



**ASHESI**

**ASHESI UNIVERSITY**

**ELECTRICITY THEFT DETECTION IN LOW VOLTAGE NETWORKS**

**USING A SIMULATION APPROACH**

**CAPSTONE PROJECT**

B.Sc. Electrical and Electronic Engineering

**Keziah Asantewaa Boamah**

**2022**

**ASHESI UNIVERSITY**

**ELECTRICITY THEFT DETECTION IN LOW VOLTAGE NETWORKS USING A  
SIMULATION APPROACH**

**CAPSTONE PROJECT**

Capstone Project submitted to the Department of Engineering, Ashesi University in partial fulfilment of the requirements for the award of Bachelor of Science degree in Electrical and Electronics Engineering.

Keziah Asantewaa Boamah

2022

## DECLARATION

I hereby declare that this capstone is the result of my own original work and that no part of it has been presented for another degree in this university or elsewhere.

Candidate's Signature:

.....

Candidate's Name:

Keziah Asantewaa Boamah

.....

Date:

15/05/2022

.....

I hereby declare that preparation and presentation of this capstone were supervised in accordance with the guidelines on supervision of capstone laid down by Ashesi University.

Supervisor's Signature:

.....

Supervisor's Name:

.....

Date:

.....

## **ACKNOWLEDGEMENTS**

I want to thank God Almighty, who has brought me this far in my capstone journey and gave me the strength to complete a considerable amount of work. I would also like to earnestly acknowledge the sincere efforts and valuable time assigned by my supervisor, Mr. Francis Gatsi.

I am grateful for his guidance, ideas, advice, and feedback. Also, I would like to mention the support system of my family, who have always been there for me. Special appreciation goes to my lecturers, Mr. Richard Awingot and Mr. Bright Tetteh and my close friends for their help, support, and insightful advice.

Finally, I would like to thank everyone who helped and motivated me to work on this project.

# Table of Contents

<b>DECLARATION</b> .....	i
<b>ACKNOWLEDGEMENTS</b> .....	ii
<b>CHAPTER 1: INTRODUCTION</b> .....	1
1.1 Background .....	1
1.2 Problem Definition.....	2
1.3 Objectives of the project.....	2
1.4 Expected outcomes of the project work.....	3
1.5 Motivation for project topic.....	3
1.6 Research methodology to be used .....	4
1.7 Scope of work.....	4
<b>CHAPTER 2: LITERATURE REVIEW</b> .....	5
<b>CHAPTER 3: METHODOLOGY</b> .....	8
3.1 Approach and Design Process.....	8
3.2 Assumptions.....	9
3.3 System Requirement.....	9
3.4 System Design Architecture .....	10
3.4.1 Hardware Design.....	10
3.4.2 Components Choices .....	11
3.4.3 Software Implementation.....	14
<b>CHAPTER 4: SIMULATION SETUP AND IMPLEMENTATION</b> .....	17
4.1 Design Implementation of Loads and Power Line Filters .....	17
4.2 Design Implementation of High Frequency circuit .....	18
4.3 Design Implementation of Current Sensor and Serial Communication Module .....	19
4.4 Computation of Power Spectral Density.....	20
4.5 Simulation Setup in Proteus Software .....	21
4.6 Simulation Setup in Simulink .....	24
<b>CHAPTER 5: RESULT ANALYSIS AND DISCUSSION</b> .....	25
<b>5.1 Results Obtained from Various Cases and Discussion</b> .....	25
5.1.1 Results showing Case Two and Case Three .....	25
5.1.2 Results showing the variations in the PSD graphs due to different power ratings of the loads	26
5.1.3 Results indicating the changes in the Frequency Component.....	28

5.1.4 Results showing the variations in the PSD graphs due to different frequency values .....	30
5.1.4 Tabulated results of the average PSD values for all the Test Cases .....	31
5.2 Discussion.....	32
<b>CHAPTER 6: CONCLUSION</b> .....	<b>34</b>
6.3 Recommendations .....	35
<b>REFERENCES</b> .....	<b>36</b>
<b>APPENDIX</b> .....	<b>41</b>
A.1 MATLAB Code for Case One.....	41
A.2 MATLAB Code for Case Two .....	43
A.3 MATLAB Code for Case Three.....	45
A.5 Code for Current Sensor .....	49
A.6 Interviews from Electricity Company of Ghana Personnel.....	50

# CHAPTER 1: INTRODUCTION

## 1.1 Background

Electrical energy is one of the most vital resources in our everyday lives, which also serves as the essential pillar in the effective running of industries. As the demand for electricity increases, we find an increasing occurrence of power theft. Power loss refers to the difference in the generated power and what is effectively billed. The power system's losses include technical and non-technical losses (NTLs) [1]. The technical losses involve the losses that occur naturally caused due to the malfunction of the electrical equipment used from the generating station to the distributing stations. These technical losses occur in power dissipation in resistive components, leakages due to improper isolation, and others.

Electricity theft is mainly associated with non-technical losses, also known as commercial losses. These activities include tampering with meters, stealing electricity bypassing a meter, billing irregularities, and unpaid bills [2]. Studies show that both developed and developing countries suffer from NTLs. There is a loss of more than \$96 billion yearly worldwide due to electricity theft [3]. Theft of electricity is detrimental since it results in a significant loss of revenue for the energy company. This practice reduces the effective operations of the company since they cannot make the adequate profit they need for the distribution of power [4].

Over the years, prepaid meters have been adopted to curb these losses. However, these meters are still at risk of attacks that make power theft prevalent [3]. It has also been discovered that meter bypassing is the most common form of theft. It only takes a personnel's physical inspection of the meters to detect any such occurrence [5]. Meaning until there is an adequately conducted inspection in the homes of such offenders, the utility company will not be able to detect it. Also,

in meter bypassing, power may be tapped directly from the distribution lines, and for this matter, the utility company will not be able to detect the theft.

This project seeks to conduct investigations and analyses on how the injection of a high-frequency signal into low voltage networks can help detect and hence mitigate the occurrences of power theft on these low voltage lines. The main power theft occurrences that will be explored are meter bypassing and direct hooking.

## **1.2 Problem Definition**

Energy crisis is a significant problem faced in our world today; however, one of the most escalating problems many developing countries like Ghana face is the high rate of electricity theft. Electricity theft affects the income generation capacity of the country's utility company. These losses also affect the quality of electricity supply, electrical load on the generating station, and the tariffs imposed on the electricity consumed by customers.

## **1.3 Objectives of the project**

This research project investigates the various types of NTLs associated with electricity theft, particularly meter bypassing and hooking (direct tapping from the line). This project also aims at designing an effective system that predicts and detects meter bypassing and hooking in real-time monitoring on low voltage networks. The specific objectives are as follows:

1. To understand the techniques involved in power theft, especially meter bypassing and hooking.
2. To determine whether using an algorithm involving a high frequency signal and the Power Spectral Density is effective in detecting theft.



3. To determine how a high-frequency signal affects different kinds of load with different power ratings.

#### **1.4 Expected outcomes of the project work**

It is expected that the following outcomes will be achieved at the end of this project:

1. In-depth research of the problem which results in knowledge acquisition to nurture innovation in finding the best technique for this problem
2. A proper and detailed simulation of design, including various valuable calculations
3. A deeper understanding and detailed inference in the use of the suggested algorithm and approach

#### **1.5 Motivation for project topic**

Electrical energy is one of the most used forms of energy globally. As the population in Ghana keeps growing, the demand for electricity increases. Thus, the electricity company must be able always to supply the right amount of energy to their customers. This will reduce cases of power outages in the form of load shedding. To supply energy to the country, they purchase the power from the power generators, which involves money. As they pay to get the power to supply, those they supply need to pay back the amount they purchased. When people do not pay and use crude methods to get the electrical supply for free, the electricity company runs at a loss. Hence, this affects their ability to supply a quality amount of electricity to the country. This research project thus, seeks a way to combat such problems using a detection algorithm, especially as meter bypassing is a common form of electricity theft.

## **1.6 Research methodology to be used**

1. Systematic Literature Review: Research from various related articles to gain more information on this project.
2. In-depth interviews and questionnaires: An interview with individuals from the utility company to understand the problem better and what they go through to prevent people from engaging in such activities.
3. Computer modeling and simulation

## **1.7 Scope of work**

This project is limited to designing a system that detects theft using electronics simulation and signals analysis. This system is implemented using an algorithm to monitor, detect, and analyze data derived from a sensor to perform calculations needed for the appropriate inference. The design focuses more on low voltage networks and not on the smart meters directly.

## CHAPTER 2: LITERATURE REVIEW

Power theft is a significant issue that plagues the power sector and the country as it causes losses to the utility companies. According to a survey conducted by JoyFm last year, they were informed by the regional director of the Accra East branch of the Electricity Company of Ghana (ECG) that they lost about four million Ghana cedis to theft within a space of nine months [6]. That is a tremendous amount of revenue and what is worse is that this amount was generated for just one region. Therefore, the government is forced to provide subsidies to the power sector to maintain a reasonable price of electricity in some cases.

Through an interview with an ECG personnel, the discovery was that improvements had been made in the energy sector over the years. Initially, energy meters were electromechanical, consisting solely of postpaid meters. These meters had magnetic disks and high exposure to electricity theft. The ECG company then thought it wise to discard all such meters and introduced electronic/electric meters, and those were made of both postpaid and prepaid. It was observed that the prepaid meters still had some challenges as individuals still engaged in stealing power. Thus, smart prepaid meters were introduced. These meters solved both issues of billing and meter tampering. Even though the smart meters cover the functionality of detecting meter tampering, they cannot detect meter bypasses, which tend to be the most rampant theft. With the meter bypassing, the input terminals of the load are disconnected and tapped from the lines going into the meter's terminal input. Meter bypassing and direct hooking typically occurs on low voltage lines, thus the reason for this project's scope.

Several papers have discussed some methods that have been explored to detect electricity theft in low voltage networks. This section thus analyzes the effectiveness of these systems developed in the papers.

Uvais, in his article, developed a controller-based system that takes the voltage and current readings from the low terminal (LT) side of the transformer and energy meters. Theft is detected based on additional voltage drops and current in the distribution lines [7]. Thus, the voltage drops and additional current flows in the low voltage lines are calculated, and theft is detected if it exceeds a threshold. The controller sends a signal to the circuit breaker to prevent electrical energy from flowing. This is a good approach; however, due to voltage compensation, which will be explained later, the approach may not be an ideal one.

Another paper discussed a detection algorithm used to detect meter bypassing and hooking with the help of consumer load profiling. A high voltage pulse is sent to the distribution line using a tapping transformer. Theft is then detected by forming a load profile of the amount of power used by the consumer, and readings are taken to check for abnormalities. A change in the consumer's load profile will indicate theft at the customer's end [8]. The voltages used in this paper do not depict the actual voltages used in practicality. Thus, it is not highly accurate since the distribution networks are approximately 13kV to 11kV, and a typical household runs on 110V [9].

In the article, *The Detection of Power Theft using Power Line Communication*, the author worked on detecting power theft through the injection of a narrowband power line carrier signal. Theft could be detected with a differential change in the amplitude of the injected narrowband signal [13]. Additional loads reduce the signal amplitude, which was sensed using gain detectors [13].

With inspiration from the last article written, this project also works on detecting theft by injecting a high-frequency signal into the low voltage lines. However, unlike the paper, this project uses an algorithm that involves a Power Spectral Density (PSD) to detect whether there is theft or not in a system. The frequency component is considered in these projects because it is vital in

power systems. A change in load leads to a change in the frequency component. There is a greater emphasis on frequency use than on voltage because momentary voltage sags accompany voltage drops. These sags are usually compensated with equipment such as capacitor banks, tap changers, and FACTS compensators to make the power system stable [13]. Thus, using voltage as an element for analysis may not be as accurate as compensation exists in the voltage across the load [13].

This project focuses primarily on meter bypassing and direct hooking forms of electricity theft. For meter bypassing, the service power line connected to the energy meter is disconnected and instead connected to the wire before the meter panel board. Thus, the meter cannot measure the complete units of electrical energy being consumed. Direct hooking also is when customers tap into the power line from any point ahead of the meter, and here, energy consumption is not measured. The Power Spectral density through the use of frequency helps check when either of these two practices has occurred. The power spectrum describes the distribution of power into frequency components in that signal. The spectrum also offers valuable description or information about the signal, and thus, analyzing the spectrum helps detect theft.

## CHAPTER 3: METHODOLOGY

### 3.1 Approach and Design Process

This project investigates the accuracy of using power spectral density on high-frequency signals to detect theft. This section details the methods and approach to developing the proposed system using the appropriate components. The service line, which is supplied with a voltage of 220V, is placed between two LC traps to detect theft, as shown in Fig.3.1. One of these LC traps is placed near the power line pole, while the second LC trap is placed at the output terminals of the meter. The low pass LC traps are designed to prevent the high-frequency signal from affecting other components and home appliances connected to the power line's receiving end [12]. The high-frequency signal with a low amplitude is generated and injected after the first LC trap near the input terminal of the meter. Two current sensors are made use of, and the values from these current sensors help in the calculation of the PSD. The high-frequency circuit consists of a coupling transformer used to step up the transmission lines signals to ensure that the impedance at the power source is equal to the impedance at the load.

The current sensors are connected to the ATmega32 microcontroller, which is the brain of the project. The values from the current sensor are transferred from proteus to MATLAB through a serial communication mechanism. These values are stored in a file in MATLAB, and then the PSD algorithm is performed on the values. This system is implemented in the proteus software due to the availability of most components. The software can simulate most electrical components and is used for a quick checkup of code written for microcontrollers.

### **3.2 Assumptions**

In this project, the focus is to analyze and monitor low voltage lines for electricity theft. For a suitable design to be developed, several assumptions were derived, and these assumptions are listed below:

- The system considers a residential load power system.
- The design is for a single-phase power system.
- The system considers the low voltage network for one residence and not the entire community; that is, the low voltage network for one house.
- The energy meter is placed right before the home load.
- The load, both the illegal and the household load, is represented using several parallel resistors, representing the active power ratings for appliances in the home.

### **3.3 System Requirement**

For a project to be successful, some requirements should be met, and here, the focus is more on the system requirements. The system requirements consider the features that the solution must have to ensure the proper functioning of the system. These requirements are critical to the project's success because they serve as a reference point to keep in check what is required for the project to be thriving. The system requirements are as follows.

- The system's design should read, analyze, and record accurate values in real-time and when the load is varied.
- The capacity of the power line filters should be able to eliminate the high frequency being injected into the transmission lines.

- The algorithm should be able to make the necessary inferences to detect meter bypassing on the transmission lines.
- The consumer's load should remain unaffected even with the high frequency.

### 3.4 System Design Architecture

#### 3.4.1 Hardware Design

The hardware architecture of this research project is denoted by a power supply, microcontroller system connected to an energy meter, a load source, serial communication medium, virtual terminal, and current transformers. The energy meter is placed between two LC traps to prevent the high-frequency signal generated in the circuit from affecting the load [30].

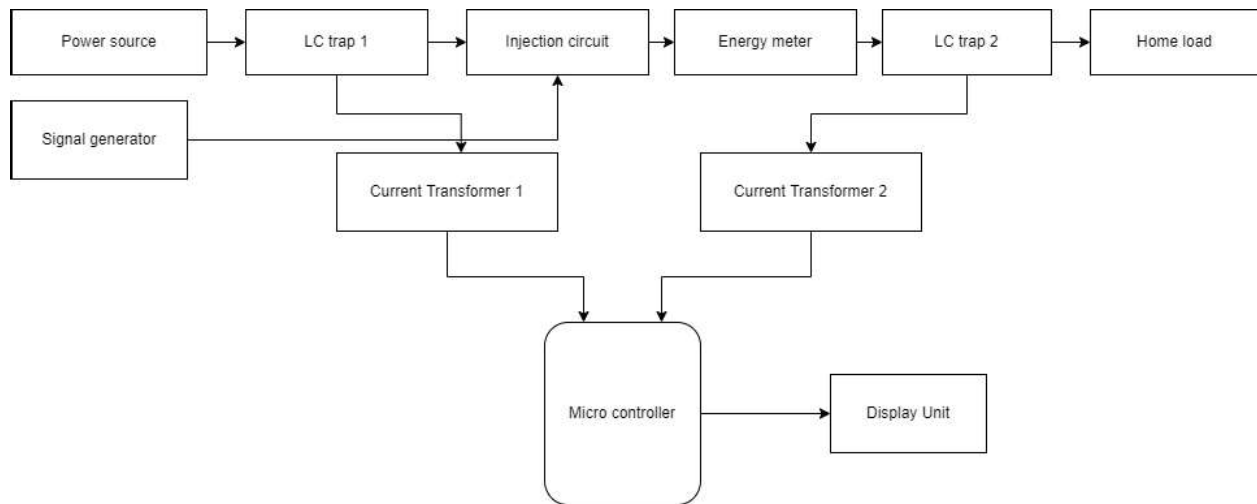


Fig.3.1 A block diagram of the hardware design



### 3.4.2 Components Choices

#### 1. Current Sensor

ACS772LCB-100B current sensor is a high accuracy, hall-effect based, 200kHz bandwidth galvanically isolated current sensor IC with 100uOhms current conductor. It is bidirectional and can measure both AC and DC in both negative and positive directions. It has an operational supply voltage of 5V and a maximum output voltage of 6.5V with a sensitivity of 20mV/A. It has a total pin count of 5 with a primary sampled current of +/-100A [10].



Fig.3.1 ACS772 Current Sensor and its Pinout Diagram

#### 2. ATmega32 microcontroller unit

It is an 8-bit microcontroller that can control and interact with sensors, motors, relays, and other electronic devices [11]. This microcontroller unit has a flash memory of 32KB, 1kB EEPROM, 54/69 general-purpose I/O lines with 32 general purpose working registers, and three flexible timers or counters.

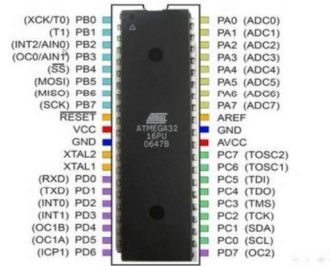


Fig.3.2. Pinout diagram of ATmega32 microcontroller

### 3.LC traps

The LC traps offer a high impedance to the high frequency injected in the circuit to ensure the frequency does not affect the components. Two components make up the LC traps: the power line filter and an LC-type resonant filter, and they help filter out the injected frequency. The B84112GG136 power line filter will be used in this process. It is a 50Hz/60Hz power line filter with a 36A 250VAC threaded stud flange mount filter. However, in the simulation, capacitors and inductors are used to represent the LC traps [14].



Fig.3.3. B84112GG136 Power filter

### 4.COMPIN

In Proteus, COMPIM is used to model physical COM interfaces [15]. It captures and buffers serial signals before presenting them to the electrical circuit. All serial data coming from the CPU or the

UART model will be transmitted over the computer's serial ports. Baud rate conversion is possible when employing the COMPIM model [15]. On the other hand, Virtual Terminal is a Proteus tool that can be used to view data from Serial Port and transfer data to Serial Port [16].

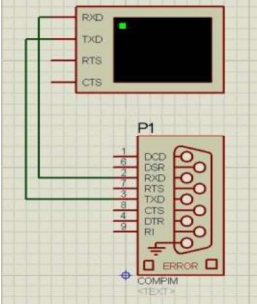


Fig.3.4. COMPIN connected to Virtual Terminal in Proteus

5. Coupling transformer

Coupling transformers are usually used to step-up transmission line signals [17]. They are also known for matching the impedance in electronic circuits. These transformers can achieve a higher gain and are efficient in their operation.

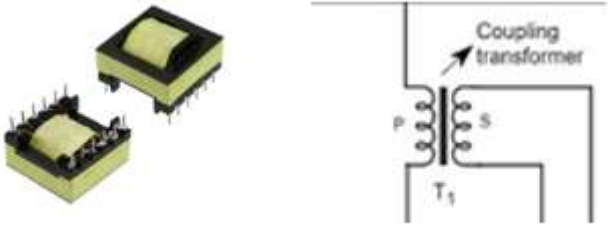


Fig.3.5. Coupling transformer

### 3.4.3 Software Implementation

The algorithm used to detect theft in this solution involves the use of Power Spectral Density (PSD). The power content of a signal is measured using a Power Spectral Density (PSD) [18]. The PSD signal describes how a power signal is represented in terms of frequency, which is usually stated in watts per hertz. A truncated Fourier transform is used to calculate the frequency of this signal, in which the signal is integrated across a finite interval  $[0, T]$  [30]. In a power spectral density, the FFT's amplitude is multiplied by its complex conjugate and normalized to the frequency bin width (PSD). This enables precise comparison of random vibration signals of various signal lengths [19]. The following steps are outlined below to perform the PSD algorithm, and the flowchart in Fig.3.6 gives a more detailed framework of these steps.

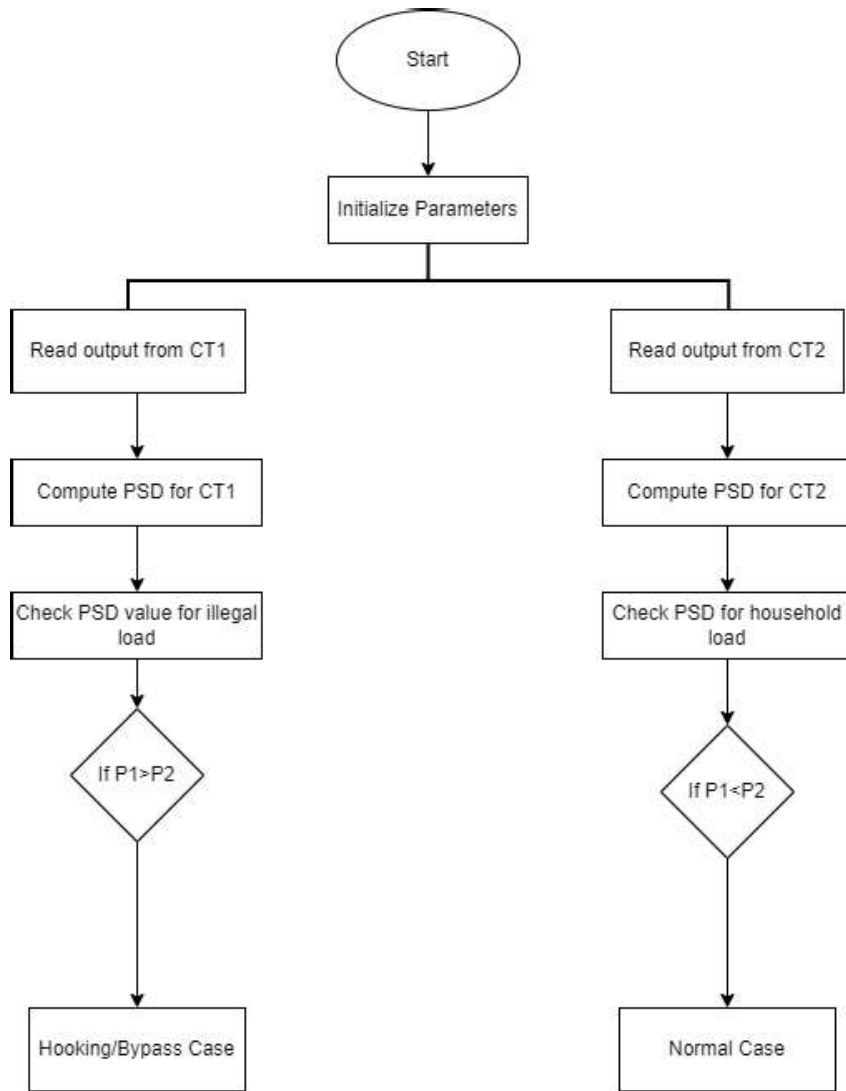


Fig.3.6. A diagram of the flow chart design

**Step One:** The output values from the current transformers are read and recorded. They are stored and ready for further calculations.

**Step Two:** The PSD calculations are performed on the output values from the two current transformers, CT1 and CT2. Therefore, the PSD uses values from three ammeters in all, the one in the injection circuit, the one for the home load, and the one where the illegal load will be placed. The CT1 will be placed between the injection circuit and that gives  $I_1$  and the illegal load while

CT2 is placed at the home load end, which gives  $I_2$ . Thus, we have  $P1(f)$  representing the PSD value for the ammeter values in  $I_1$  and  $P2(f)$  representing the PSD value from the ammeter values in  $I_2$ .

**Step Three:** In this stage, comparisons are made to ensure a logical check. This is because the PSD measures the energy of a signal. Thus, if the signal's energy is more, meaning a load has been hooked directly, the PSD value in this instance becomes greater. Also, since there are loads connected to the meter, the PSD value should ideally be greater in this instance. So, if the PSD is lesser, that means the meter has been bypassed. The simple analysis bowls down to the following conclusion in Table 3:

Table 3: Decision Algorithm

Logic	Inference
If $P1(f) > P2(f)$	“Normal case”
If $P1(f) < P2(f)$	“Hooking case or illegal load is attached”

**Step Four:** Based on the condition, it helps predict when there is a theft case or when it is a normal case. The frequency is varied with a range of values to ensure the system's efficacy. These values are based on international standards such as CENELEC 50065-1, which assigns a frequency spectrum of 3 kHz to 148.5 kHz for communication via Low Voltage lines [20].

## CHAPTER 4: SIMULATION SETUP AND IMPLEMENTATION

There were some constraints in building a physical model of the system, and these constraints were due to the unavailability and the high cost of some components. However, several simulations and test cases were carried out to ensure the system's effectiveness. The circuit was developed, tested, and used to produce relevant results for analysis using proteus software. Calculations were made in selecting some electrical components, such as the inductors and the capacitors for the LC traps. Calculations were also made to confirm the values that the software was generating.

### 4.1 Design Implementation of Loads and Power Line Filters

An *electrical load* is a device that consumes electrical energy. In other words, it is a device that consumes electrical energy in the form of current and converts it into useful work such as heat, light, work, and other types of energy [21]. An electrical load could be resistive, inductive, capacitive, or a mix of the three. According to an assumption made for this project, the focus is on resistive loads mainly because most appliances in the homes use active power instead of reactive power since it is the quantity of unused power found in reactive components. Moreover, circuits containing reactive components only alter the voltage and current waveforms, and since this project's studies only the frequency component, using reactive components may not be highly required [22]. As a result, various typical household loads were employed in each example to represent the loads that should be used in our houses. According to the wattage worksheet provided by LCEC, some major appliances were selected, including the light bulb, the refrigerator, the ceiling fan, the water pump, and others [23]. These appliances were rated at 60W, 700W, 800W, 1000W, and more. Thus, to make simulations easier, resistors were used to represent each load and placed in parallel. The resistance values were calculated based on the power ratings given using (1). Computations were made to compare the calculated current values to the measured

current values in proteus. Fig. 4.1 shows the connection of the resistors in parallel in the circuit in proteus.

The power line filters are designed from resonant-type LC and low pass circuits. The base values of L and C were obtained from the primary reference paper [12]. However, at each varied frequency value, the values of L and C were changed to suit the new frequency using (2). The purpose of the LC traps is to eliminate the high-frequency signal that has been injected into the circuit.

$$R = \frac{V^2}{P} \quad (1)$$

$$f_R = \frac{1}{2\pi\sqrt{LC}} \quad (2)$$

#### **4.2 Design Implementation of High Frequency circuit**

As mentioned earlier, frequency is an essential component in power systems. The frequency injection circuit is made of low amplitude, high-frequency signal, where the frequency was chosen to be 21.7kHz and the voltage 10.6V. The value of the frequency and voltage were selected based on the primary reference paper but varied in different instances [12]. The injection circuit also consists of a coupling transformer with capacitors and a resistor. The coupling transformer in the injection circuit ensures that the impedance at the load is the same as the impedance at the power source by stepping up the voltage. Since the voltage we supply in the injection circuit is smaller, the coupling transformer ensures that it steps up back in the primary circuit through impedance matching. There are ammeters in the injection circuit to measure the amount of current flowing through the circuit.



### 4.3 Design Implementation of Current Sensor and Serial Communication Module

The ACS772 current sensor employs the Indirect Sensing approach to calculate the current [24]. The Hall-effect current sensor IC uses a linear, low-offset Hall sensor circuit to sense current. The Hall effect sensor detects a magnetic field created by the current flowing through this copper conduction path [25]. The Hall sensor, used to measure current, generates a voltage proportionate to the observed magnetic field [25]. Thus, the current sensor was placed in series with the circuit and programmed in the Arduino IDE. The Arduino IDE was used because of its ability to generate hex files required in the proteus software. In Arduino, a library called the MightyCore was downloaded to access the Atmega32 board, and it was configured before the code could run in Arduino. According to the code, the current sensor is being supplied with 5V; thus, at no load, the value is 2.5. The sensor thus, uses the computation,  $currentValue = ((adcVoltage - offsetVoltage) / sensitivity)$  to calculate the value of the current passing through the circuit. Where the offsetVoltage is 2.5 and sensitivity is equal to the sensor's sensitivity, which is 20mV/A. The hex file generated from Arduino is then run in proteus to see the values the current sensor is reading.

To read the values running, one can use the serial monitor in Arduino or a virtual terminal in proteus. However, these need to be configured, and that is when the serial communication comes in. A virtual serial port driver was downloaded, and it makes use of software-based virtual null-modem cables to generate virtual COM ports and connect them in pairs [26]. Thus, local bridges were created for COM1 and COM3 and COM2 and COM4. In proteus, the COMPIN is what aids with serial communication. Thus, transmitting at a baud rate of 9600, the port was selected. The corresponding port receives the data for each port selected to send the data. The values are seen in the virtual terminal when this is run in proteus. However, choosing the corresponding port in Arduino allows viewing the serial monitor. The whole purpose of using serial communication was

to interface proteus with MATLAB since the calculation of the Power spectral density was to be done in MATLAB.

#### 4.4 Computation of Power Spectral Density

The computation of the PSD was done in MATLAB after reading the current sensor values through the serial ports. A file was created in MATLAB to store these current values. Here, the PSD of the continuous function is found using the Fourier transform of its auto-correlation function, and that can be seen in (3).

$$P(f) = \sum_{k=0}^{N-1} r(k) e^{-j2\pi f T_s k} \quad (3)$$

Where  $f$  is the frequency in Hz,  $T_s$  is the sampling time, and  $r(k)$  is the autocorrelation sequence.  $r(k)$  is derived in (4) [12].

$$r(k) = E [x(n) x^*(n - k)] \quad (4)$$

with  $x(n)$  being the input data,

$E[.]$  denoting the expectation, and  $(.)^*$  representing the complex conjugate operators [30]. The formula helps us derive the estimate for the spectral density of a signal, and the results are plotted in a graph which will be analyzed.

#### **4.5 Simulation Setup in Proteus Software**

Using the proteus software, the modelling approaches discussed earlier were put together to form a complete design. This design was broken into several case scenarios to have a broader range of test conditions to validate the solution. The case scenarios are discussed below.

##### **Case One:**

This case comprises a simple parallel resistive load configuration connected to a voltage source. This circuitry represents the distribution configuration of the power system where the distribution lines are delivered straight to the load in the homes through the electrical meters. A current sensor was placed in series in the circuit to measure the current signal in the circuit and this can be seen in Fig.4.1. The values were sent to the microcontroller and then using serial communication, the values were transferred to MATLAB for further computations. The COMPIN component in proteus aids in the serial communication.

##### **Case Two:**

Case two introduces the high frequency injection into the circuit. With the high frequency, the LC traps are also placed in the system to prevent the damage to the electrical loads. Here, there are two current sensors, and one is placed between the injection circuit and the first LC trap, and the other is placed before the home load respectively. The values from the current sensors are used to compute the PSD coefficients in MATLAB with the help of serial communication.

##### **Case Three:**

Case three is a buildup of case two where there is a presence of an illegal load. Thus, in this circuit, the current sensors are placed between the high frequency circuit and the position of the illegal

load. To get the illegal load, the power ratings of the light bulb and the fan were placed in parallel and thus, the equivalent resistance was found and that is what is represented as illegal load. The home load, however, was removed, indicating that the meter was completely bypassed. After the values of the current have been computed with PSD, the PSD values are compared.

### Case Four

Case four is basically a set of tests to either validate the assumptions and hypothesis derived or to invalidate it. Therefore, in case four, the values of the power ratings are varied for both the home load and the illegal load. PSD is computed at the end of each scenario.

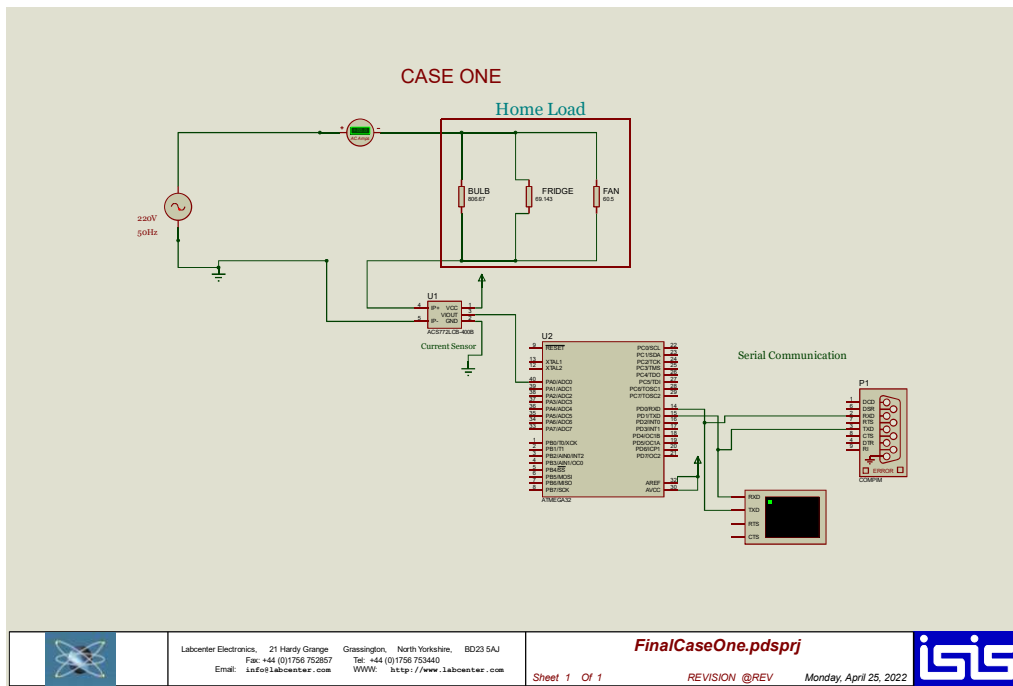


Fig.4.1 A figure of the simulation for Case One in Proteus

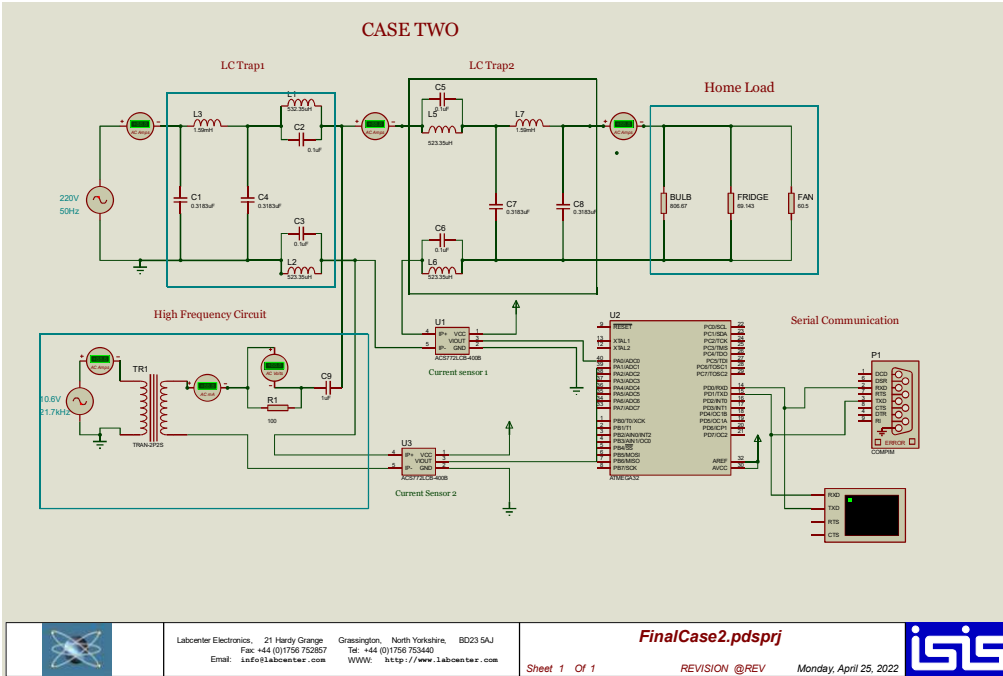


Fig.4.2. A figure of the simulation for Case Two in proteus

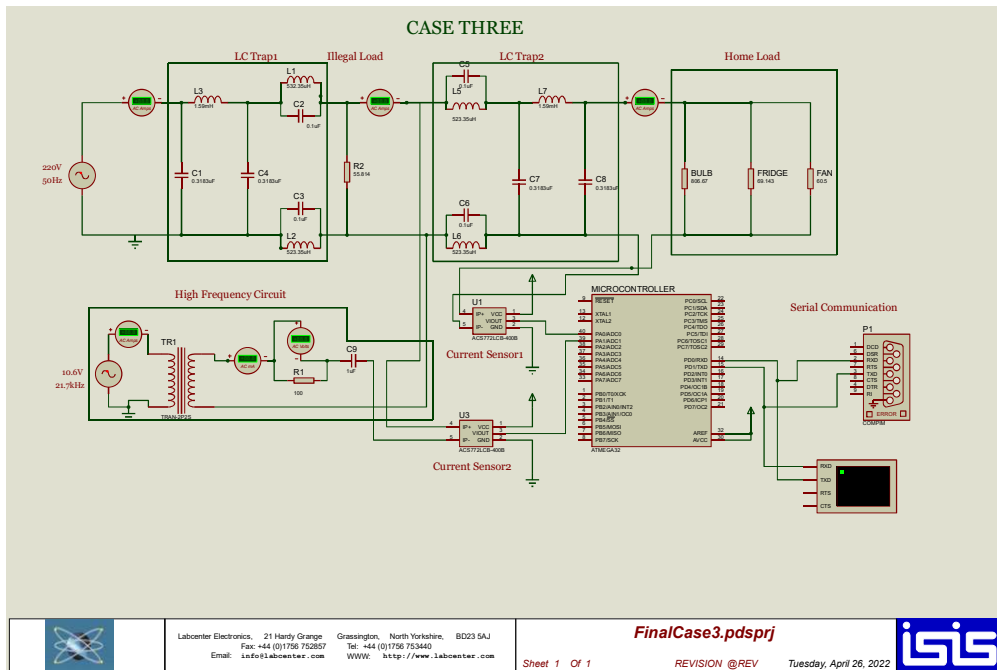


Fig.4.3. A figure of the simulation for Case Three in Proteus

#### 4.6 Simulation Setup in Simulink

The simulation was also conducted in MATLAB using Simulink. This simulation was to confirm the accuracy of the results obtained from the Proteus simulation. The same circuitry was implemented in Simulink using electrical components, displays, scopes, ammeters, and function blocks. The design can be seen in the figure below. In Simulink, the same loads were used to get accurate results, while the frequencies varied. Therefore, the illegal load was kept at 1000W, and the home load was kept at 100W. For these ratings, the frequency component in the injection circuit was changed from 21.kHz to 11.7kHz and 31.7kHz. At each change in the frequency, the values of the inductors and capacitors were also changed according to (2).

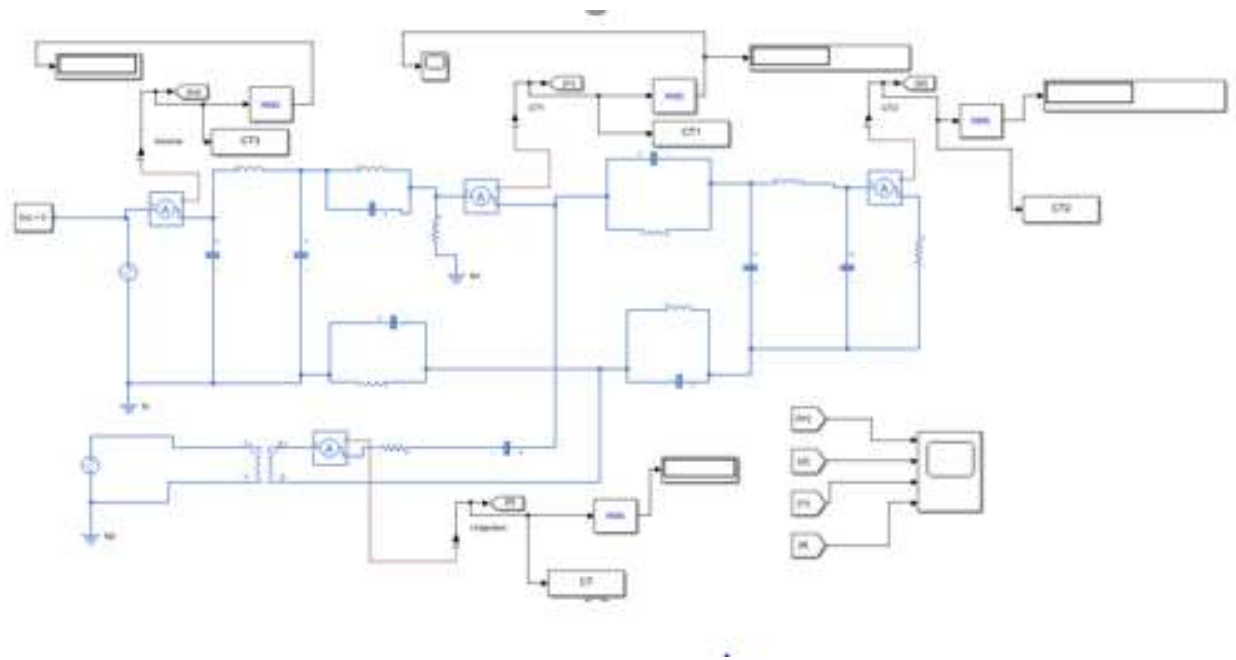


Fig.4.4. A figure of the simulation In Simulink

## **CHAPTER 5: RESULT ANALYSIS AND DISCUSSION**

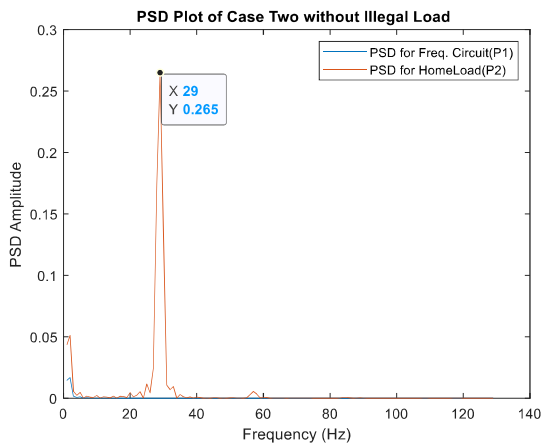
The high-frequency injection with the use of Power Spectral Density needed to be tested to ascertain whether it is a reasonable solution in detecting electricity theft. For an accurate simulation to be carried out, various test cases were implemented. The simulations were broken down into cases to get a holistic view of the analysis. Below, the multiple cases are discussed, and their results are analyzed.

### **5.1 Results Obtained from Various Cases and Discussion**

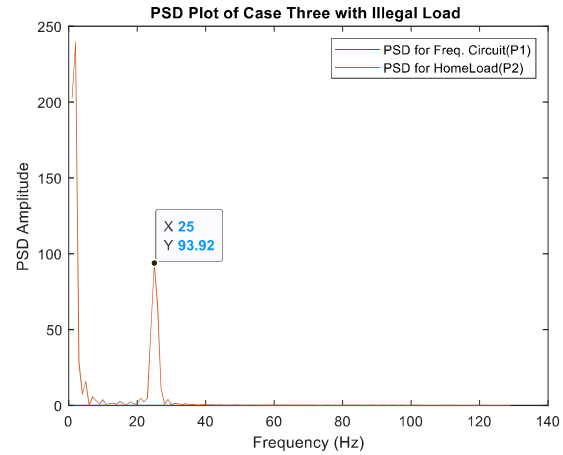
The cases were analyzed systemically, and the results are based on the test cases discussed in chapter four. Two different types of graphs were plotted in MATLAB for the cases: the PSD graph using a log scale and one using a linear scale. The logarithmic scale illustrates the rate of change in the number of frequency components over time, whereas the linear scale depicts the absolute number of frequency components over time [27].

#### **5.1.1 Results showing Case Two and Case Three**

Fig. 5.2 shows the PSD plots for when there is an unauthorized load and when there is not. Here, the power rating of the home is 0W for Case three, while the illegal load is 3.64kW. For Case Two, there is no illegal load, and the home load is rated at 860W. Fig.5.2 helps compare the PSD amplitudes of a typical meter bypassing case. Fig.5.3, on the other hand, portrays the comparisons between the two cases but on a log scale.

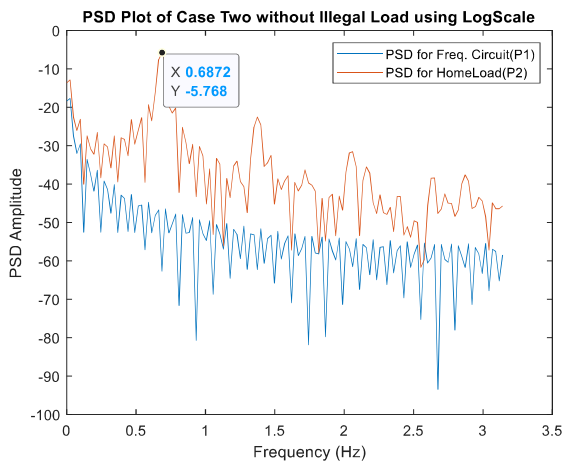


(a)

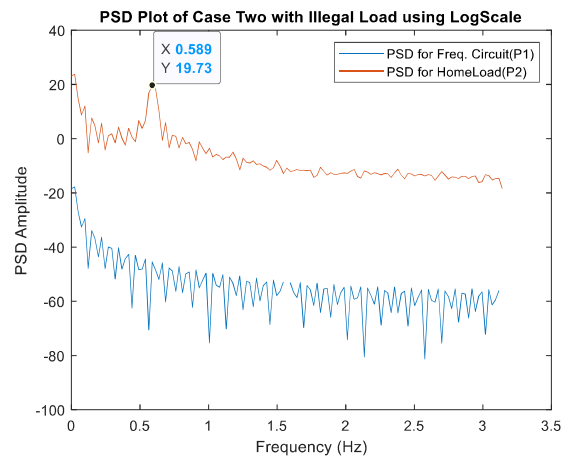


(b)

Fig. 5.1 PSD plots of Case Two (a) and Case Three (b) on a linear scale



(a)



(b)

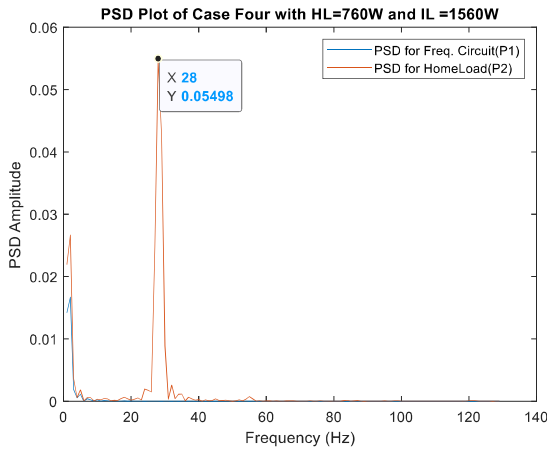
Fig. 5.2 PSD plots of Case Two (a) and Case Three (b) on a log scale

### 5.1.2 Results showing the variations in the PSD graphs due to different power ratings of the loads

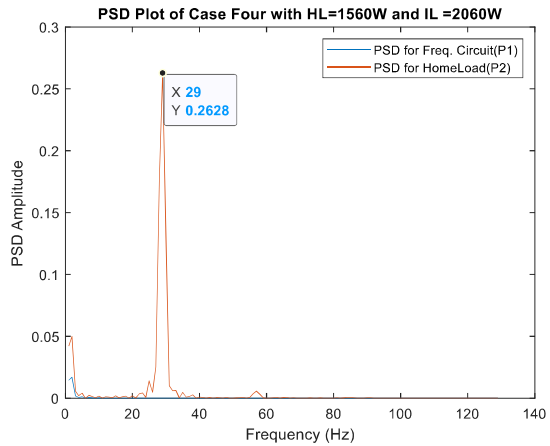
In this section, the loads are varied to test the effects of increasing the demand for power consumption, especially for illegal load conditions. In Fig.5.4a and Fig.5.5a, the home load is rated 760W, while the illegal load is 1.56kW. In Fig.5.4b and Fig.5.5b, the home load is rated 1.56kW



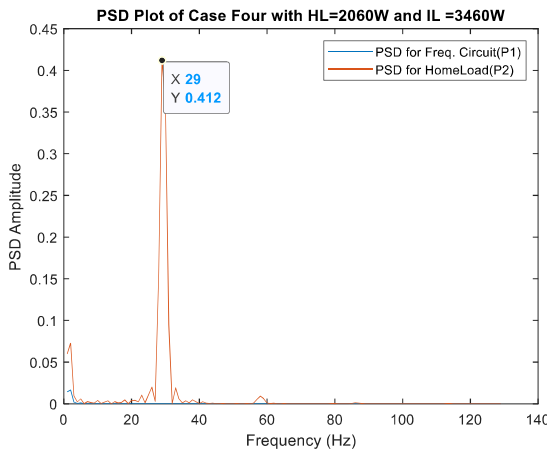
while the illegal load is 2.06kW. In Fig.5.4c and Fig.5.5c, the home load is rated 2.06kW while the illegal load is 3.64kW. In Fig.5.4d and Fig.5.5d, the home load is rated 2.06kW while the illegal load is 860W. All these power ratings are based on calculations using (1), and these power ratings are derived from the addition or reduction of loads using the wattage worksheet.



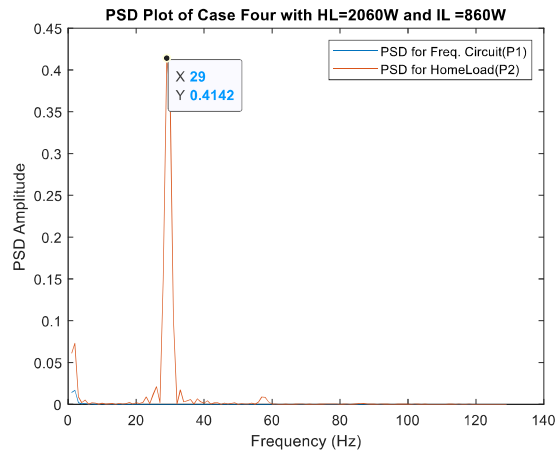
(a)



(b)

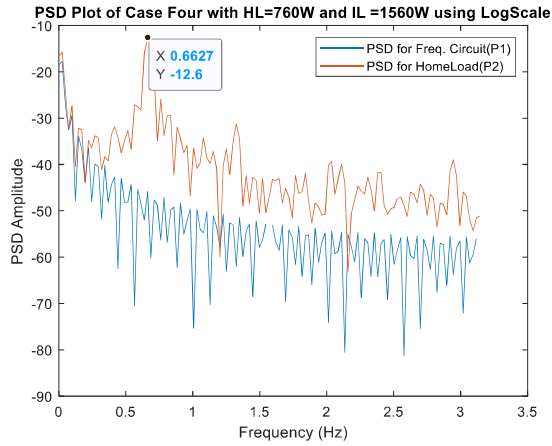


(c)

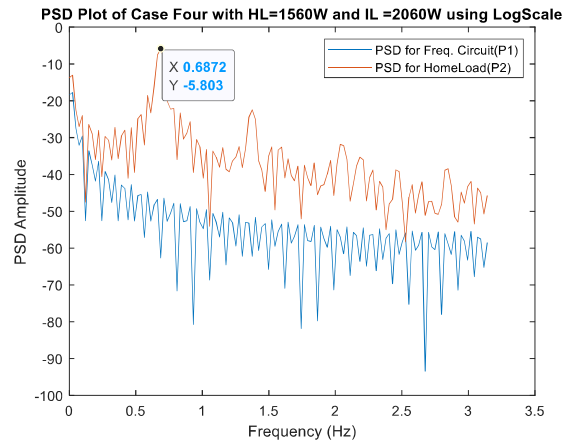


(d)

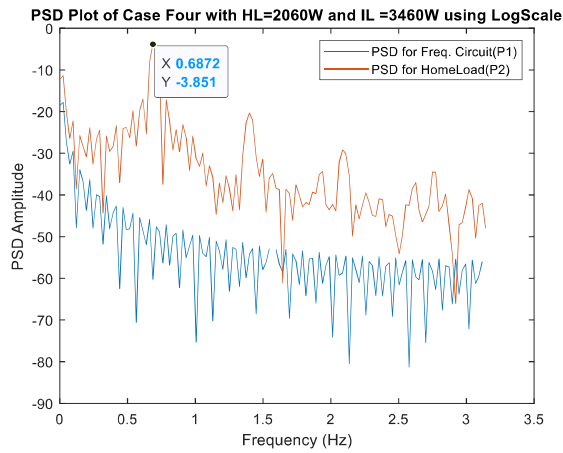
Fig. 5.3 PSD plots of Case Four with different power ratings of the load on a linear scale



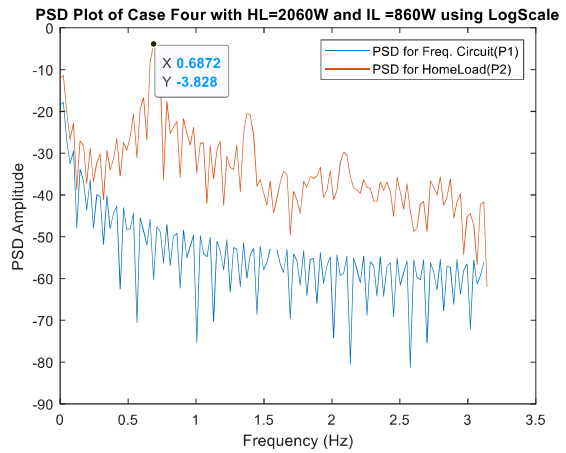
(a)



(b)



(c)

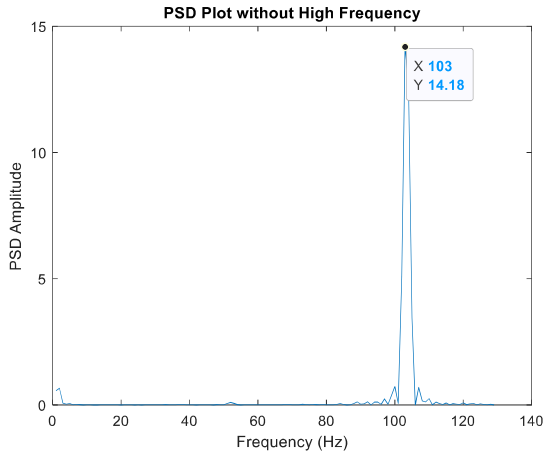


(d)

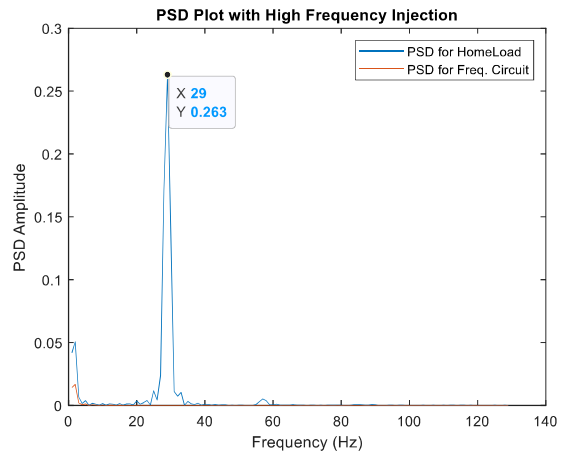
Fig. 5.4 PSD plots of Case Four with different power ratings of the load on a log scale

### 5.1.3 Results indicating the changes in the Frequency Component

This section shows the effect of high-frequency injection through visual observation. The graphs in this section involved an injected frequency and when there was none.



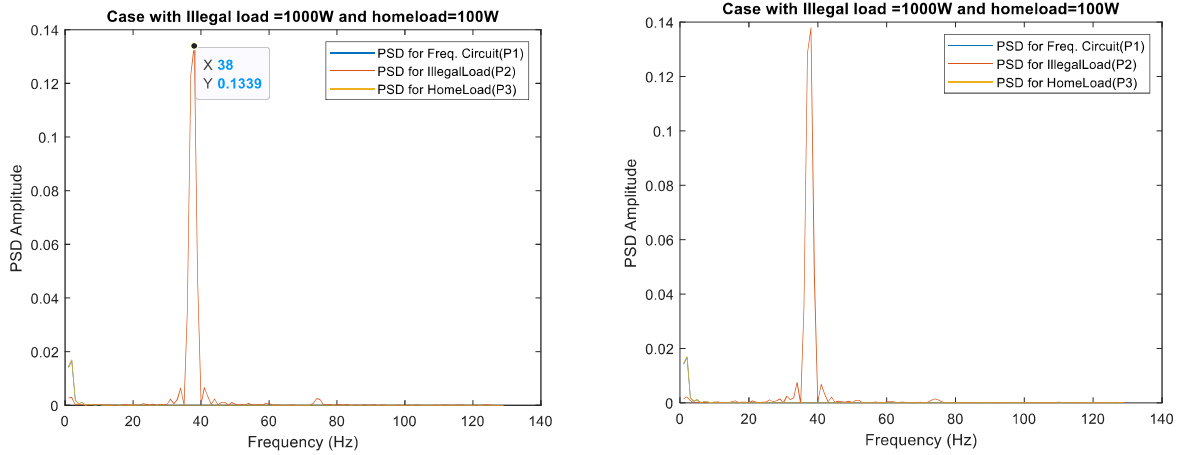
(a)



(b)

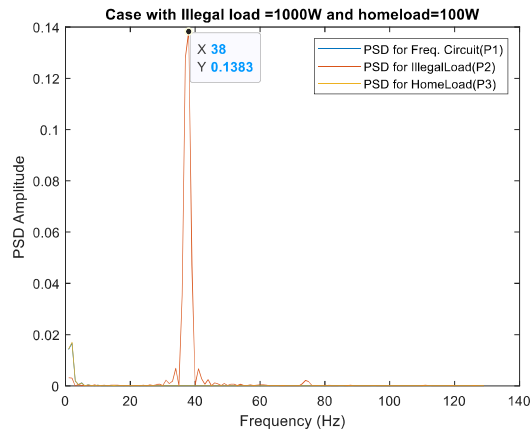
Fig. 5.5 PSD plots of Case One without a high-frequency signal and Case Two with high-frequency signal

### 5.1.4 Results showing the variations in the PSD graphs due to different frequency values



(a)

(b)



(c)

Fig. 5.6 PSD plots of Different Frequency values, (a) being 21.7kHz, (b) being 31.7kHz and (c) being 11.7kHz

### 5.1.4 Tabulated results of the average PSD values for all the Test Cases

Table 5.1: PSD Coefficients for Case Two and Case Three

PSD Coefficients	Case Two	Case Three
PSD1	2.8426e-04	2.8144e-04
PSD2	0.00063	5.9715

Table 5.2: PSD Coefficients for varying cases of Case Four

PSD Coefficients	Case Four 1	Case Four 2	Case Four 3	Case Four 4
PSD1	2.8144e-04	2.8426e-04	2.8144e-04	2.8144e-04
PSD2	0.0016	0.0062	0.0103	0.0104

Table 5.3: PSD Coefficients for Varying Frequency Cases in Proteus

PSD Coefficients	Sensor 1 (illegal Load)	Sensor 2 (Home load)
11.7kHz	0.0031	2.8645e-04
21.7kHz	0.0031	2.8645e-04
31.7kHz	0.0031	2.9145e-04

Table 5.4: PSD Coefficients for Varying Frequency Cases in Simulink

PSD Coefficients	Sensor 1 (illegal Load)	Sensor 2 (Home load)
11.7kHz	0.0369	0.0322
21.7kHz	0.0369	0.0322
31.7kHz	0.0369	0.0322

## 5.2 Discussion

The graphs using the logarithmic scale aid in visualizing graphs that skew towards large values in a dataset [28]. Thus, the analysis will mainly be done on the linear scale graphs. We will first analyze Fig.5.1

Comparing Fig.5.1a and Fig.5.1b, there is a considerable difference between the PSD amplitudes for both cases. Case two shows a higher PSD peak amplitude, which implies that when there is an unauthorized load, the PSD coefficient increases. In Fig.5.2., the high-frequency circuit appears to be relatively similar for both cases as the current values in the injection circuit do not change as much.

Analyzing Fig. 5.3., there is a constant rise in the peaks of the PSD amplitude for the various cases. This confirms that when there is an illegal load, the PSD coefficient increases. The increase, however, depends on the power rating of both the home load and the illegal load. For instance, in Fig.5.3c and Fig.5.3b, the PSD amplitude are almost similar, and this is because the ratings of the home load are kept constant. This suggests that no matter the amount of illegal load tapped on the line, the PSD amplitude increases; however, there is a more significant rise when

the home load is relatively smaller than the illegal load. The exact inference can be seen in Fig.5.4, which uses the log scale.

The last analysis will be in Fig.5.5. In Fig.5.5a, the PSD is measured on a circuit that has no additional components that draw some line current, and this explains why the PSD amplitude is higher than that of Fig.5.5b. However, we observe a change in the frequency axis of the graphs. This is due to the differences in the frequency components in each case. Energy signals tend to diminish as frequency increases [29]. This accounts for why the PSD of the high-frequency injection signal case is lower than that of the one without high frequency.

The analysis can also be made on the values from Table 5.1 and Table 5.2. According to the decision algorithm in Table 3, if  $P1 < P2$ , it is a hooking or meter bypass case. Thus, this logic is accurate for Case Three and all the cases in Table 5.2., as the PSD2 values are all greater than that their PSD1 values.

Lastly, the results from Simulink, which were to confirm the results, are analyzed. Here, we realize from Table 5.3 that the PSD coefficients for the different frequency values are almost close, and for Table 5.4, the values are all the same. This indicates that the PSD values are consistently similar when there is a high-frequency signal within the range stipulated by the CENELEC-5004. This is confirmed by the values in Table 5.4.

## **CHAPTER 6: CONCLUSION**

The injection of high frequency is a practical approach to detecting electricity theft. The deductions, constraints, and recommendations are discussed below.

### **6.1 Conclusion**

This project was implemented using high-frequency injection and a power spectral density algorithm in MATLAB. The various tests conducted indicate that the infusion of high frequency to a low voltage network with the help of the PSD algorithm can help identify any occurrences of tapping the low voltage networks directly. Table 5.1 and Table 5.2 indicate that the PSD value will be greater whenever there is an unauthorized load in any part of the circuit before the meter. Thus, it can be concluded that the PSD from the load is always higher than the PSD from the injection circuit. This helps in detecting electricity theft, particularly hooking and meter bypassing. Although there was the presence of the LC traps, if these traps are not built to the suitable capacity, there will be much damage to the appliances of many consumers, which can further lead to other issues like fires. Hence, in considering a system like this, there needs to be a suitable power line filter that can eliminate the high frequency safely.

### **6.2 Future Work**

In future work, a suitable system will be developed to have functionalities that detect and prevent electrical theft using a high-frequency signal through further research. Hardware would be used to implement the suggested system. This will enable one to evaluate the entire system's performance and not solely the software bit. Further work also needs to be done to probe any other alternative algorithm, such as Wavelet which is more robust and more suited for this project. There needs to



be more research on power spectral density in electrical energy in power systems. Also, there can be an expansion of the project's scope where it goes beyond one residence but looks at a whole community.

### **6.3 Recommendations**

A recommendation for this approach would be that researchers should make their datasets available and give detailed guidelines to the project rather than summarizing and leaving out seemingly relevant information. Also, moving on further, one can consider how best to work with high frequency directly injected into the low voltage networks and then create a device that can be used in conjunction with the electrical meters which step down these high frequencies.

## REFERENCES

- [1] A. A. Chauhan, "Non-Technical Losses in Power System and Monitoring of Electricity Theft over Low-Tension Poles," 2015 Second International Conference on Advances in Computing and Communication Engineering, 2015, pp. 280-284, doi: 10.1109/ICACCE.2015.106.
- [2] N. Mohammad, A. Barua and M. A. Arafat, "A smart prepaid energy metering system to control electricity theft," 2013 International Conference on Power, Energy and Control (ICPEC), 2013, pp. 562-565, doi: 10.1109/ICPEC.2013.6527721.
- [3] J. Y. Kim, Y. M. Hwang, Y. G. Sun, I. Sim, D. I. Kim and X. Wang, "Detection for Non-Technical Loss by Smart Energy Theft With Intermediate Monitor Meter in Smart Grid," in IEEE Access, vol. 7, pp. 129043-129053, 2019, doi: 10.1109/ACCESS.2019.2940443.
- [4] Ogu, R. E., Chukwudebe, G. A., & Ezenugu, I. A. (2016). An IoT Based Tamper Prevention System for Electricity Meter. *American Journal of Engineering Research (AJER)*, 5, 347–353. [www.ajer.org](http://www.ajer.org)
- [5] S. Sahoo, D. Nikovski, T. Muso and K. Tsuru, "Electricity theft detection using smart meter data," 2015 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), 2015, pp. 1-5, doi: 10.1109/ISGT.2015.7131776.
- [6] *Accra West ECG loses ₵3.9million in nine months through illegal connections - MyJoyOnline.com.* (n.d.). Retrieved January 4, 2022, from <https://www.myjoyonline.com/accra-west-ecg-loses-₵3-9million-in-nine-months-through-illegal-connections/>

- [7] M. Uvais, "Controller Based Power Theft Location Detection System," 2020 International Conference on Electrical and Electronics Engineering (ICE3), 2020, pp. 111-114, doi: 10.1109/ICE348803.2020.9122940.
- [8] M. B. Shahid, M. O. Shahid, H. Tariq and S. Saleem, "Design and Development of An Efficient Power Theft Detection And Prevention System through Consumer Load Profiling," 2019 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), 2019, pp. 1-6, doi: 10.1109/ICECCE47252.2019.8940644.
- [9] *PJM Learning Center - Transmission & Distribution*. (n.d.). Retrieved April 25, 2022, from <https://learn.pjm.com/electricity-basics/transmission-distribution.aspx>
- [10] *ACS772 Datasheet by Allegro MicroSystems | Digi-Key Electronics*. (n.d.). Retrieved April 21, 2022, from <https://www.digikey.at/htmldatasheets/production/2926181/0/0/1/acs772-datasheet.html>
- [11] *ATmega32 | Microchip Technology*. (n.d.). Retrieved March 20, 2022, from <https://www.microchip.com/en-us/product/ATmega32>
- [12] *A. K. Gupta, A. Mukherjee, A. Routray and R. Biswas, "A novel power theft detection algorithm for low voltage distribution network," IECON 2017 - 43rd Annual Conference of the IEEE Industrial Electronics Society, 2017, pp. 3603-3608, doi: 10.1109/IECON.2017.8216611.*

- [13] A. V. Christopher, G. Swaminathan, M. Subramanian and P. Thangaraj, "Distribution line monitoring system for the detection of power theft using power line communication," 2014 IEEE Conference on Energy Conversion (CENCON), 2014, pp. 55-60, doi: 10.1109/CENCON.2014.6967476.
- [14] EPCOS, T. (2015). *EMC filters SIFI-G for enhanced insertion loss* (Issue January).
- [15] *Working With the Serial Port Model in Proteus | Custom | Maker Pro*. (n.d.). Retrieved April 21, 2022, from <https://maker.pro/custom/projects/working-with-the-serial-port-model-in-proteus>
- [16] *How To Use Virtual Terminal in Proteus ISIS - The Engineering Projects*. (n.d.). Retrieved April 25, 2022, from <https://www.theengineeringprojects.com/2013/05/how-to-use-virtual-terminal-in-proteus.html>
- [17] Graf, R. F. (1999). S. *Modern Dictionary of Electronics*, 662–758.  
<https://doi.org/10.1016/B978-0-08-051198-6.50024-2>
- [18] LMS. (2020). *What is a Power Spectral Density ( PSD )? Picture 1*, 1–16.  
<https://community.sw.siemens.com/s/article/what-is-a-power-spectral-density-psd>
- [19] *Vibration Analysis: FFT, PSD, and Spectrogram Basics [Free Download]*. (n.d.). Retrieved April 22, 2022, from <https://blog.endaq.com/vibration-analysis-fft-psd-and-spectrogram#psd>
- [20] A. V. Christopher, G. Swaminathan, M. Subramanian and P. Thangaraj, "Distribution line monitoring system for the detection of power theft using power line communication," 2014 IEEE

Conference on Energy Conversion (CENCON), 2014, pp. 55-60, doi:  
10.1109/CENCON.2014.6967476.

[21] Globe, C. (2017). *What is Electrical Load? Definition & Types - Circuit Globe.*

<https://circuitglobe.com/electrical-load.html>

[22] *Reactive Power Compensation of Reactive Components.* (n.d.). Retrieved April 25, 2022,

from <https://www.electronics-tutorials.ws/accircuits/reactive-power.html>

[23] Homelite. (2015). *Storm / Emergency Use Recreational Use Essentials.*

[24] MANABU, T., KEN, M., & HIROYUKI, H. (2018). *Current Sensors.* 35.

<https://www.engineersgarage.com/current-sensors/>

[25] *Product Overview | Allegro ACS712 Hall-Effect Sensors | Arrow.com.* (n.d.). Retrieved

April 25, 2022, from <https://www.arrow.com/en/research-and-events/articles/product-insight-allegros-ac712-hall-effect-current-sensor-ic>

[26] *FREE Virtual Serial Ports driver, Rs-232 null modem emulator.* (n.d.). Retrieved April 25,

2022, from <https://freevirtualserialports.com/>

[27] Robbins, N. (2012). *When Should I Use Logarithmic Scales in My Charts and Graphs?*

Forbes. <https://www.forbes.com/sites/naomirobins/2012/01/19/when-should-i-use-logarithmic-scales-in-my-charts-and-graphs/?sh=1ddf82265e67>

[28] *The Power of Logarithmic Scale - DataClarity Corporation.* (n.d.). Retrieved April 27,

2022, from <https://www.dataclaritycorp.com/the-power-of-logarithmic-scale/>

[29] Cygnus Research International. (2017). *Power spectral density function*.

<https://www.cygres.com/OcnPageE/Glosry/SpecE.html>

[30] S. Bose, S. Das, A. Dey, J. Das and S. B. Raha, "Power Theft Detection in Low Voltage Distribution Network," 2020 IEEE 1st International Conference for Convergence in Engineering (ICCE), 2020, pp. 269-274, doi: 10.1109/ICCE50343.2020.9290534.

## APPENDIX

### A.1 MATLAB Code for Case One

```
%%  
% Final Case One  
% Normal distribution line condition with no high frequency signal  
clear  
clc  
s = serialport('COM3',9600) %initialize serial object with baudrate 9600,  
  
ndata = 100; %number of data elements to record or sample from serial  
  
%initialize 1 by ndata row vector to hold read data  
current = zeros(1,ndata);  
volt = zeros(1,ndata);  
  
|  
for i = 1:ndata+1  
data = s.readline(); %read each line of data - this is of type string  
conv_data = str2num(data); %convert to a number - type double  
if length(conv_data) >2 % prevent index error on first read.  
    %Serial tends to miss the first data on start  
    volt(i) = conv_data(1); %pu2t converted in their corresponding row vectors  
    current(i) = conv_data(2);  
  
end  
end  
  
% This section writes the values into an excel sheet file  
filename = 'CaseOne.xls'  
data = [current',volt'];  
writematrix(data,filename)
```

```
%%  
readData = readmatrix('CaseOne.xls')  
current = readData(:,1);  
  
[pxx1,f1] = periodogram(current); %calculates the psd for current sensor 1  
  
figure(5)  
plot(f1,10*log10(pxx1))  
title("PSD Plot of Case One using LogScale")  
xlabel("Frequency (Hz)")  
ylabel("PSD Amplitude")  
  
figure(6)  
plot(pxx1)  
title("PSD Plot of Case One")  
xlabel("Frequency (Hz)")  
ylabel("PSD Amplitude")
```



## A.2 MATLAB Code for Case Two

```
%%
% Final Case Two
% When high frequency is injected into the circuit
clear
clc
s = serialport('COM4',9600)%initialize serialobject with baudrate 9600,

ndata = 100; %number of data elements to record or sample from serial

%initialize 1 by ndata row vector to hold read data
CT12 = zeros(1,ndata);
VT12 = zeros(1,ndata);
CT22 = zeros(1,ndata);
VT22 = zeros(1,ndata);

for i = 1:ndata+1
    data = s.readline(); %read each line of data - this is of type string
    conv_data = str2num(data); %convert to a number - type double
    if length(conv_data) >2 %prevent index error on first read.
        %Serial tends to miss the first data on start
        VT12(i) = conv_data(1); %put converted in their corresponding row vectors
        CT12(i) = conv_data(2);
        VT22(i) = conv_data(3); %put converted in their corresponding row vectors
        CT22(i) = conv_data(4);
    end
end

% CT12 is for current sensor 1;
% CT22 is for current sensor 2
% This section writes the values into an excel sheet file
filename = 'CaseTwo.xls'
data = [CT12',VT12',CT22',VT22'];
writematrix(data,filename)
```

```

%%
readData = readmatrix('CaseTwo.xls')
CT12 = readData(:,1);
CT22 = readData(:,3);

[pxx1,f1] = periodogram(CT12); %calculates the psd for current sensor 1
[pxx2,f2] = periodogram(CT22); %calculates the psd for current sensor 2

|
figure(1)
plot(f1,10*log10(pxx1))
hold on
plot(f2,10*log10(pxx2))
legend('PSD for Freq. Circuit(P1)', 'PSD for HomeLoad(P2)')
title("PSD Plot of Case Two without Illegal Load using LogScale")
xlabel("Frequency (Hz)")
ylabel("PSD Amplitude")

figure(2)
plot(pxx1)
hold on
plot(pxx2)
legend('PSD for Freq. Circuit(P1)', 'PSD for HomeLoad(P2)')
title("PSD Plot of Case Three without Illegal Load ")
xlabel("Frequency (Hz)")
ylabel("PSD Amplitude")

```

### A.3 MATLAB Code for Case Three

```
%%
% Final Case Three
% When high frequency is injected into the circuit and there is illegal
% load with no home load
clear
clc
s = serialport('COM4',9600) %initialize serial object with baudrate 9600,

ndata = 100; %number of data elements to record or sample from serial

%initialize 1 by ndata row vector to hold read data
CT13 = zeros(1,ndata);
VT13 = zeros(1,ndata);
CT23 = zeros(1,ndata);
VT23 = zeros(1,ndata);

for i = 1:ndata+1
    data = s.readline(); %read each line of data - this is of type string
    conv_data = str2num(data); %convert to a number - type double
    if length(conv_data) >2 % prevent index error on first read.
        %Serial tends to miss the first data on start
        VT13(i) = conv_data(1); %put converted in their corresponding row vectors
        CT13(i) = conv_data(2);
        VT23(i) = conv_data(3); %put converted in their corresponding row vectors
        CT23(i) = conv_data(4);
    end

% CT13 is for current sensor 1;
% CT23 is for current sensor 2
% This section writes the values into an excel sheet file
filename = 'CaseThreeAlt.xls'
data = [CT13',VT13',CT23',VT23'];
writematrix(data,filename)
```

```

%%
readData = readmatrix('CaseThree.xls')
CT13 = readData(:,1);
CT23 = readData(:,3);

[pxx1,f1] = periodogram(CT13); %calculates the psd for current sensor 1
[pxx2,f2] = periodogram(CT23); %calculates the psd for current sensor 2

figure(5)
plot(f1,10*log10(pxx1))
hold on
plot(f2,10*log10(pxx2))
legend('PSD for Freq. Circuit(P1)','PSD for HomeLoad(P2)')
title("PSD Plot of Case Three with Illegal Load using LogScale")
xlabel("Frequency (Hz)")
ylabel("PSD Amplitude")

figure(6)
plot(pxx1)
hold on
plot(pxx2)
legend('PSD for Freq. Circuit(P1)','PSD for HomeLoad(P2)')
title("PSD Plot of Case Three with Illegal Load ")
xlabel("Frequency (Hz)")
ylabel("PSD Amplitude")

```

## A.4 MATLAB Code for Case Four

```
%%  
% Final Case Four  
% When both home load and illegal load are present  
% With HL=760W and IL =1560W  
clear  
clc  
s = serialport('COM4',9600) %initialize serial object with baudrate 9600,  
  
ndata = 100; %number of data elements to record or sample from serial  
  
%initialize 1 by ndata row vector to hold read data  
CT14 = zeros(1,ndata);  
VT14 = zeros(1,ndata);  
CT24 = zeros(1,ndata);  
VT24 = zeros(1,ndata);  
  
for i = 1:ndata+1  
    data = s.readline(); %read each line of data - this is of type string  
    conv_data = str2num(data); %convert to a number - type double  
    if length(conv_data) >2 % prevent index error on first read.  
        %Serial tends to miss the first data on start  
        VT14(i) = conv_data(1); %put converted in their corresponding row vectors  
        CT14(i) = conv_data(2);  
        VT24(i) = conv_data(3); %put converted in their corresponding row vectors  
        CT24(i) = conv_data(4);  
    end  
end
```



```

% CT14 is for current sensor 1;
% CT24 is for current sensor 2
% This section writes the values into an excel sheet file
filename = 'CaseFour1.xls'
data = [CT14',VT14',CT24',VT24'];
writematrix(data,filename)

%%
readData = readmatrix('CaseFour1.xls')
CT14 = readData(:,1);
CT24 = readData(:,3);

[pxx1,f1] = periodogram(CT14); %calculates the psd for current sensor 1
[pxx2,f2] = periodogram(CT24); %calculates the psd for current sensor 2

figure(1)
plot(f1,10*log10(pxx1))
hold on
plot(f2,10*log10(pxx2))
legend('PSD for Freq. Circuit(P1)', 'PSD for HomeLoad(P2)')
title("PSD Plot of Case Four with HL=760W and IL =1560W using LogScale")
xlabel("Frequency (Hz)")
ylabel("PSD Amplitude")

figure(2)
plot(pxx1)
hold on
plot(pxx2)
legend('PSD for Freq. Circuit(P1)', 'PSD for HomeLoad(P2)')
title("PSD Plot of Case Four with HL=760W and IL =1560W")
xlabel("Frequency (Hz)")
ylabel("PSD Amplitude")

```

## A.5 Code for Current Sensor

```
//Code for Two current sensors|
//int vol = PA0;
int cur1 = PA0;
int cur2 = PA1;
float offsetVoltage = 2.5;
float adcValue1 = 0;
float adcVoltage1 = 0;
float voltageValue1 = 0;
float currentValue1 = 0;
float adcValue2 = 0;
float adcVoltage2 = 0;
float voltageValue2 = 0;
float currentValue2 = 0;
double sensitivity = 0.185; //this has to change since it is not acs712

void setup() {
  // put your setup code here, to run once:
  Serial.begin(9600);

  pinMode(cur1, INPUT);
  pinMode(cur2, INPUT);
}

void loop() {
  // put your main code here, to run repeatedly:
  // for current sensor one
  adcValue1 = analogRead(cur1);
  adcVoltage1 = (adcValue1 / 1024.0) * 5.0;
  voltageValue1 = adcVoltage1;
  currentValue1 = ((adcVoltage1 - offsetVoltage) / sensitivity);

  adcValue2 = analogRead(cur2);
  adcVoltage2 = (adcValue2 / 1024.0) * 5.0;
  voltageValue2 = adcVoltage2;
  currentValue2 = ((adcVoltage2 - offsetVoltage) / sensitivity);

  //Serial.print("\t Voltage1(mV) = ");
  Serial.print(voltageValue1);
  Serial.print(" ");
  //Serial.print("\t Current1 = ");
  Serial.print(currentValue1);
  Serial.print(" ");
  //Serial.print("\t Voltage2(mV) = ");
  Serial.print(voltageValue2);
  Serial.print(" ");
  //Serial.print("\t Current2 = ");
  Serial.println(currentValue2);
}
```

## **A.6 Interviews from Electricity Company of Ghana Personnel**

The following is a list of responses gathered from interviews had with the ECG personnel. Questions were asked as the dialogue progressed, based on their comments. These interviews helped validate the problem of electricity theft. The following are summaries of the responses received.

1. Electromechanical (analog) and electronic (digital) meters are Ghana's different kinds of meters. These meters are mainly postpaid. However, some electronic meters are prepaid.
2. For postpaid meters, people steal theft by delaying the payment of electricity and not paying at all. ECG has curbed this by introducing prepaid meters, which ensure one pays before using the electricity.
3. For meter tampering, there is a seal at the terminal cover of the meter, so the moment someone tampers with it, the seal is broken. However, till an ECG personnel goes for a physical inspection, they will not find out.
4. There has been an introduction of smart meters, which caters to both meter tampering and bill irregularities, thus reducing electricity theft.
5. There is, however, no solution provided yet, especially in Ghana, for meter bypassing cases
6. This is one of the most common cases as the utility company cannot identify the theft until they do a physical inspection.