Journal Européen des Systèmes Automatisés
Vol. 57, No. 6, December, 2024, pp. 1687-1695
Journal homepage: http://iieta.org/journals/jesa

A Phase Modulation-Based Approach for Theft-Proof Electricity Distribution in India Using CDMA Technology

Gaurav Saxena[1], Subodh Kumar Singhal[2], Snehal Bhosale[3*], Prateek Pandey[1]

[1] Department of Computer Science & Engineering, Jaypee University of Engineering and Technology, Guna 473226, India
[2] Department of Electronics & Communication Engineering, Jaypee University of Engineering and Technology, Guna 473226, India
[3] E&TC Department, Symbiosis Institute of Technology, Pune Campus, Symbiosis International (Deemed University), Pune 412115, India

Corresponding Author Email: snehal.bhosale@sitpune.edu.in

https://doi.org/10.18280/jesa.570616

Received: 1 November 2024
Revised: 26 November 2024
Accepted: 6 December 2024
Available online: 31 December 2024

Keywords:
product modulator, wave shaping, NRZ, phase modulation, A/D converter

ABSTRACT

Power theft is a major challenge in many developing nations, disrupting the consistent supply of electricity and undermining efforts to provide affordable energy to legitimate consumers. In densely populated countries such as India, frequent power outages and inflated energy prices are further exacerbated by illegal grid tapping, which hinders economic growth. This problem not only drains financial resources from utility companies but also results in unreliable electricity supply, affecting industries, businesses, and households alike. Addressing this requires a robust solution that ensures secure and efficient power distribution. This article proposes a theft-proof method of distributing electricity from power substations to homes, utilizing phase modulation and Code Division Multiple Access (CDMA) technology. Phase modulation encodes power signals in such a way that only authorized users with the correct decoding mechanism can access the electricity, while CDMA assigns unique codes to each user, ensuring secure, simultaneous energy distribution to multiple consumers without interference. These techniques make unauthorized access to the grid virtually impossible. The proposed system was simulated using MATLAB software to test its effectiveness. The encouraging results demonstrated the feasibility of the approach, highlighting its potential to be implemented at full capacity in real-world scenarios, offering a reliable solution to combat power theft while improving grid stability and energy efficiency.

1. INTRODUCTION

In present era, every human-being require some electrical and electronic equipment for their comfortable living. However, electronics and electrical equipment works on electrical energy, the generation and distribution of the electricity is a challenging issue for many developing countries. The electrical energy can be generated from various ways based on the availability of natural resources. Most of the countries are producing electrical energy according to their needs, but they are not getting the expected value out of that energy. A significant portion of electricity losses in India, exceeding 20%, stems from inefficiencies during transmission and the rampant theft of electricity during its distribution. These issues not only undermine the reliability of the power supply but also impose substantial financial burdens on utility providers, highlighting the urgent need for systemic reforms [1]. In terms of Peak, all the regions except Western Region are likely to face deficit varying from 1.0% to 7.9% with 1.0% in North-Eastern Region, 1.8% in Southern Region, 7.3% in Northern Region and 7.9% in Eastern Region [2]. Therefore, transmission and distribution of electricity is a challenging task for any developing country like India, compared to the generation of electricity.

On the other hand, uninterrupted power distribution to the schools, offices, households and the industries is indispensable for any country to remain significant in the cohesive global eco-system. Energy theft in India is so common during the distribution of electricity, which causes more than ₹ 1 trillion losses annually [3]. This leads to power outages and interruptions in planned or unplanned manner in the schools, offices and households. In present time the electricity has reached all the households of India, rural or urban, and many precautions has been taken during distribution of energy to protect it from transmission loss as well as from theft, but the problem of power theft has still not been addressed adequately.

There are broadly two ways in which electricity is being stolen in India: one is meter fraud- manipulating data of electricity usage; second is unmetered usage- tapping into the supply lines or bypassing the meter [4]. Political influence often makes it hard to report the crime of theft against the culprits by the distribution companies. Besides, most of the overhead electrical wires in India are not insulated, which adds to the challenges to the distribution companies.

A lot of effort has been made by many researchers in last two decades for the detection of illegal tapings on the distribution lines [5, 6]. Based on their findings, they have categorized illegal tapping detection into the power distribution lines in two ways: (i) data analytical practices and (ii) electrical losses identification techniques. The data analytics methods of tracking illegal tapping are based on the comparison of current month bill of electricity with the previous month bills for finding the irregularities in the power consumptions. It also has another way of comparison in which current month bill is compared with the load consumption of house hold appliances. On the other hand, electrical loss identification technique is based on the smart meters employed at customer end. In the smart meter there is a provision to detect the theft when power is taken directly from the supply by bypassing the electrical meter. Various research papers have been reported in the literature based on these two approaches for illegal tapping detection, which are discussed in chronological order in next paragraph.

In this section, the methodology adopted for designing of illegal tapping protection system and proposed end-to-end protection system is developed. In present era, every human-being require some electrical and electronic equipment for their comfortable living. However, electronics and electrical equipment works on electrical energy, the generation and distribution of the electricity is a challenging issue for many developing countries. The electrical energy can be generated from various ways based on the availability of natural resources. Most of the countries are producing electrical energy according to their needs, but they are not getting the expected value out of that energy. The main reason behind this is the losses during transmission and theft of electricity during distribution. Therefore, transmission and distribution of electricity is a challenging task for any developing country like India, compared to the generation of electricity.

On the other hand, uninterrupted power distribution to the schools, offices, households and the industries is indispensable for any country to remain significant in the cohesive global eco-system. Energy theft in India is so common during the distribution of electricity, which causes more than one trillion rupees losses annually [3]. This leads to power outages and interruptions in planned or unplanned manner in the schools, offices and households. In present time the electricity has reached all the households of India, rural or urban, and many precautions has been taken during distribution of energy to protect it from transmission loss as well as from theft, but the problem of power theft has still not been addressed adequately.

There are broadly two ways in which electricity is being stolen in India: one is meter fraud- manipulating data of electricity usage; second is unmetered usage- tapping into the supply lines or bypassing the meter [4]. Political influence often makes it hard to report the crime of theft against the culprits by the distribution companies. Besides, most of the overhead electrical wires in India are not insulated, which adds to the challenges to the distribution companies.

A lot of effort has been made by many researchers in last two decades for the detection of illegal tapings on the distribution lines [5-7]. Based on their findings, they have categorized illegal tapping detection into the power distribution lines in two ways: (i) data analytical practices and (ii) electrical losses identification techniques. The data analytics methods of tracking illegal tapping are based on the comparison of current month bill of electricity with the previous month bills for finding the irregularities in the power consumptions. It also has another way of comparison in which current month bill is compared with the load consumption of house hold appliances. On the other hand, electrical loss identification technique is based on the smart meters employed at customer end. In the smart meter there is a provision to detect the theft when power is taken directly from the supply by bypassing the electrical meter. Various research papers have been reported in the literature based on these two approaches for illegal tapping detection, which are discussed in chronological order in next paragraph.

Jokar et al. [8] have reported AMI data-based approaches for the detection of illegal power theft. This article adopted the strategies that depend on classification-based, state estimation-based, and game theory-based algorithms for detection of various energy-thefts. Smart meters and data collectors can help judicial processes in cases of electricity theft [9]. Kadurek et al. [10] talked on current smart metering practices and the circumstances in the Netherlands. They also provide a brand-new automated technique for detecting fraud and tampering. Nizar et al. [11] conducted research on non-technical losses utilizing cutting-edge tools including data mining and machine learning. A statistical model of technical losses and non-technical losses is estimated to detect theft in the study [12]. It accomplishes this by estimating that each user is directly linked to its local distribution terminal and computing the effective resistances between the distribution terminals and the customer premises. Pattern recognition algorithms are suggested as a way to detect stealing of electricity [13]. And in the study [14], it is suggested to use a state estimation-based method to identify electricity theft in micro grids while maintaining secrecy.

Therefore, for addressing the issue of power theft, this article presents, a phase-modulation based electricity waveform masking method that imposes a high penalty for the electricity theft, which indirectly discourages the illicit tapping into the supply lines of the electricity. The waveform masking produces the random shifting of the phase angle of transmitted power and the direct use of masked signal may produce the severe harm to the utility devices. The proposed method is demonstrated through a MATLAB-based simulation, where all components are virtually integrated. The remainder of this paper is organized as follows: In Section 2, proposed system methodology has been discussed. Section 3 presents the proposed model for Electricity Theft Protection and its calculation in detail. In Section 4, the simulation results are discussed. Finally, concluding remarks and future scope are included in Section 5 and Section 6, respectively.

2. PROPOSED SYSTEM

In this section, the methodology adopted for designing of illegal tapping protection system and proposed end-to-end protection system is developed.

2.1 Methodology

In general, most of the house hold appliances used for various purposes receive AC power from the supply and works on the phenomenon of inductance, capacitance and resistance as their integral part [15]. Therefore, we have gone through the working of these components and observed that inductance and capacitance are majorly influenced by change in phase of applied AC signal. Based on this study, we reach to the conclusion that if the phase of input signal is changed after a random interval of time, then this type of signal is not suitable for the proper working of these household appliances and create malfunctioning [16, 17]. Besides, some phenomenon is needed to create this type of secured signal whose phase changes with random interval of time sent by the electricity board and must be retrievable at the customer end. This idea can help in prevention of theft of electricity through illegal tapping. To make this idea on real ground, literature on various secured code signal have been made. From the literature, it is found that orthogonal signals have a property: if they are multiplied with the input signal, they produce a coded output. Further, if this output is multiplied by any other orthogonal code, it produces a zero output. It will give only 1 when it is multiplied by the same code that produced the original signal, which remains the same as it was at the sending end [18, 19].

There has been literature produced on different secured code signals in order to put this theory into practice [20, 21]. According to the literature, orthogonal signals have the ability to produce a coded output when multiplied with the input signal. They also produce a zero output when multiplied by another orthogonal code, and only yield a 1 when multiplied by the same code, which results in the original signal that was present at the sending end.

For producing the orthogonal signals, it is required to generate a binary sequence of finite length and this sequence must follow the property of orthogonality. The Walsh code has been adopted for generation of binary sequence, which is fundamentally based on Hadamard Transform. The procedure of the binary sequence generation through the Walsh code is described in the following sub-section.

2.2 Binary sequence generation

For the generation of binary sequences, a Walsh table is used, which is basically a two-dimensional table with an equal number of rows and columns, as shown in Eq. (1).

$$W_N = \begin{bmatrix} +1 & +1 & +1 & +1 & +1 & - & - & - & N \\ +1 & -1 & +1 & -1 & +1 & - & - & - & N \\ +1 & +1 & -1 & -1 & +1 & - & - & - & N \\ +1 & -1 & -1 & +1 & +1 & - & - & - & N \\ +1 & +1 & +1 & -1 & +1 & - & - & - & N \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & N \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & N \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & N \\ N & N & N & N & N & N & N & N & N \end{bmatrix} \tag{1}$$

$$W_{2N} = \begin{bmatrix} W_N & W_N \\ W_N & \overline{W_N} \end{bmatrix} \tag{2}$$

$$W_1 = [+1] \tag{3}$$

$$W_2 = \begin{bmatrix} +1 & +1 \\ +1 & -1 \end{bmatrix} \tag{4}$$

$$W_4 = \begin{bmatrix} +1 & +1 & +1 & +1 \\ +1 & -1 & +1 & -1 \\ +1 & +1 & -1 & -1 \\ +1 & -1 & -1 & +1 \end{bmatrix} \tag{5}$$

Generalized equation for Walsh table (W_N) is given in Eq. (1). From the Eq. (1), it can be seen that elements of each row of Walsh table are a binary sequence of either +1(logic '1') or -1 (logic '0'). According to Walsh, the square matrix W_{2N} can be generated by using W_N that is given in Eq. (2) where W_N with the overbar $\overline{W}_N$ stands for the complement of W_N, during complement each +1 is changed to -1 and vice versa. Therefore, for N=1, W_1 has a binary sequence of one row and one column, we can choose -1 or +1 for the chip for this trivial table (we took +1) as shown in Eq. (3) [17], whereas for N=2, it has two rows and two columns and the matrix can be developed by using (2) which is shown in Eq. (4). To generate sequence N=4, Eq. (2) is used which replicates W_2 in two rows and two columns with the last one the complement form of W_2. Of course, W_8 is composed of four W_4's, and so on. This process is used to generate any binary sequence for different values on N where N varies in the form of 2N.

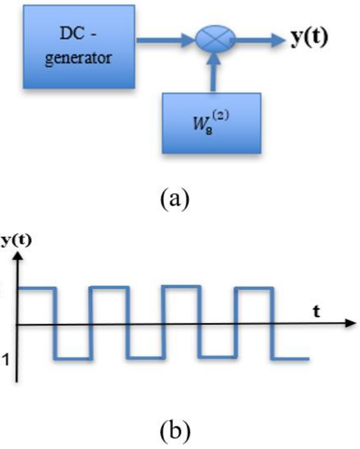
2.3 Generation of orthogonal signal

For the generation of the orthogonal signal, any one of the rows of the Walsh table which basically represent the binary sequence can be used [22-25]. To understand this, the Walsh table (W_N) with N=8 is considered which has 8 rows of binary sequence. Suppose if second row, i.e.,

$$W_8^{(2)} = \{+1, -1, +1, -1, +1, -1, +1, -1\}$$

which is used then generation of orthogonal signal with this binary sequence is shown in Figure 1.

The orthogonal signal generator as shown in Figure 1 consists of three elements i.e. (i) DC generator, (ii) Binary sequence generator using Walsh table and (iii) product modulator. The DC generator generates a constant dc signal of fixed amplitude with zero frequency whereas binary sequence generator, generates a sequence of +1 and -1 according to Walsh table ($W_8^{(2)}$).



(a)

(b)

Figure 1. (a) Orthogonal signal generator; (b) generated waveform

Finally, the product modulator multiplies the binary sequence with DC signal which will produce the required orthogonal masking signal as shown in Figure 1(b). This orthogonal masking signal will be utilized to develop power theft protection system which is described in next section.

3. PROPOSED ELECTRICITY THEFT PROTECTION SYSTEM (ETPS)

In present electricity distribution system, the electricity is transmitted from the main substation to the distribution pole (DP) located in the particular region where electricity has to be provided. At DP, the transformer is placed to maintain the constant power supply and this constant power supply is distributed to the consumer resides in the apartment/ houses. During transmission of electricity from DP to the house, one can theft the electricity through cable pinning or bypassing the meter which otherwise should be recorded in the meter of consumer. This type of electricity theft causes financial losses to the power distribution company. Protection from electricity theft is a challenging issue for any of the developing country. Therefore, in this paper Electricity Theft Protection System (ETPS) is developed to overcome the electricity theft issue from various means as mentioned in previous sections. The proposed ETPS model is shown in Figure 2. In the proposed system the electricity distribution company will send a unique code to the DP as well as consumer meter through cloud as shown in Figure 2. At DP this unique code will be combined with the electrical signal to generate secured electrical signal. Further, this secured electrical signal will be transmitted to the consumer meters. On the other side, the code received from the cloud at consumer meter will be used to decode the secured signal transmitted from the DP to get the original electrical signal. Therefore, special design of transmitter and receiver is required where transmitter will be attached at DP end to generate secure signal and receiver attached to consumer meter end to decode the signal, which are discussed in next sub sections.

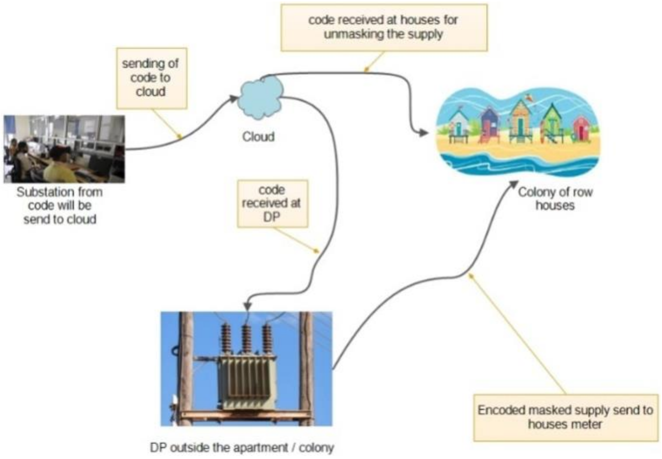

code received at houses for unmasking the supply
sending of code to cloud
Cloud
Substation from code will be send to cloud
code received at DP
Colony of row houses
Encoded masked supply send to houses meter
DP outside the apartment / colony

Figure 2. Overview diagram of proposed “ETPS” distribution structure

Design of Transmitter for ETPS:

The design of transmitter for ETPS system is shown in Figure 3. It consists of code receiver, Analog to Digital converter, wave shaping circuit, product modulator, and input power supply. Basically, code receiver receives a signal from the cloud which contains the unique code. Further, A/D converter is deployed in the transmitter to extract the unique code from the received signal. This extracted unique code is send to the wave shaping circuit which converts unique code in the form of non-return-to-zero (NRZ). The NRZ form of signal have only two levels i.e. +1 to -1, where +1 indicates logic one and -1 indicates logic zero. Further the product modulator is used which receives the NRZ signal from wave shaping circuit and input signal from raw power supply (220V/50Hz) substation and produces a secured output signal to disincentivize electricity theft.

This secured output signal is transmitted through transmission line to the consumer houses. During transmission, if anyone tries to steal the electricity from the wire then this coded signal creates malfunctioning and may damage their electronic and electric equipment. This happens because transmission line carries the secured output signal which is not in the form as desired by the available home appliances. This secured output signal can prevent the electricity theft from any of unauthorized means. Besides, authorized customer must have receiver with the meter for converting this secured signal into a desired form before applying to home appliances. Therefore, a receiver is required to get the desired output from the secured signal which is discussed in next subsection.

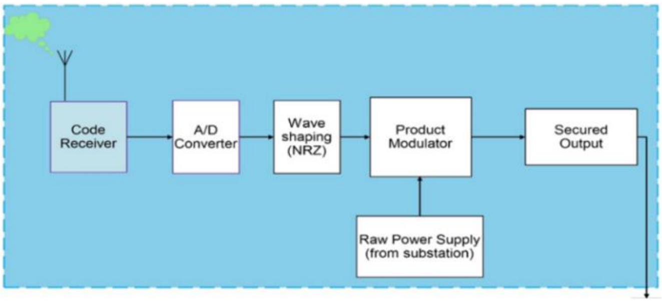


Figure 3. Block diagram of ETPS transmitter

Design of Receiver for ETPS:

The receiver consists of code receiver, A/D converter, wave shaping circuit, product modulator as shown in Figure 4. In receiver section first block is code receiver which receives a signal from the cloud that contains the unique code and this unique code is extracted from the received signal through A/D converter connected next to the code receiver block. After the A/D converter, wave shaping circuit block is connected to convert unique code in the form of non-return-to-zero (NRZ). Further the product modulator is used which receives the NRZ signal from wave shaping circuit and secured signal from the transmission line and produces a desired AC output signal (220V/50Hz) for the use of home appliances.

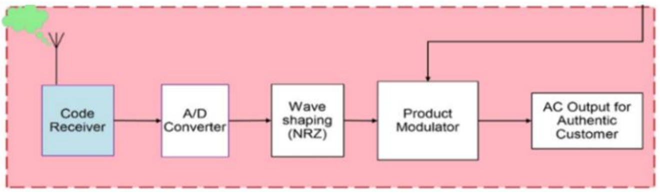


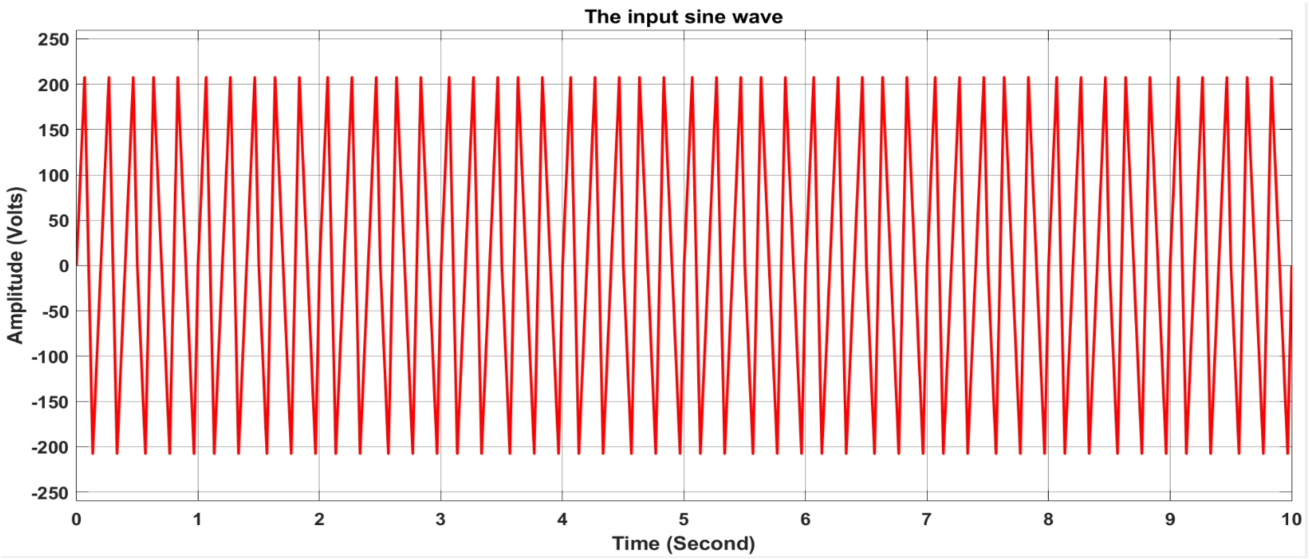
Figure 4. Block diagram of proposed method

4. EXPERIMENTAL RESULTS AND ANALYSIS

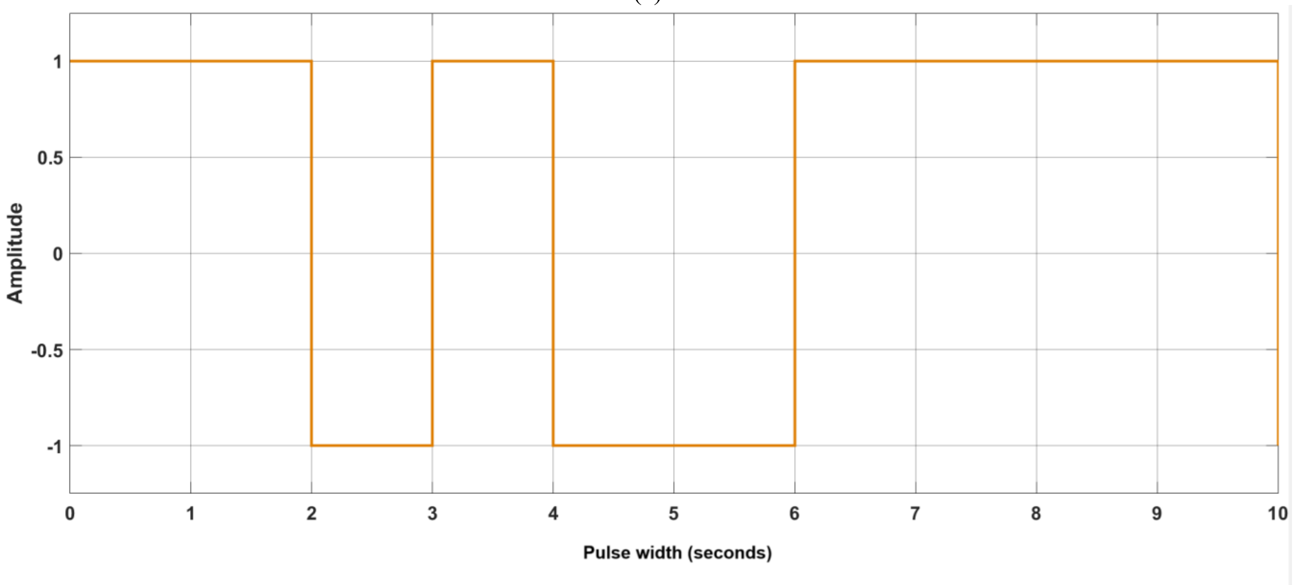
To set up the experiment, a computer system with a 64-bit Core i7 processor and 6GB of RAM was used. MATLAB 19 was employed to complete the system simulation and analysis, specifically for developing the transmitter and receiver models to validate the proposed system. As illustrated in Figure 5, a unique code and sinusoidal input signal were also generated in MATLAB. The input signal is fed solely to the transmitter, while both the transmitter and receiver models receive the unique code. The transmitter model was simulated in MATLAB, resulting in the output waveform shown in Figure 5. The waveform exhibits a phase shift whenever the code changes from 1 to 0 or vice versa. If this phase-modulated waveform is intercepted during transmission and used unauthorizedly, it could cause an imbalance in the equipment. This imbalance refers to any deviation in the voltage or current waveform, either in magnitude or phase shift. The following effects can be observed when using an unbalanced signal across various equipment:

- Unbalance raises the working temperature, which shortens the equipment's lifespan and decreases motor efficiency by creating excessive heating. The motor windings deteriorate and grease or oil in the bearings breaks down as a result of the increased heat.
- Negative sequence currents run alongside positive sequence currents in induction motors that are linked to an imbalanced supply, decreasing the percentage of productive current and motor efficiency. Motor performance is greatly impacted by an imbalance of more than three percent.
- There are fluctuations as a result of the motor's torque, and by extension, its speed becoming irregular. These abrupt torque changes cause damage, noise, and a decrease in the equipment's overall efficiency by increasing vibrations in the gearbox or related machinery.
- Variable frequency drives connected to an unbalanced system may trip, as they interpret severe unbalances as phase faults, leading to earth fault or missing phase fault triggers. Unbalances also result in the de-rating of power cables, increasing iron losses. For distribution cables, the de-rating factor indicates the portion of total current effectively contributing to productive outcomes.
- UPS or inverter supplies operate with reduced efficiency and introduce higher harmonic currents when the system experiences unbalances.
- Negative phase sequence currents caused by unbalance can lead to motor faults, potentially resulting in tripping or permanent damage to electrical equipment.

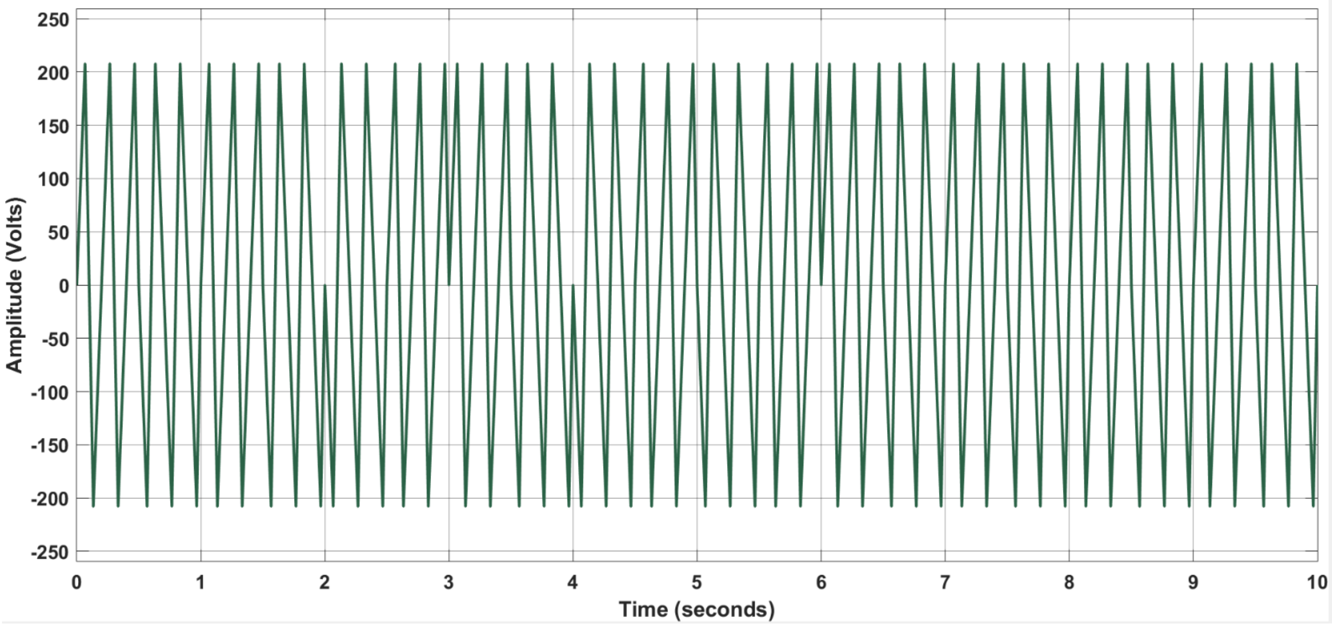
It can be concluded that the primary components of most home appliances are resistors, capacitors, and inductors. Among these, phase shifts have the greatest impact on the operation of inductors and capacitors, leading to an imbalance that affects the appliances' functionality. If an unauthorized individual attempt to access the power supply, their appliances may become unbalanced, potentially causing malfunctions or even permanent damage to the equipment. Furthermore, the next sub section clearly demonstrates how the proposed system generates an unbalanced situation in response to any type of illegal power usage.



(a)



(b)



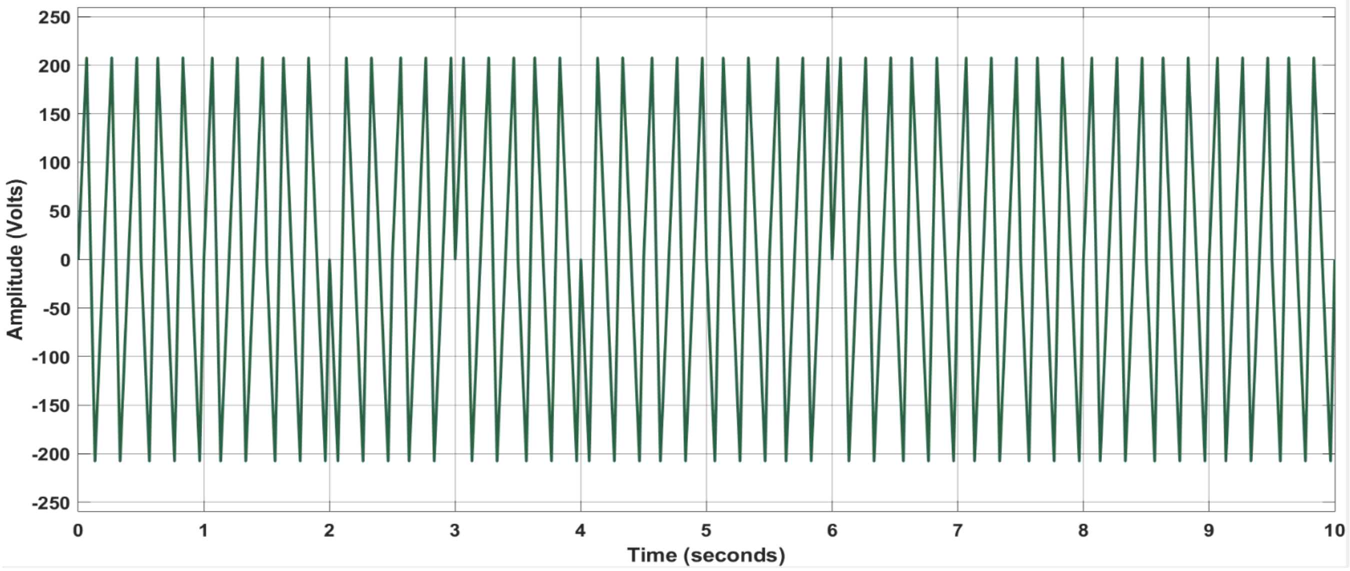
(c)

Figure 5. Waveform developed from transmitter section of proposed method: (a) Original Signal from main supply, (b) Coded NRZ signal and (c) Secured signal from transmitter

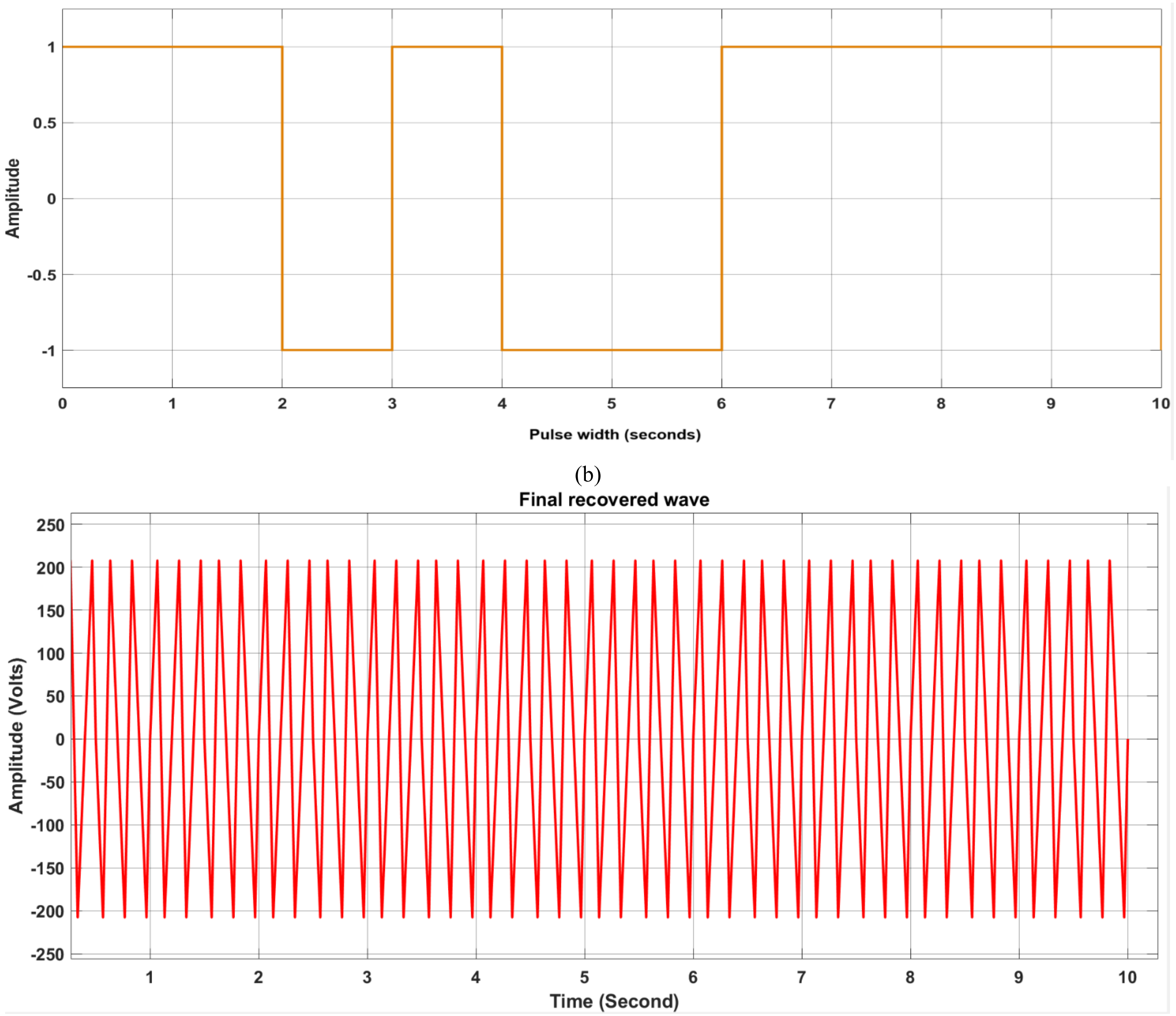
The results of the simulated transmitter section at various stages are illustrated in Figure 5. The outputs from each section are as follows: Figure 5(a) displays the unencrypted sinusoidal wave input to the transmitter. Figure 5(b) shows the NRZ waveform generated using a code downloaded from the cloud. Finally, Figure 5(c) illustrates the encrypted and secured output waveform produced by the transmitter, which will be used for power transmission. Further, according to the proposed model, the generated theft proof signal from transmitter are now send to the consumer house as showed in Figure 5(c). In authentic consumer house there is a receiver provision inside the electricity measuring meter to recover the original required waveform with same phase and frequency.

According to the proposed model receiver section, the theft-proof waveform developed by the transmitter is sent to the customer's home. An internal receiver enables the electricity meter in a genuine consumer's house to retrieve the original waveform at the same frequency and phase. As mentioned earlier, the receiver comprises several stages, which can be simulated in MATLAB. These stages include the code receiver, A/D converter, wave-shaping circuit, and product modulator. The code obtained from the cloud is further retrieved and sent to the product modulator section together with the secured signal obtained from DP in order to obtain the receiver outcome.

The product modulator's intended output is now available for the user to employ for a variety of purposes. Figure 6 displays the results of the simulated receiver section. The input encrypted sinusoidal wave to the receiver section is displayed in Figure 6(a). The NRZ waveform created using code downloaded from the cloud is displayed in Figure 6(b). The output recovered waveform is finally shown in Figure 6(c), where it will be further utilised by the customer.



(a)



(b)

(c)

Figure 6. Waveform developed from receiver section of proposed method: (a) Original Signal from main supply, (b) Coded NRZ signal and (c) Secured signal from receiver

The proposed system is analyzed both qualitatively and quantitatively as follows:

Qualitative Analysis:

The perfect recovery of the useful signal from the encrypted, secured signal received from the transmitter is evident in Figures 5 and 6. Figure 5(a) shows the original signal supplied by the grid, while Figure 6(c) displays the decrypted signal from the receiver—both are identical. This ensures that the receiver output will not cause any issues for authorized users. However, if an unauthorized user bypasses the electricity meter to access the direct signal (which is actually the secured signal shown in Figure 5(c)), they may face equipment damage or malfunction.

Quantitative Analysis:

The qualitative analysis is further validated through the measurement of quantitative parameters. In this context, the mean square error (MSE) is calculated between the original signal and the authorized user's signal, as well as between the original signal and the unauthorized user's signal (i.e., the encrypted signal), using the Eq. (6) below.

$$MSE = \frac{1}{N \times M} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} [X(i,j) - Y(i,j)]^2 \quad (6)$$

where, $X(i,j)$ and $Y(i,j)$ are the image of recovered signal and original signal respectively. The value of $X(i,j)$ and $Y(i,j)$ are taken from Figures 5 and 6, and the computed value of MSE is shown in Table 1.

Table 1. Computed value of MSE

Parameter	**Comparison Between Signal Received**	
	by Authorized User	**by Unauthorized User**
MSE	0	6.5e+3
PSNR	∞	9.9873

To quantitatively analyses the consistency of the proposed model, from Figures 5 and 6, up to three peaks with a minimum distance of three units were selected, and signal statistics such as peak-to-peak, mean, median, and RMS values were computed. The results are presented in Table 2.

Table 2. Signal statistics

Signal	Peak to Peak	Mean	Median	RMS
Original	4.15e+02	-2.238e-13	0	1.638e+02
Encrypted	4.15e+02	1.741e-13	0	1.638e+02
Decrypted	4.15e+02	-2.238e-13	0	1.638e+02

As shown in Table 2, the mean value of the encrypted signal (secured signal from the transmitter) changes noticeably, while the other values remain consistent during encryption. This indicates that the secured signal effectively creates obstacles for unauthorized users only.

5. CONCLUSIONS

The conversion of the power signal into the secured signal and its transfer to the consumer will be the foundations of the system's successful prevention of unauthorized tapings from distribution lines. This strategy sought to completely eliminate the threat that unlawful recording has become in our modern society. These illegal tapings have a negative impact on the local economy as well as the transmission company's economy, both of which may be protected. In this method, there is no need to report any vigilance team about the occurrence of theft, because if there is any illegal tapping occurs, it will automatically create malfunction in the appliances of thieves. The development of the working model for this system can be done at a reasonable cost without the need for a significant capital expenditure. This additional investment is nothing as compared to the capital loss bear by the government or the utility company because of the electricity theft. This study should be helpful in developing a smart power distribution system for contemporary smart city government projects. Implementing this technique in a distribution automation system will bring considerable advantages to the power utility.

6. FUTURE SCOPE

The security of the current ETPS relies solely on a single-phase parameter. In the future, the integration of additional security features can be explored to enhance system robustness. More advanced security measures can be incorporated into the proposed ETPS to improve its reliability. Furthermore, while the present system is designed for single-phase systems, it can be extended for application in three-phase systems.

REFERENCES

[1] Gaur, V., Gupta, E. (2016). The determinants of electricity theft: An empirical analysis of Indian states. Energy Policy, 93: 127-136. https://doi.org/10.1016/j.enpol.2016.02.048

[2] India's Load Generation Balance Report 2024-25. https://cea.nic.in/wpcontent/uploads/l_g_b_r_reports/2023/LGBR_2024_25.pdf.

[3] Dubash, N.K., Rajan, S.C. (2001). Power politics: Process of power sector reform in India. Economic and Political Weekly, 36(35): 3367-3390. http://www.jstor.org/stable/4411059.

[4] Liu, X.X., Zhu, P.D., Zhang, Y., Chen, K. (2015). A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure. IEEE Transactions on Smart Grid, 6(5): 2435-2443. https://doi.org/10.1109/TSG.2015.2418280

[5] Yan, Y., Qian, Y., Sharif, H., Tipper, D. (2012). A survey on smart grid communication infrastructures: Motivations, requirements and challenges. IEEE Communications Surveys & Tutorials, 15(1): 5-20. https://doi.org/10.1109/SURV.2012.021312.00034

[6] Salinas, S.A., Li, P. (2015). Privacy-preserving energy theft detection in microgrids: A state estimation approach. IEEE Transactions on Power Systems, 31(2): 883-894. https://doi.org/10.1109/TPWRS.2015.2406311

[7] Dangar, B., Joshi, S.K. (2015). Notice of violation of IEEE publication principles: Electricity theft detection techniques for metered power consumer in Guvnl, Gujarat, India. In 2015 Clemson University Power Systems Conference (PSC), Clemson, USA, pp. 1-6. https://doi.org/10.1109/PSC.2015.7101683

[8] Jokar, P., Arianpoo, N., Leung, V.C. (2015). Electricity theft detection in AMI using customers' consumption patterns. IEEE Transactions on Smart Grid, 7(1): 216-226. https://doi.org/10.1109/TSG.2015.2425222

[9] Erol-Kantarci, M., Mouftah, H.T. (2013). Smart grid forensic science: Applications, challenges, and open issues. IEEE Communications Magazine, 51(1): 68-74. https://doi.org/10.1109/MCOM.2013.6400441

[10] Kadurek, P., Blom, J., Cobben, J.F.G., Kling, W.L. (2010). Theft detection and smart metering practices and expectations in the Netherlands. In 2010 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT Europe), Gothenburg, Sweden, pp. 1-6. https://doi.org/10.1109/ISGTEUROPE.2010.5638852

[11] Nizar, A.H., Dong, Z.Y., Wang, Y. (2008). Power utility nontechnical loss analysis with extreme learning machine method. IEEE Transactions on Power Systems, 23(3):946-955.

[12] Gill, T.S., Shehwar, D.E., Memon, H., Khanam, S., Ahmed, A., Shaukat, U., Mateen, A., Zaidi, S.S.H. (2021). IoT based smart power quality monitoring and electricity theft detection system. In 2021 16th International Conference on Emerging Technologies (ICET), Islamabad, Pakistan, pp. 1-4. https://doi.org/10.1109/ICET54505.2021.9689908

[13] Kato, Y., Kojima, T. (2019). A chip timing recovery scheme for walsh-hadamard code division multiplexing. In 2019 3rd International Conference on Recent Advances in Signal Processing, Telecommunications & Computing (SigTelCom), Hanoi, Vietnam, pp. 1-4. https://doi.org/10.1109/SIGTELCOM.2019.8696187

[14] Pylarinos, D. (2022). Using Google My Maps as a geospatial ticket management system for scheduling and monitoring power distribution network works: Case study of Patras Area's distribution network engineering & construction section. Engineering, Technology & Applied Science Research, 12(1): 8143-8150. https://doi.org/10.48084/etasr.4642

[15] Abdellatif, A.A., Amer, A., Shaban, K., Massoud, A. (2023). A novel multivariate and accurate detection scheme for electricity theft attacks in smart grids. In 2023 International Conference on Computing, Networking and Communications (ICNC), Honolulu, USA, pp. 558-562.

https://doi.org/10.1109/ICNC57223.2023.10074440

[16] Nikovski, D.N., Wang, Z., Esenther, A., Sun, H., Sugiura, K., Muso, T., Tsuru, K. (2013). Smart meter data analysis for power theft detection. In International Workshop on Machine Learning and Data Mining in Pattern Recognition, Berlin, Germany, pp. 379-389. https://doi.org/10.1007/978-3-642-39712-7_29

[17] Bandim, C.J., Alves, J.E.R., Pinto, A.V., Souza, F.C., Loureiro, M.R., Magalhaes, C.A., Galvez-Durand, F. (2003). Identification of energy theft and tampered meters using a central observer meter: A mathematical approach. In 2003 IEEE PES Transmission and Distribution Conference and Exposition, Dallas, USA, pp. 163-168. https://doi.org/10.1109/TDC.2003.1335175

[18] Huang, L.J., Qin, H., Pan, Z., Yu, M. (2022). Electricity theft detection based on iterative interpolation and fusion convolutional neural network. In 2022 7th International Conference on Power and Renewable Energy (ICPRE), Shanghai, China, pp. 567-571. https://doi.org/10.1109/ICPRE55555.2022.9960403

[19] Khan, M.H., Pathan, E., Asad, M., Sadiq, M.A., Qureshi, A.A., Shahid, M., Pathan, A.K., Shaikh, N.I. (2021). Seamless transition between islanded and grid connected three-phase VSI-based microgrids. Engineering, Technology & Applied Science Research, 11(2): 6882-6888. https://doi.org/10.48084/etasr.4045

[20] Abdellatif, A.A., Chiasserini, C.F., Malandrino, F., Mohamed, A., Erbad, A. (2021). Active learning with noisy labelers for improving classification accuracy of connected vehicles. IEEE Transactions on Vehicular Technology, 70(4): 3059-3070. https://doi.org/10.1109/TVT.2021.3066210

[21] Komolafe, O.M., Udofia, K.M. (2020). A technique for electrical energy theft detection and location in low voltage power distribution systems. Engineering and Applied Sciences, 5(2): 41-49. https://doi.org/10.11648/j.eas.20200502.12

[22] Hanzo, L.L., Yang, L.L., Kuan, E.L., Yen, K. (2004). SpaceTime spreading aided singlecarrier wideband CDMA communicating over multipath Nakagami fading channels. In Single- and Multi-Carrier DS-CDMA: Multi-User Detection, Space-Time Spreading, Synchronisation, Networking and Standards, Wiley-IEEE Press, USA. pp. 279-310. https://doi.org/10.1002/0470863110.ch8

[23] Boubaker, S., Jouili, K. (2024). Fuzzy logic energy management system-based nonlinear sliding mode controller for the stabilization of DC microgrids. Engineering, Technology & Applied Science Research, 14(4): 15408-15414. https://doi.org/10.48084/etasr.7658

[24] Pylarinos, D. (2023). Investigating the effect on productivity of a geospatial ticket management system for power distribution network studies. Engineering, Technology & Applied Science Research, 13(5): 11616-11621. https://doi.org/10.48084/etasr.6202

[25] Linh, N.T., Long, P.V. (2023). A novel solution method for the distribution network reconfiguration problem based on an objective function and considering the cost of electricity transmission. Engineering, Technology & Applied Science Research, 13(6): 12366-12372. https://doi.org/10.48084/etasr.6568