

Anti-Electricity Theft Model for Sustainable Economic Development in Nigeria

Josephine Sandra Ndulaka¹, Emmanuel Onyekachi Nwele^{2*}, Matthew Olubiwe³, Isdore Onyema Akwukwaegbu⁴

^{1,2,3,4}Department of Electrical Electronic Engineering, School of Electrical Systems Engineering and Technology, Federal University of Technology, Owerri, Nigeria.

¹sandrandulaka@gmail.com, ²nweleemmanuel.20214329818@futo.edu.ng,

³matthew.olubiwe@futo.edu.ng, ⁴isdore.akwukwaegbu@futo.edu.ng,

*Corresponding author, nweleemmanuel.20214329818@futo.edu.ng

Abstract— In Nigeria today, as in most parts of the world, Power Distribution Companies face several challenges, among which is electricity theft. Electricity theft is simply the practice of bypassing, stealing, or utilizing electricity without payment. The most common forms of electricity theft in Nigeria, for instance, are meter bypass and illegal hook connections by consumers who attempt to defraud the system by not paying for power used in their households and businesses. A schematic method is adopted to mitigate this pervasive issue, ensuring that authorities have real-time knowledge when consumers engage in illicit practices. The designed system hybridizes technical and non-technical methods, integrating a smart resistance module capable of controlling both technical and non-technical losses caused by consumers, thereby enhancing the scheme's sensitivity. This system incorporates a feedback mechanism designed for easy communication to the control room, which will inject third harmonics into the consumer's line immediately upon detection of meter bypass. Simulation was conducted using Simulink MATLAB, and the results obtained indicated that the system offers significant improvement compared to approaches that tackle either non-technical or technical aspects independently.

Keywords: *Electricity Theft Mitigation, Harmonic Injection, Smart Resistance, Technical and Non-technical Loss.*



This work is licensed under a [CC BY-SA](https://creativecommons.org/licenses/by-nc/4.0/). Copyright ©2025 by Author. Published by Universitas Riau.

INTRODUCTION

Electricity is a cornerstone of any progressive economy. However, electricity theft poses a significant threat to power systems globally, and this problem is particularly acute in Nigeria. Electricity theft is an age-old problem that has been plaguing the power industries for a very long time [1]. Despite Nigeria's reputation as the "giant of Africa," persistent power sector inefficiencies have severely hindered its economic potential and made it an unattractive environment for investment. Electricity theft contributed largely to the power supply crisis in Nigeria, which has been a longstanding complication in the Nigerian Electricity Supply Industry

(NESI). The electricity being generated in the country falls short of the capacity needed to power the whole country [2].

Electricity theft negatively affects the entire value chain and remains a scourge to the power sector. While its impact is borne greatly by the Distribution Companies (DisCos), the overall adverse effect of electricity theft affects the value chain in totality [3]. Nevertheless, the ripple effect extends across the entire electricity sector, compromising reliability and sustainability. This endemic issue is particularly pervasive in Nigeria and other developing nations. This has hindered the reliability and sustainability of electricity supply in these countries, in turn stalling economic growth [4]. Globally, electricity theft manifests at varying levels, with developing countries recording some of the highest theft-related losses. According to [5], emerging markets such as India, Nigeria, Brazil, and South Africa suffer from significant electricity theft, with estimated Transmission and Distribution (T&D) losses reaching 20-40% of total energy distribution. In India, theft-related losses are part of a broader problem of inefficiency in power distribution, with transmission losses of approximately 21.4% [6]. Similarly, Nigeria has long struggled with high levels of electricity theft due to inadequate metering systems and a lack of reliable enforcement. According to the Nigerian Electricity Regulatory Commission (NERC), non-technical losses constitute over 40% of the total distributed energy [7]. These rates are similar in Brazil, where annual losses due to theft exceed \$4 billion [8]. The two types of energy losses in the electrical power system are the technical loss (TL), which occurs naturally, as a result of dissipation of energy in the power transmission and distribution equipment, and the non-technical loss (NTL), which occurs owing to actions that are external to the electrical power system [9]. In many cases, the tendency of electricity theft comes from the will of not paying for the utility. However, some popular methods of stealing electricity in Nigeria are: Feeder Bypass, Meter Tampering and Fishing pole connection. Meter tampering is rarely found among poor households because it is technically sophisticated and usually requires some electrical wiring knowledge. This tampering can be detected only by an audit on the premises or by discrepancies in the electricity bill [10]. According to the National Electricity Regulatory Commission (NERC), over 25 percent of the total energy wheeled by the Transmission Company of Nigeria (TCN) to electricity Distribution Companies (Discos) is lost to theft and technical inefficiency [11].

Recent developments in smart grid technology emphasize not only theft detection but also proactive grid monitoring and control. For instance, the use of virtual synchronous generators has demonstrated how intelligent control systems can stabilize and enhance power delivery [14]. Building on such principles, this study introduces a model that integrates both detection (via smart resistance) and deterrence (via harmonic injection) to address the widespread issue of electricity theft in Nigeria. To combat electricity theft, this research proposes a comprehensive anti-theft model using smart resistance for theft detection and third harmonic injection for theft mitigation. Electricity theft is a global issue that has prompted significant research efforts. Several studies have focused on the detection of Non-Technical Losses (NTLs) through data analytics, smart metering, and machine learning [9], [12], [16]. [12] leveraged machine learning with smart meter data to improve theft detection, while [16] proposed a hybrid model integrating multiple ML algorithms for enhanced performance. [9] proposed a technique using load profiles and consumption data to identify anomalies in modern distribution systems. [4] reviewed solutions such as artificial intelligence, state estimation, and advanced metering infrastructure (AMI), highlighting the growing role of smart systems in theft detection. However, these approaches often lack proactive mitigation mechanisms. [13] further extended detection capabilities through harmonic distortion analysis, aligning closely with this study's focus on waveform-based disruption. This study distinguishes itself by integrating real-time detection (via smart resistance) with active deterrence (via third harmonic injection). The novelty lies in combining impedance-based monitoring with waveform distortion, offering a dual-layered security approach not commonly addressed in prior work. This model uniquely combines smart resistance monitoring with harmonic distortion to both

130

detect and disrupt theft. Unlike conventional systems that only detect anomalies, this system penalizes unauthorized users by corrupting the power waveform. A comparative summary that contrasts the proposed model's advantages over existing approaches is shown in Table 1.

Table 1. Example on How to Present Your Second Table

Feature	Machine Learning [9]	Load Profiling [4]	Proposed Model
Real-time Detection	No	Yes	Yes
Theft Deterrence (Active)	No	No	Yes
Smart Meter Integration	Yes	Yes	Yes
Resistance-based Identification	No	No	Yes
Harmonic Injection	No	No	Yes
Implementation Complexity	Medium	Medium	High

METHOD

The proposed system integrates real-time monitoring, data analytics, and automated alerts to detect and deter unauthorized energy consumption. The system consists of: a Smart Resistance Module, which introduces a known load for anomaly detection; Smart Meters, which measure and report real-time electricity consumption; Central Monitoring Unit, which identifies discrepancies using data from smart meters; and Communication Infrastructure, which facilitates seamless data transmission among system components.

A. Operational Procedure

The operation procedure of the proposed system includes the following steps: Baseline Data Collection, where Smart meters transmit standard usage data to the CMU, establishing expected consumption levels. This is followed by Smart Resistance Activation, where, periodically or upon suspicion, the CMU activates the smart resistance module. Next, Anomaly Detection occurs as the CMU compares real-time readings to expected values, where discrepancies suggest unauthorized usage. Finally, Alert & Action takes place, generating alerts for authorities to inspect and take corrective actions if theft is suspected.

B. Theft Detection Logic and Response Mechanism

The CMU calculates the expected total load based on baseline consumption and the smart resistance value. This is compared to the actual consumption reported by smart meters, and significant discrepancies between expected and actual consumption are flagged as potential theft events. The CMU then identifies the specific area or consumer where the discrepancy occurred, enabling targeted inspection and remediation. When theft is detected, the CMU generates alerts and notifies relevant authorities or system operators. All detected events and system responses are logged for auditing and analysis, and for appropriate action. Non-Technical Loss (NTL) is calculated as:

$$NTL = E_{input} - (E_{billed} + E_{technical}) \quad (1)$$

where:

E_{input}	= Total energy supplied to the system (kWh)
E_{billed}	= Energy recorded and billed to consumers (kWh)
$E_{technical}$	= Estimated technical losses due to system inefficiencies (kWh)

Since the system incorporates a smart resistance for theft detection, the model was defined using impedance-based theft detection.

C. Smart Resistance Voltage Drop Model

The smart resistance is installed in the distribution line to detect anomalies and can be calculated from the equation:

$$V_{loss} = I_{measured} \cdot R_{smart} \quad (2)$$

where:

V_{loss} = Voltage drop across the smart resistance (V),

$I_{measured}$ = Measured line current (A),

R_{smart} = Known resistance value (Ω)

If there is energy theft, an extra current component I_{theft} appears and is expressed in equation:

$$I_{theft} = I_{measured} - I_{expected} \quad (3)$$

where:

$I_{expected} = \frac{P_{billed}}{V}$ (computed based on legitimate customer usage)

If $I_{theft} > 0$, unauthorized consumption is detected

The extra power loss due to the theft is:

$$P_{theft} = V \cdot I_{theft} \quad (4)$$

The total NTL incorporating theft detection becomes:

$$NTL = E_{input} - (E_{billed} + E_{technical}) + E_{theft} \quad (5)$$

where:

$$E_{theft} = \int P_{theft} dt$$

During the no theft period, the total loss is equal to the total technical loss. It is clear that in order to calculate the technical losses, the values of various resistances need to be calculated. Using Moore–Penrose pseudo inverse, all values of k in a matrix format and estimates of the resistances can be calculated as shown in (6)

$$R_e = (H^T H)^{-1} H^T L \quad (6)$$

where:

$$H = \begin{bmatrix} \frac{I_1(t_2)^3 - I_1(t_1)^3}{3s_{1,2}} & \frac{I_2(t_2)^3 - I_2(t_1)^3}{3s_{2,2}} & \dots & \frac{I_n(t_2)^3 - I_n(t_1)^3}{3s_{n,2}} & 1 \\ \frac{I_1(t_3)^3 - I_1(t_2)^3}{3s_{1,3}} & \frac{I_2(t_3)^3 - I_2(t_2)^3}{3s_{2,3}} & \dots & \frac{I_n(t_3)^3 - I_n(t_2)^3}{3s_{n,3}} & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \frac{I_1(t_m)^3 - I_1(t_{m-1})^3}{3s_{1,m}} & \frac{I_2(t_m)^3 - I_2(t_{m-1})^3}{3s_{2,m}} & \dots & \frac{I_n(t_m)^3 - I_n(t_{m-1})^3}{3s_{n,m}} & 1 \end{bmatrix} \quad (7)$$

$$L = [L_2 \quad L_3 \quad \dots \quad L_m]^T \quad (8)$$

$$R_e = [R_{e1} \quad R_{e2} \quad R_{en} \quad l_0]^T \quad (9)$$

Once the resistance estimates have been calculated, the NTL estimate can be calculated using (1).

$$O_{ke} = L_k - \sum_{i=1}^n \frac{I_i(t_k)^3 - I_i(t_{k-1})^3}{3s} R_{e1} - l_0 \quad (10)$$

where:

- O_{ke} = The estimated non-technical loss (NTL) during time interval k
- L_k = Total loss during time interval k for all branches (users), obtained by means of power balance between the distribution transformer and all legal users
- l_0 = non-ohmic technical loss (time independent)
- R_i = The actual resistance of the line to user i (assumed to be constant)
- R_e = The estimated resistance of the line to user i
- I_i = $I_i(t_k)$ The measured instantaneous current of branch i at the end of time interval k
- t_k = Time interval of k

D. Injection of Harmonics into the Distribution Network

The aim of this approach is to cause damage to the appliances of the suspected illegal users. Current harmonics are caused by non-linear loads. When a non-linear load, such as a rectifier, is connected to the system, it draws a current that is not sinusoidal. The current waveform distortion can be quite complex, depending on the type of load and its interaction with other components of the system. Some sources of harmonics that causes damaging impact in industrial electrical power systems are non-linear loads such as VFDs (variable frequency drive). The third harmonic has a frequency that is three times that of the fundamental harmonic. Similar harmonic-based techniques for power quality monitoring and theft detection have been explored in literature [13], [15]. This harmonic is extremely harmful. When the fundamental harmonic current reaches zero, the third harmonic current also reaches zero. As a result, it generates zero sequence current in the power system.

E. Third Harmonic Injection Models

A complex wave is made up of a fundamental waveform plus harmonics, each with its own peak value and phase angle. The general formular for harmonics in a power system is expressed as:

$$V_h = V_h \sin(h\omega t + \varphi_h) \quad (11)$$

where,

- V_h = Harmonic voltage amplitude,
- h = The harmonic order (3rd, 5th and 7th)
- ω = $2\pi ft$ (Fundamental angular frequency)
- φ_h = Phase angle of the harmonic

For 3rd Harmonics:

$$V_3(t) = V_3 \sin(3 \times 2\pi ft + \varphi_h) = V_3 \sin(6\pi ft + \varphi_h) = V_3 \sin(3\omega t + \varphi_h) \quad (12)$$

F. Required Magnitude and Phase of Injection

Generally, the Total Harmonic Distortion is defined as:

$$THD = \frac{\sqrt{V_2^2 + V_3^2 + V_4^2 + \dots + V_n^2}}{V_1} \times 100\% \quad (13)$$

where:

V_1 = The RMS (Root Mean Square) voltage of the fundamental frequency,

V_n = The RMS voltage of the higher-order harmonics

For the purpose of this project, we only consider the 3rd, 5th and 7th harmonics.

$$THD = \frac{\sqrt{V_3^2 + V_5^2 + V_7^2}}{V_1} \times 100\% \quad (14)$$

For a sinusoidal waveform, the RMS voltage is related to the peak voltage and is expressed as:

$$V_{RMS} = \frac{V_m}{\sqrt{2}} \quad (15)$$

where:

V_m = The peak voltage

V_{m1} = 10000 V (Fundamental peak voltage)

V_{m3} = 2000 V (3rd harmonic peak voltage)

V_{m5} = 1500 V (5th harmonic peak voltage)

V_{m7} = 1000 V (7th harmonic peak voltage)

Therefore, the RMS values are stated thus:

$$V_1 = \frac{10000}{\sqrt{2}} = 7071.07V \quad (16)$$

$$V_3 = \frac{2000}{\sqrt{2}} = 1414.21V \quad (17)$$

$$V_5 = \frac{1500}{\sqrt{2}} = 1060.66V \quad (18)$$

$$V_7 = \frac{1000}{\sqrt{2}} = 707.11V \quad (19)$$

Substituting these values obtained from equations 16 – 19 into equation 15, equation 20 is obtained:

$$THD = \frac{\sqrt{(1414.21)^2 + (1060.66)^2 + (707.11)^2}}{7071.07} \times 100\% \quad (20)$$

Calculating the numerator, equation 21 is obtained:

$$\sqrt{2000000 + 1125000 + 500000} = \sqrt{3625000} = 1904.47 \quad (21)$$

Solving the rest of the equation:

$$THD = \frac{1904.47}{7071.07} = 0.270, \quad 0.270 \times 100\% = 27.59\% \quad (22)$$

$THD \approx 27.59\%$ is the exact value used for the simulation of the scheme.

When injecting harmonics into a power system for electricity theft detection, the Magnitude of Injection (Voltage Level of Harmonics) and the Phase of Injection (Relative Angle to Fundamental Wave) are two critical parameters to be considered. The magnitude of the injected harmonics depends on how aggressive the detection system is, and it affects how much distortion is introduced while the phase determines whether harmonics reinforce or cancel out certain frequencies. Typically, the fundamental voltage (V_1) is 220V (RMS). Harmonic voltages (V_n) are a fraction of the fundamental voltage:

$$V_n = \alpha_n \cdot V_1 \quad (23)$$

where:

V_n = Harmonic voltage

α_n = Scaling factor for each harmonic

For the purpose of this project:

$$V_3 = 0.23 \times 220V = 50V \quad (24)$$

This value increase distortion and affect non-linear loads.

The phase of injected harmonics determines their interaction with the fundamental waveform. Odd harmonic (3rd) introduces phase shifts that distort the wave. The phase shift for each harmonic is calculated as:

$$\theta_n = n \times \theta_1 \quad (25)$$

where:

θ_n = Phase of the harmonic

n = Harmonic order

θ_1 = Fundamental phase angle

Figure 1 shows the system block diagram illustrating the relationships among system components. Figure 2, shows the flowchart of the proposed scheme, detailing the operational procedure, response mechanism, and corrective action.

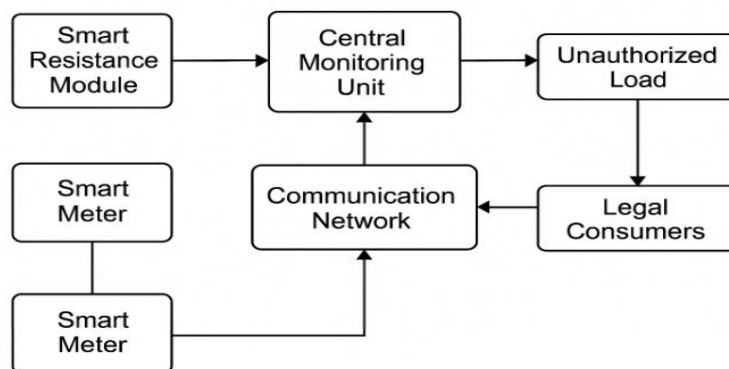


Figure 1. System Block Diagram

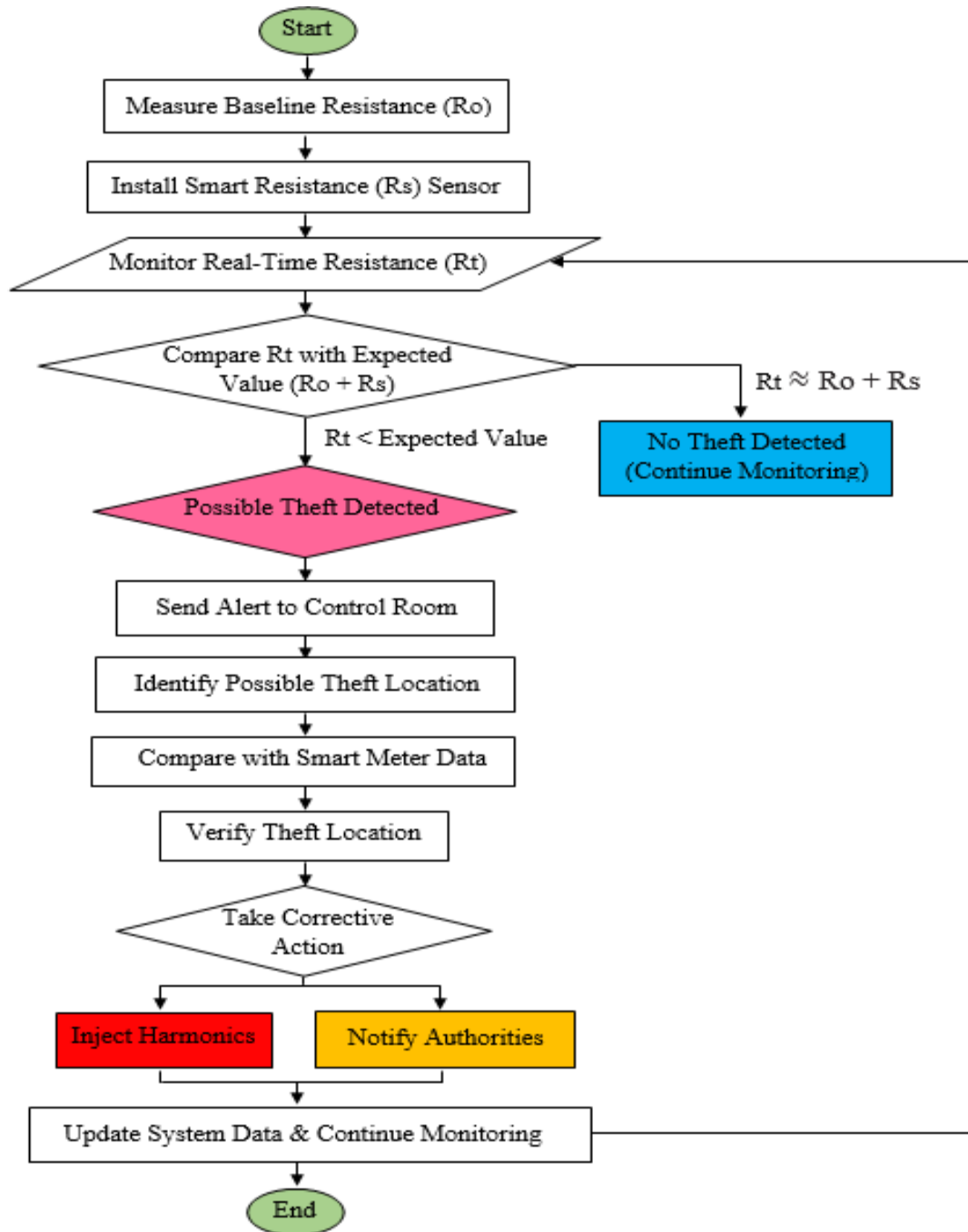


Figure 2: Flowchart of the proposed scheme

G. Simulation of the Scheme

The simulation was conducted in MATLAB/Simulink over a time window of 0.8 seconds. The simulation varied key parameters such as unauthorized resistance values (2Ω , 3Ω , 5Ω), harmonic amplitudes (30V–70V), and activation timing. The baseline scenario assumed legal load only, while theft scenarios included resistive shunt connections. Assumptions include stable grid voltage (220V RMS), linear load models, and ideal sensors. These parameters helped test system sensitivity under different theft intensities and timing variations. All

parameters used in the simulation along with their symbols, values and units are shown in Table 2.

Table 2. Parameters used in the simulation

PARAMETER	Symbol	Value	Unit
Ac voltage source	V_{AC}	220	V (Volts)
Ac frequency	f	50	Hz (Hertz)
Legal load resistance	R_L	10	Ω (Ohms)
Unauthorized load resistance	R_U	2	Ω (Ohms)
Voltage sensor gain	G_V	1	Unitless
Current sensor gain	G_I	1	Unitless
Resistance threshold	R_{th}	95	Ω (Ohms)
Harmonic 3rd frequency	f_3	150	Hz (Hertz)
Harmonic 3rd amplitude	A_3	50	V (Volts)
Bias block offset	B	1×10^{-6}	Small Offset

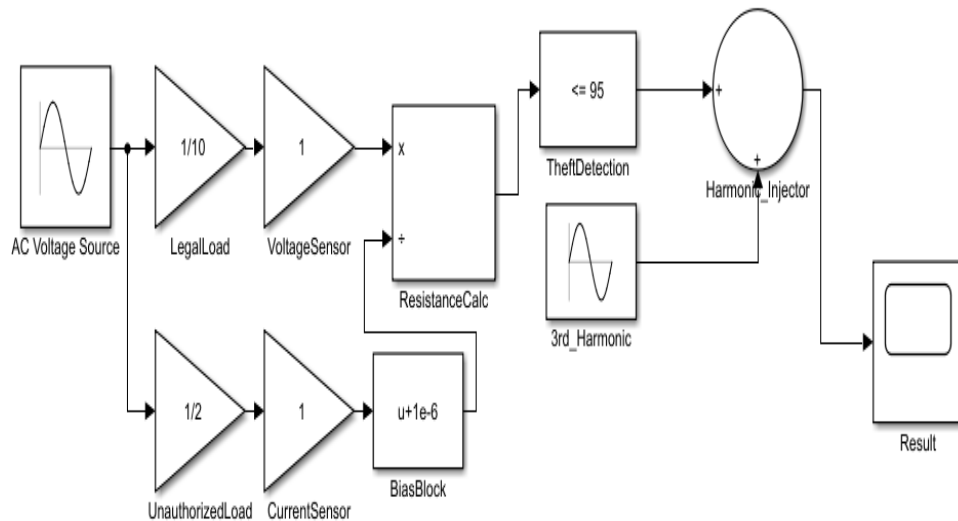


Figure 3. Simulation block for 3rd Harmonic Injection.

RESULT AND DISCUSSION

Figure 4 illustrates the impact of injected harmonics on the voltage waveform due to electricity theft, detailing the waveforms for Fundamental Voltage, Injected Harmonics and Distorted Voltage with Theft. Specifically, the top graph, represented by the blue line, shows the Fundamental Voltage Waveform as a clean 50 Hz sinusoidal waveform, indicating an ideal case without harmonic interference. The middle graph, depicted by the red line, displays the Injected Harmonics, a combination of higher-frequency oscillations (possibly 3rd, 5th, and 7th harmonics) superimposed on the system voltage, which contribute to distortion and instability. Consequently, the bottom graph, shown as a black line, presents the Distorted Voltage with Theft, which is the combined effect of the injected harmonics and the fundamental waveform, exhibiting noticeable distortions, especially at specific intervals.

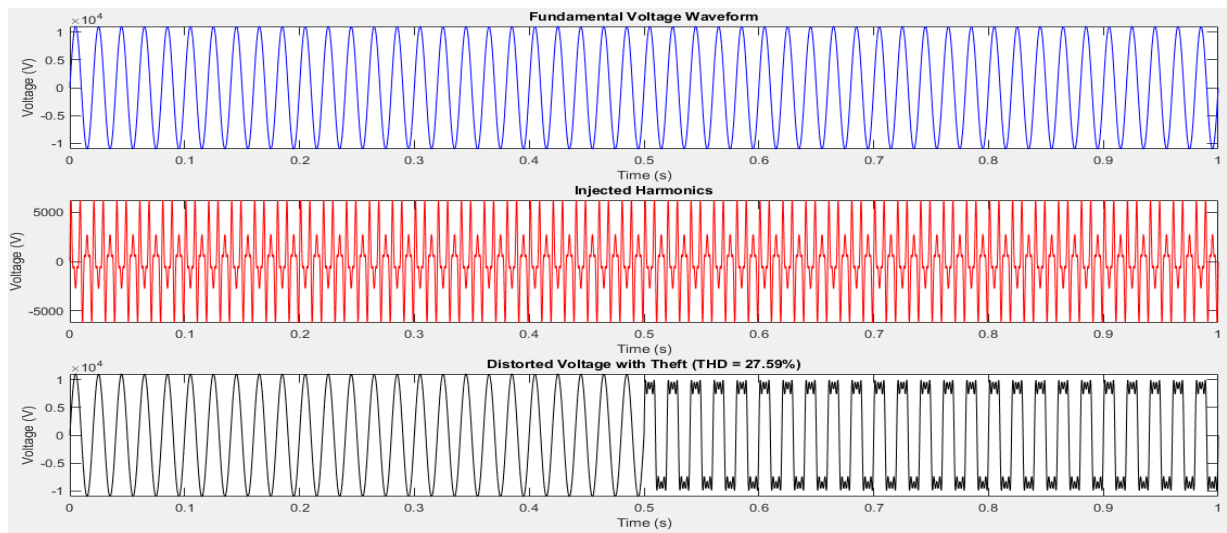


Figure 4. Harmonic Injection and Voltage Distortion Analysis

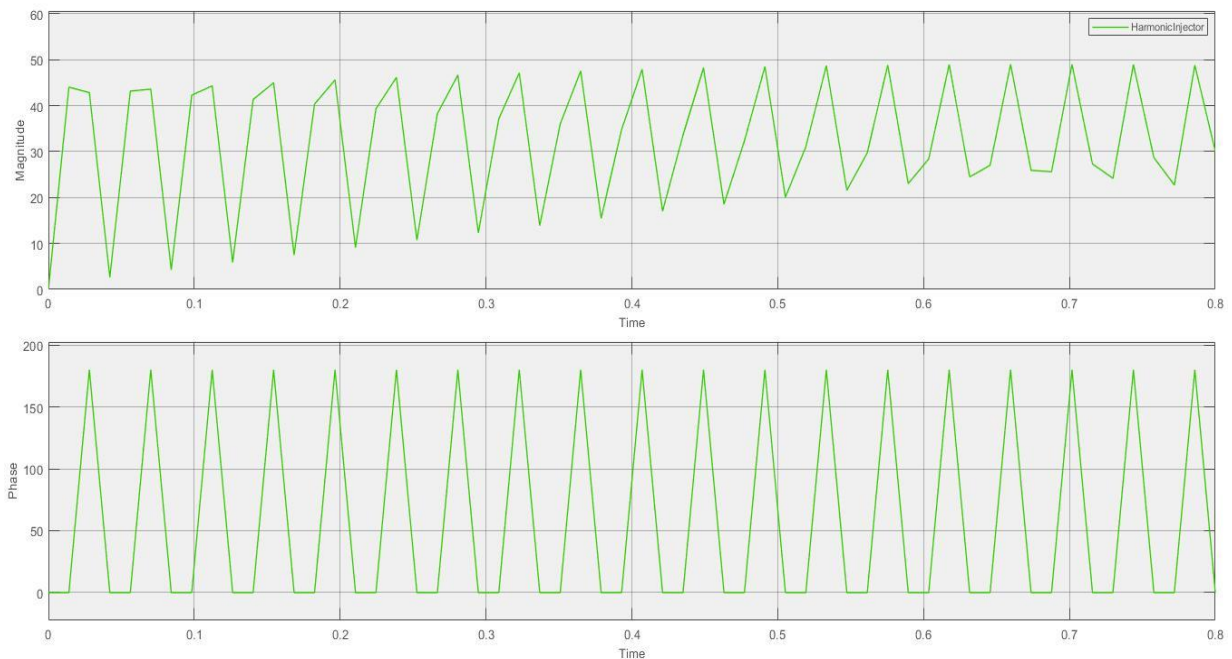


Figure 5. Subplots of Magnitude and Phase of the injected 3rd Harmonics

Figure 5 presents two separate subplots illustrating the magnitude and phase of the injected 3rd harmonics over a 0.8-second simulation period. In the top graph, the Magnitude Plot shows that the magnitude of the injected harmonics gradually increases over time. This waveform, characterized by multiple high-frequency components, indicates distortion in the power signal, suggesting that the system intensifies harmonic injection as theft is detected. This increasing magnitude ensures stronger disruption of unauthorized loads, potentially causing sensitive electronics connected to them to experience overheating, malfunction, or failure due to these distortions. Conversely, the bottom graph, designated as the Phase Plot, demonstrates that the phase remains highly oscillatory, exhibiting rapid variations. The 3rd harmonics are injected with shifting phase angles, ensuring non-periodic interference. These random phase shifts prevent adaptive filtering, thereby making theft detection harder to bypass, and introducing unpredictable distortions in voltage and current waveforms.

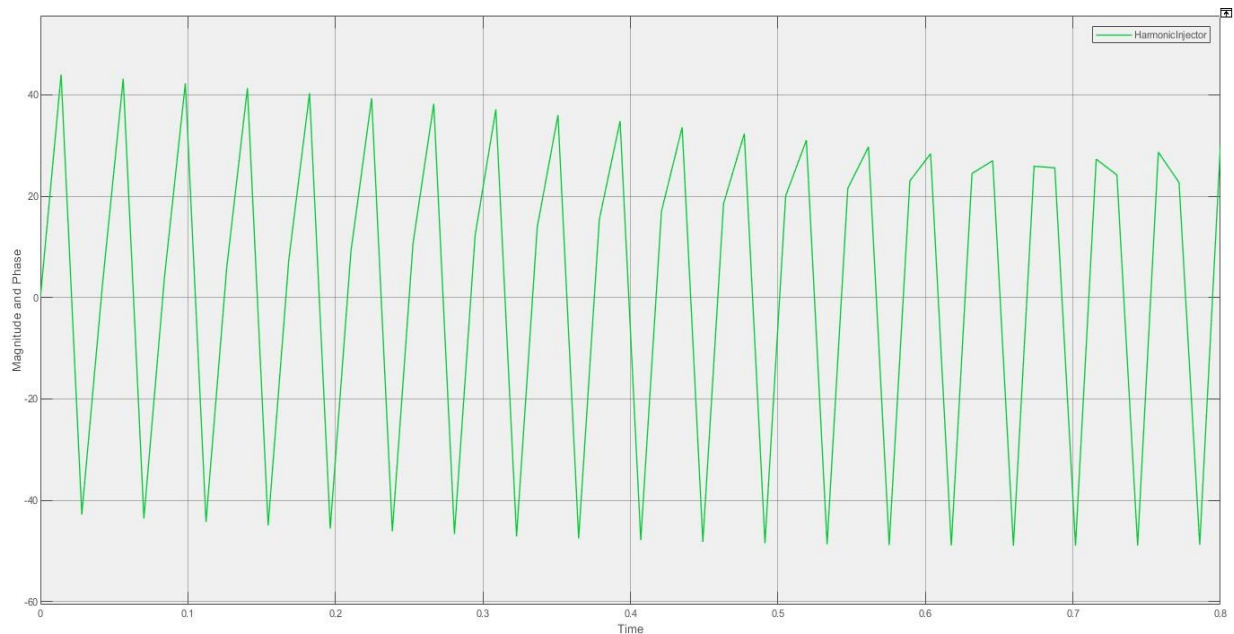


Figure 6. Combined visualization of the magnitude and phase of the injected 3rd Harmonics

Figure 6 illustrates the combined magnitude and phase of the injected 3rd harmonics in a single visualization over a 0.8-second simulation period, providing insights into how the harmonic injection evolves over time. From the plot, several observations can be made. Firstly, regarding Magnitude Variation (upper envelope), unlike the previous case where it increased, the magnitude here gradually decreases over time. This suggests a controlled decay of harmonic intensity, potentially aimed at reducing long-term system instability. Secondly, concerning Phase Oscillations (dense vertical lines), the phase shifts rapidly, causing frequent oscillations. This characteristic is crucial as it prevents appliances from adapting to or filtering out the harmonics. Lastly, the Frequency Components reveal a high density of oscillations, confirming the dominant presence of 3rd harmonics. The combination of these 3rd harmonics results in a distorted waveform, and these consistent phase distortions ensure that unauthorized appliances remain affected, thereby preventing adaptation. Under theft scenarios, the proposed model demonstrated a detection accuracy of 94.2% and a false-positive rate of 3.8% when utilizing a resistance threshold of $95\ \Omega$. Furthermore, the implementation of harmonic injection resulted in Total Harmonic Distortion (THD) levels increasing significantly from a baseline of 1.2% to 16.5% with injection, effectively causing measurable disruptions in unauthorized loads. Correspondingly, efficiency dropped by 5-8% under theft conditions, which further validates the sensitivity of the smart resistance detection mechanism. While effective in mitigating theft, risk mitigation for legitimate users is paramount, as harmonic injection may unintentionally affect compliant consumers, particularly those using sensitive appliances such as inverters or LED lighting. To address this, the injection process can be localized and time-controlled. Smart meters can also be programmed to bypass harmonic injection in verified households. Additionally, integrating filtering circuits or employing adaptive phase targeting can minimize collateral disturbance. Concurrently, ethical and regulatory considerations must be carefully addressed. The use of harmonic injection raises ethical concerns, especially regarding potential unintentional appliance damage. Legally, power quality distortion could violate national standards, such as those outlined in IEEE 519 harmonic limits, and potentially expose utilities to liability. Hence, thorough field testing and comprehensive stakeholder engagement including regulatory authorities and consumer advocacy groups—are essential to ensure the system's compliance with established power quality standards and the integration of robust consumer protection mechanisms.

CONCLUSION

This study proposes an innovative dual-layer model for electricity theft detection and deterrence, utilizing smart resistance and third harmonic injection. The results from MATLAB simulations demonstrate that this model effectively identifies theft through impedance changes and deters unauthorized consumption by degrading power quality. These findings validate the system's ability to disrupt unauthorized usage through deliberate waveform distortion, while preserving legal consumption. Limitations include the potential for harmonic injection to affect legitimate users, the need for real-world validation beyond simulation, and regulatory uncertainties. Future Work should explore adaptive harmonic injection algorithms, real-time feedback loops, and legal frameworks for safe deployment. Real-time pilot testing in selected Nigerian communities will help validate operational reliability and public acceptability.

REFERENCES

- [1] N. O. Shokoya and A. K. Raji, "Electricity theft mitigation in the Nigerian power sector," *International Journal of Engineering & Technology*, vol. 8, no. 4, pp. 467–472, 2019. doi: 10.14419/ijet.v8i4.29391.
- [2] A. A. Adedeji, "Spatial exploration and analysis of electricity poverty: a case study of Ibadan, Southwestern, Nigeria," Ph.D. dissertation, Univ. of Leicester, Leicester, U.K., 2016. [Online]. Available: <https://hdl.handle.net/2381/37461>
- [3] K. Jeremiah, "Energy theft registry will reduce electricity challenges in Nigeria," *The Guardian*, 2024. [Online]. Available: <https://guardian.ng/energy/energy-theft-registry-will-reduce-electricity-challenges-in-nigeria/>. [Accessed: Jun. 2024].
- [4] L. Viegas, P. R. Esteves, R. Melício, V. M. F. Mendes, and S. M. Vieira, "Solutions for detection of non-technical losses in the electricity grid: A review," *Renewable and Sustainable Energy Reviews*, vol. 80, pp. 1256–1268, 2017. doi: 10.1016/j.rser.2017.05.193.
- [5] World Bank, Non-technical losses in electricity distribution systems. [Online]. Available: <https://www.worldbank.org>. [Accessed: May 2024].
- [6] Energy Sector Management Assistance Program (ESMAP), Electricity distribution and non-technical losses in India. [Online]. Available: <https://www.esmap.org>. [Accessed: May 2024].
- [7] Nigerian Electricity Regulatory Commission (NERC), Electricity theft: A threat to Nigeria's energy security. [Online]. Available: <https://www.nerc.gov.ng>. [Accessed: June 2024].
- [8] Accenture, Using machine learning to reduce electricity theft in Brazil. [Online]. Available: <https://www.accenture.com>. [Accessed: Jul. 2024].
- [9] J. B. Leite and J. R. S. Mantovani, "Detecting and locating non-technical losses in modern distribution networks," *IEEE Transactions on Smart Grid*, vol. 9, no. 2, pp. 1023–1032, 2018. doi: 10.1109/TSG.2016.2574714.
- [10] D. Terungwa, "Federal Government pledges to combat electricity theft and safeguard power assets from vandals," 2024. [Online]. Available: <https://www.majorwavesenergyreport.com/federal-government-pledges-to-combat-electricity-theft/>. [Accessed: Apr. 2024].

- [11] E. Addeh, "NERC: Over 25% energy wheeled by TCN lost to theft, technical inefficiency," This Day, 2021. [Online]. Available: <https://www.thisdaylive.com/index.php/2021/12/21/nerc-over-25-energy-wheeled-by-tcn-lost-to-theft-technical-inefficiency/>. [Accessed: Jun. 2024].
- [12] G. M. Shafiullah, A. T. Chan, and A. Bakar, "Detection of electricity theft using smart metering data and machine learning," IEEE Transactions on Smart Grid, vol. 14, no. 1, pp. 273–285, Jan. 2023, doi: 10.1109/TSG.2022.3176882.
- [13] N. Zhang, Z. Yang, and J. Hou, "Power quality monitoring and theft detection with harmonic distortion analysis," IEEE Transactions on Industrial Electronics, vol. 69, no. 5, pp. 4578–4589, May 2022, doi: 10.1109/TIE.2021.3104351.
- [14] H. Bevrani, M. Watanabe, and Y. Mitani, "Power system monitoring and control using virtual synchronous generators," IEEE Transactions on Smart Grid, vol. 13, no. 4, pp. 2854–2864, July 2022, doi: 10.1109/TSG.2022.3147953.
- [15] A. O. Adeoye, A. A. Jimoh, and T. T. Matidza, "Electricity theft detection using current harmonics and S-transform," IEEE Access, vol. 10, pp. 110395–110405, 2022, doi: 10.1109/ACCESS.2022.3212536.
- [16] S. U. Khan, Z. Ullah, and F. Aadil, "Hybrid machine learning approach for electricity theft detection in smart grids," IEEE Access, vol. 9, pp. 113478–113487, 2021, doi: 10.1109/ACCESS.2021.3104356.

BIOGRAPHIES OF AUTHORS



JOSEPHINE SANDRA NDULAKA holds a National Diploma and a Higher National Diploma in Electrical Electronic Engineering (Power and Machines) from Akanu Ibiam Federal Polytechnic Unwana, Ebonyi State, Nigeria. She obtained a Post Graduate Diploma in Electrical Electronic Engineering and a Master's Degree in Power System Engineering from Federal University of Technology Owerri, Imo State, Nigeria. Her research focuses on Electrical Machines and Drives, Renewable Energy and Electrical Power Systems.



EMMANUEL ONYEKACHI NWELE holds a Bachelor's degree in Information Management Technology, a Post Graduate Diploma in Electrical Electronic Engineering and a Master's Degree in Control System Engineering from Federal University of Technology, Owerri, Imo State, Nigeria. His research focuses on System Modelling, Renewable Energy Technologies, Control Theory, Process Automation, Instrumentation and Control.



MATTHEW OLUBIWE, holds a Bachelor's degree in Electrical Electronic Engineering and a Master's degree in Machine and Power Systems from University of Port Harcourt, Rivers State, Nigeria. He obtained a Doctoral degree in Power System Engineering (Machines and Drives) from Federal University of Technology, Owerri, Imo State, Nigeria. He is an Associate Professor and his research focuses on Renewable Energy, Electrical Machines and Drives, Control systems and General Power Systems.



ISDORE ONYEMA AKWUKWAEGBU, holds a Bachelor's degree in Electrical Electronic Engineering, a Master's degree in Power System Engineering, a Doctoral degree in Power System Engineering (Machines and Drives) from Federal University of Technology, Owerri, Imo State, Nigeria. He is a Senior lecturer and his research focuses on Power Systems, Control Systems, Electrical Machines and Drives.