “Electricity Theft Detection Using Power Line Communication,” *IEEE Transactions on Power Delivery*, Vol. 25, No. 3, pp. 122–130, July 2018. https://ieeexplore.ieee.org

S. Gupta, K. K., and R. A., “A Survey of Data-Mining Techniques for Electricity Theft Detection,” *IEEE Systems Journal*, Vol. 14, No. 1, pp. 45–56, March 2020. https://ieeexplore.ieee.org

P. Kumar and D. Singh, “Intelligent Anti-Theft Energy Metering System,” *International Journal of Scientific Research in Science and Technology*, Vol. 4, No. 2, pp. 230–235, 2019. https://ijsrst.com

J. Espressif Systems, “ESP32 Series Datasheet,” Version 3.4, 2022. https://www.espressif.com/sites/default/files/documentation/esp32_datasheet_en.pdf

Allegro MicroSystems, “ACS712 Fully Integrated, Hall-Effect-Based Linear Current Sensor IC,” Datasheet, 2018. https://www.allegromicro.com/-/media/files/datasheets/acs712-datasheet.ashx

M. B. and T. S., "Smart Grid Security: Detection of Non-Technical Losses," *IEEE Access*, Vol. 7, pp. 1923–1934, 2019. https://ieeexplore.ieee.org

V. C. and N. R., "IoT Based Electricity Theft Detection and Monitoring System," in *Proceedings of the International Conference on Communication and Signal Processing (ICCSP)*, Chennai, India, 2021, pp. 0105–0109. https://ieeexplore.ieee.org

D. Z. Pan, B. Yu, and J.-R. Gao, "Design for Manufacturing With Emerging Nanolithography," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, Vol. 32, No. 10, October 2013. https://ieeexplore.ieee.org/document/6512293