DETECTION SYSTEM OF ELECTRICITY THEFT AT SERVICE CONDUCTORS OF ELEVATED METERING CENTERS

Jonathan Evans H. Andaya[1], Eljhon J. Capili[1,b], Jon Arvin D. Peguit[1],
Benjamin T. Tiongson[1], and Kim Hubert M. Enrile[2,a]
[1]Bachelor of Science in Electrical Engineering, College of Engineering and Information Technology
[2]Faculty Member, Electrical Engineering Program, College of Engineering and Information Technology
[a]kimhubert.enrile@letran.edu.ph, [b]eljhon.j.capili@gmail.com

ABSTRACT

In the Philippines, one of the solutions to energy theft from utilities involves the relocation of electric meters to elevated metering centers, away from the residential building. The length of the service conductorshad made it vulnerable to illegal connections. The proposed solution is a system with theft recognition and magnitude determination mechanisms. The two mechanisms work based on voltage and energyreadings. The system was designed and tested using a residential building-rated microcontroller-based prototype utilizing an energy monitor as input device and the ZigBeeprotocol for wireless communication. The sensitivity, specificity, and success rate of the recognition mechanism were all 100 percent. The percent error of the theft magnitude determination mechanism ranged from 0 to 2.17 percent. Through cost-benefit analysis, the system was found to have positive net benefit at theft probabilities higher than 3.94 percent. The system has excellent usability as assessed though System Usability Scale.

Keyword: *Home computing; Microcontrollers; Consumer protection; Electricity theft detection*

INTRODUCTION

Interest in the prevention and detection of electricity theft has risen in the midst of high prices of energy, concerns about electrical safety, and emphasis on energy saving. In the global setting, the electric power market loses $96 billion per year to electricity theft [1]. Electricity theft is the practice of unauthorized use of electric power typically in the form of meter tampering [2] and illegal connections on electric service wires of utilities and on service facilities of paying consumers [3]. Losses from electricity theft increase the price of electricity for paying consumers due to system loss cap anddivest utilities of capital investment in network infrastructure [1].

To address this problem, a few solutions, mostly involving advanced metering infrastructure, have been implemented in different countries. However, advanced metering infrastructureis expensive in many countries [4].

In the Philippines, particularly in Metro Manila, the distribution utility has dedicated resources to combating illegal connections and tampering through manual inspections and cutting of illegal connections as frequent as once a week. These manual site inspections often cost more than the value of the losses, and implementation has been challenging since the suspects frequently re-establish their lines afterward [5]. This led the utility to another alternative action – the elevation of meters as a cluster located on top of the distribution pole, termed as elevated metering centers, so that they will be less accessible to the public [6].

However, the distance between the meter, which is usually located at distribution poles, and the service equipment, which is located inside the residential building, makes the service conductors vulnerable to illegal connections. Even though the electric consumption of the illegal consumer can be metered in this type of theft, the electricity consumption of the illegal consumer becomes the expense of the duly registered consumer.In this situation, theft can often be detected by visual inspection of the cables. The proposed study shall enable unsupervised monitoring through a system that will alarm the consumers when an illegal connection is made to the service conductor and will approximate the location of the illegal connection. Doing this will eliminate the need for periodic checking of the service conductors for illegal connection.

The study aims to design and develop an electricity theft detection system for residential electricity consumers who are metered under the elevated metering centers. Specifically, it intends to design and construct a device that can recognize the presence of electricity theft and approximate its magnitude; to test the functionality of the system regarding theft recognition and theft magnitude determination; to perform a cost-benefit analysis; and to determine the system's usefulness as perceived by residential consumers with electric services under the elevated metering centers.

Through the output of this study, legitimate consumers can easily know when unauthorized consumers connect to their service conductors. This shall prevent additional electricity charges that compensate for the illegal consumption. On the distribution utility's end, it shall prevent undocumented loadings that may cause overload in distribution facilities. This study may serve as baseline or reference for future projects and other intellectual ventures since it may contribute to the literature on electricity theft recognition and magnitude determination.

The study only addresses the problem of electricity theft at the service conductor under the elevated metering centers. Electricity theft recognition and theft energy magnitude determination are the only parameters considered. The system developed consisted of a recognition mechanism that notifies the existence of an illegal connection and a theft magnitude determination mechanism that computes and displays the amount of electricity stolen.

Literature Review

Electricity theft is commonly done through: tampering the energy meter; bypassing the electric meter; evading payment; magnetic reversing of current direction in analog disc type energy meters; employing of radio frequency devices to tamper electronic meter; intermittent theft; and disconnecting the neutral from the return path [7]. These ways of electricity theft are classified into four – fraud, stealing electricity, billing irregularities, and unpaid bills. Fraud is when a consumer misleads the utility commonly by meter tampering. Stealing electricity is when a line from a power source is connected to where it is needed, bypassing a meter. Billing irregularities and unpaid bills are due to the management of the distribution system [8]. The Philippine law cites the illegal use of electricity as connecting with electric service wires without previous authority or consent of the distribution utility, connecting to the existing electric service facilities of any duly registered consumer without the latter's consent or authority, or using a tampered electrical meter [3].

In the Philippines, the Energy Regulatory Commission allowed the relocation of residential electric meters to elevated metering centers in areas where illegal service connections, meter vandalism, and meter tampering are notorious [9]. For overhead service, from the distribution pole, the service drop is connected to the terminal box, meter, or other enclosure. From this, the service conductor connects to the service equipment which contains the disconnecting means and over current protections [10].

The basic way of electricity theft detection is by manual identification. Oftentimes, utilities resort to financial rewards and periodic checking. However, most cases cannot be identified through these procedures because of the lack of timely information and the labor-intensive demand [11]. In light of these, a variety of automated ways of electricity theft detection were studied. Detection techniques for electricity theft in advanced metering infrastructures were classified into three – classification-based, state-based, and game-theory-based. From among these three types of automatic detection, this study employed the state-based technique, which involves monitoring the state of a power system to improve the theft detection rate through wireless sensor networks, radio frequency identification, and advanced metering infrastructure [12].

In a study [13], an intrusion detection system was presented. This uses information fusion to combine the sensors and consumption data from a smart meter to detect energy theft.A conceptual approach by using power line communication and advanced metering infrastructure for the smart distribution system was given in a study [7]. A system wherein advanced metering infrastructure data and SCADA data are used for feeder bus load estimation and anomalous meter data detection was proposed in one study [14]. A smart apparent energy solution by using real-time energy audit mechanism meters that report their consumption to the master audit meter using UHF transceivers was presented in a paper [15]. Extracting the consumers' daily consumption series by the automatic remote metering system is proposed in one research [16]. An internet of things-based power theft detection was designed as a means to detect unauthorized tapping of conductors through a controller that receives current signals from current transformers through bridge rectifier and a conditional operator that compares the current magnitudes [17]. The main concerns in electricity theft detection are theft recognition, theft localization, and theft magnitude determination [7]. For the current study, theft recognition and theft magnitude determination were considered.

Modelling

Since the service meter is in series with the service equipment, the current at the service meter must be equal to the current at the service equipment. If the current flowing from the service meter is not equal to the current flowing to the service equipment, another conductor must have been connected to the service conductor through which part of the current from the service meter flows. From this concept, a model was developed, shown in Figure 1.

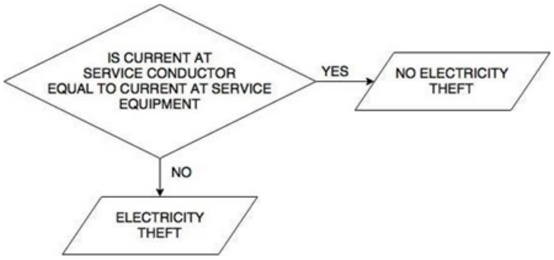

IS CURRENT AT SERVICE CONDUCTOR EQUAL TO CURRENT AT SERVICE EQUIPMENT
YES
NO ELECTRICITY THEFT
NO
ELECTRICITY THEFT

Figure 1. Model of Current-based Detection System

If there is no illegal connection, the energy supplied from the service meter is equal to the energy received at the service equipment. If there is an illegal connection, the energy supplied from the service meter shall be equal to the total of the energy consumed in the residential building and of the energy consumed by the one utilizing the illegal connection. From this concept, a mathematical model was developed as shown in Equation 1.

$$E_{theft} = E_{SM} - E_{SE} \qquad \textbf{Eqn. 1}$$

where E_{theft} is accumulated magnitude of electricity theft; E_{SM} is accumulated energy read at the service meter; and E_{SE} is accumulated energy read at the service equipment.

METHOD

Research Design

The study employed quantitative research design. Quantitative analyses were conducted to determine the sensitivity, specificity, and success rate and to measure the theft magnitude determination mechanism accuracy.

Research Procedure

The system architecture was designed to determine the required components. The system, including the hardware and software, was constructed, and it was then tested to gather the data on success rate, specificity, sensitivity, and accuracy. A cost-benefit analysis was performed, and the operation of the prototype was demonstrated to residential consumers. Afterwards, ausability assessment was conducted to determine the acceptability of the proposed system.

Hardware Implementation

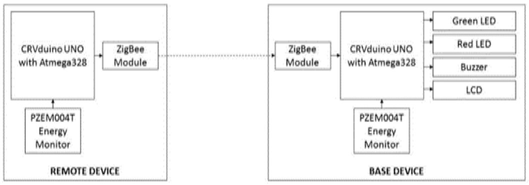


Figure 2. System Architecture Diagram

Figure 2 shows the overview of the architecture of the prototype electricity theft detector. It is composed of two main parts: the remote device intended to be located at the elevated metering center, and the base device intended to be located inside the building at the service equipment. Both devices sense current and energy using a PZEM004T Energy Monitor. Communication of sensed current and energy measurements from the remote device to the base device is established via serial communication through the use of the ZigBee protocol. Processing of parameters is done using CRVduino UNO with ATmega328 chip. Peripherals embedded to display the output are a red and green light-emitting diodes (LEDs), liquid crystal display (LCD), and buzzer.

Figure 3. Schematic Diagram of Remote Device

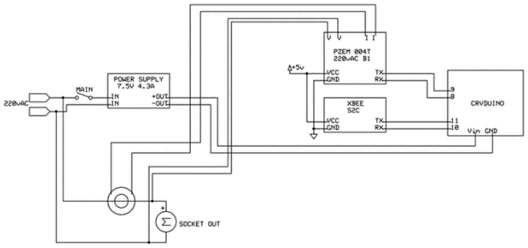
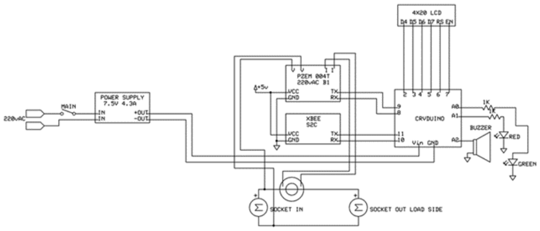


Figure 4. Schematic Diagram of Base Device



Process Implementation

The on-chip flash memory of the ATmega328 allows the program memory to be reprogrammed through the serial-USB connection by the boot program running on the chip itself. The chip communicates via the STK500 protocol made for Atmel's AVR microcontrollers [18]. The program itself may be created with a full suite of program and system development tools including: C compilers, macro assemblers, program debugger/simulators, in-circuit emulators, and evaluation kits [19]. This project uses the Arduino IDE software as its platform.

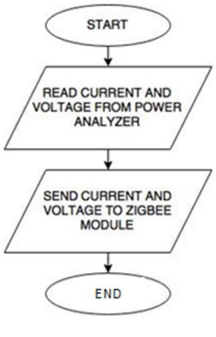

START
READ CURRENT AND VOLTAGE FROM POWER ANALYZER
SEND CURRENT AND VOLTAGE TO ZIGBEE MODULE
END

Figure 5. Process Flow of Remote Device

At the base device, the microcontroller reads the current and energy from the energy monitor and sends them to the ZigBee module.

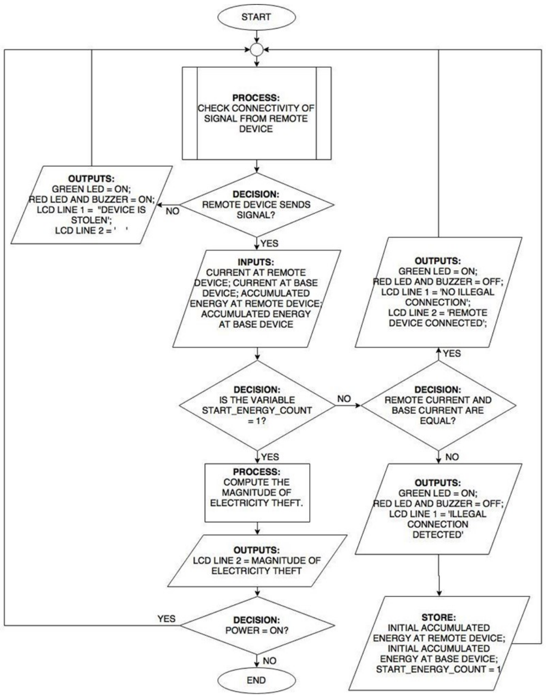

START
PROCESS:
CHECK CONNECTIVITY OF SIGNAL FROM REMOTE DEVICE
OUTPUTS:
GREEN LED = ON;
RED LED AND BUZZER = ON;
LCD LINE 1 = "DEVICE IS STOLEN";
LCD LINE 2 = ' '
NO
DECISION:
REMOTE DEVICE SENDS SIGNAL?
YES
INPUTS:
CURRENT AT REMOTE DEVICE; CURRENT AT BASE DEVICE; ACCUMULATED ENERGY AT REMOTE DEVICE; ACCUMULATED ENERGY AT BASE DEVICE
OUTPUTS:
GREEN LED = ON;
RED LED AND BUZZER = OFF;
LCD LINE 1 = 'NO ILLEGAL CONNECTION';
LCD LINE 2 = 'REMOTE DEVICE CONNECTED';
YES
DECISION:
IS THE VARIABLE START_ENERGY_COUNT = 1?
NO
DECISION:
REMOTE CURRENT AND BASE CURRENT ARE EQUAL?
YES
NO
PROCESS:
COMPUTE THE MAGNITUDE OF ELECTRICITY THEFT.
OUTPUTS:
GREEN LED = ON;
RED LED AND BUZZER = OFF;
LCD LINE 1 = 'ILLEGAL CONNECTION DETECTED'
OUTPUTS:
LCD LINE 2 = MAGNITUDE OF ELECTRICITY THEFT
YES
DECISION:
POWER = ON?
NO
END
STORE:
INITIAL ACCUMULATED ENERGY AT REMOTE DEVICE;
INITIAL ACCUMULATED ENERGY AT BASE DEVICE;
START_ENERGY_COUNT = 1

Figure 6. Process Flow of Base Device

The connectivity of signal from remote device is checked. If no signal is detected, the red LED and the buzzer turns on, and the LCD displays that the device is connected. If signal is detected, the current and instantaneous accumulated energy at remote device are read from the ZigBee module. The current and instantaneous accumulated energy at base device are read from the energy monitor. If the remote current and base current are equal, the green LED turns on, the red LED and the buzzer turns off, and the LCD displays that there is no illegal connection and that the device is connected. The process returns to the beginning and repeats. On the other hand, if the remote current and the base current are unequal, a counter starts. If the remote current and the base current are still unequal after three successive loops and, the system recognizes this as not merely due to transient fluctuations but due to illegal connection; the green LED turns off, the red LED and the buzzer turns on, and the LCD displays that an illegal connection is detected. It will then store the instantaneous accumulated energy at base device and at remote device as the initial reading from which the succeeding readings shall be subtracted to compute the accumulated energy since the detection of theft. The process returns to the beginning and repeats. At this point, the process of comparing the detected currents is bypassed. The process proceeds to calculation of the magnitude of theft by subtracting the accumulated energy at the base device from the accumulated energy at the remote device. The process returns to the beginning and repeats.

Testing Setup

The testing of the system was done using combinations of residential appliances as actual load and as theft load. The appliances were lighting, electric fan, electric flat iron, television set, and radio [10, 20]. Loading conditions were 32 possible combinations of the appliances as actual load, 31 possible combinations of the appliances as theft load, and 992 possible actual load – theft load combinations. A conductor connecting the remote device and the base device was used to model the service conductor. The theft load was connected to this conductor. The actual load was connected to the load side of the base device.

Testing of Theft Recognition Mechanism

The theft recognition mechanism was tested by determining whether the expected outputs were obtained in different states, i.e.if the green LED is on when there is no illegal connection and if the red LED and the buzzer are on when there is an illegal connection.

In finding the sensitivity, specificity, and total success rate, 278 loading conditions were selected from the 992-possible actual load – theft load combinations, for 0.95 confidence interval and 0.05 margin of error.

The decision in each testing was based on a research on power theft detection [21] and is summarized in Table 1

Table 1. Decision Matrix for Testing of Theft Recognition Mechanism

		Prototype-Indicated Condition	
		No Illegal Connection	Illegal Connection
Actual Condition	No Illegal Connection	True Negative	False Negative
	Illegal Connection	False Positive	True Positive

Success rate, sensitivity, and specificity were determined by using Equation 2, Equation 3, and Equation 4, respectively.

$$\%S = \left(\frac{TP+TN}{TP+FP+TN+FN}\right)(100\%) \quad \textbf{Eqn. 2}$$

$$\%SN = \left(\frac{TP}{TP+FP}\right)(100\%) \quad \textbf{Eqn. 3}$$

$$\%SP = \left(\frac{TN}{TN+FN}\right)(100\%) \quad \textbf{Eqn. 4}$$

where*%S* is success rate; *%SN* is sensitivity; *%SP* is specificity; *TP* is frequency of true positive results; *FP* is frequency of false positive results; *TN* is frequency of true negative results; and *FN* is frequency of false negative results.

Testing of Theft Magnitude Determination Mechanism

The accuracy of the theft magnitude determination mechanism was tested by determining whether the correct theft magnitude was displayed in the prototype's LCD.

For the accuracy testing, trials corresponding to all 31-possible theft loading were done.

Energy reading was noted after thirty minutes. The accuracy of the energy reading was determined by comparing it against the theoretical rated energy consumption and determining the percentage error.

Cost-Benefit Analysis

The methodology for cost-benefit analysis was based on cost-benefit analysis of surveillance technologies [22]. The formula for net annual benefit is shown in Equation 5.

$$B_{net} = B - C \qquad \textbf{Eqn. 5}$$

Where B_{net} is net annual benefit; B is annual benefit; and C is annual cost.

The annual cost of the system is modeled by Equation 6.

$$C = \frac{Cp+M+O}{T_s} \qquad \textbf{Eqn. 6}$$

where is annual cost; C is capital cost; M is maintenance cost; O is operation cost; and T_s is time of service. Capital cost include material cost, labor cost, and 20% markup. The time of service was assumed to be ten years. Maintenance cost include cost of regular replacement of parts and components. Operation cost include electricity cost. The electricity consumption was calculated by measuring the energy consumed by the device in one hour and converting it to annual consumption. Computation was based on the September 2017 rate of Meralco.

Annual benefit is quantified using Equation 7.

$$B = (P_{th})(C_{loss})(P_e) \qquad \textbf{Eqn. 7}$$

where$B$ is annual benefit; P_{th} is probability of illegal connection; C_{loss} is cost of loss; and P_e is percentage reduction in risk.

The cost of loss includes the annual cost of electricity stolen by the illegal connection. For the purpose of this study, the average annual electricity consumption cost per household as determined by the Philippine Statistics Authority was used as the basis for this variable. The latest data is PhP 22 524 [20]. Probability of illegal connection is the likelihood that a successful illegal connection will take place in the absence of the system. Since making an estimation of likelihood is difficult, the employed method is the approach used in cost-benefit analysis of other security technologies [23] – a breakeven cost-benefit analysis where the minimum probability of successful illegal connection for the benefit of the system was set to equalize the cost. Percentage reduction in risk is the amount of risk reduction achieved by deploying the system. This feature was based on the sensitivity obtained during the system testing.

Usability Assessment

The population of interest was the residential electricity consumers metered under the elevated metering centers at Barangay 92, District 1, Tondo, Manila. Eighty-four samples were taken from the population through random sampling.

The instrument used was the System Usability Scale [24], a reliable tool that measures device or system usability. It consists of a 10-item questionnaire with five response options for respondents – from Strongly Agree to Strongly Disagree [24].

After securing a permit to conduct the assessment, the researchers demonstrated the operation of the system to the respondents. Afterwards, the respondents answered the questionnaire.

The participant's scores for each question in the System Usability Scale were converted to a score contribution ranging from 1 to 4. For positive items, the score contribution is the score plus 1. For negative items, the score contribution is 5 minus the score. The score contribution was added together and then multiplied by 2.5 to convert the original scores of 0-40 to 0-100 [24].

RESULTS AND DISCUSSION

Success Rate, Specificity, and Sensitivity of Theft Detection

Table 2 presents the statistical measures of performance based on binary classification (true or false) of the theft detection mechanism.

Table 2. Success Rate, Specificity, and Sensitivity of Theft Detection

	Number of Trials	Number of True Detections	Number of False Detections	Rate
Sensitivity	278	278	0	100%
Specificity	278	278	0	100%
Success Rate	278	278	0	100%

The sensitivity of the prototype is 100 percent. This implies that no electricity theft conditions are missed or overlooked by the system. The specificity is also 100 percent. This means that the detection represents the condition of interest, which is electricity theft, and not the other conditions being mistaken for it. Overall, the device detection success rate is 100 percent. Specificity and sensitivity results are higher than an artificial intelligence-based electricity theft detection system in [25]. A high detection rate of success shall effectively solve the problem of unknown electricity theft [26].

Accuracy of Theft Magnitude Determination

Table 3 shows the result of the accuracy test of the theft magnitude determination mechanism at various loading conditions.

Table 3. Accuracy Testing

Theft Loading	Theoretical Theft Energy Per 0.5 Hour (watthour)	Measured Theft Energy (watthour)	Percent Error (percent)
Radio	21	21	0
electric fan	52	53	1.92
electric fan, radio	73	74	1.37
television set	46	47	2.17
television set, radio	67	67	0
television set, electric fan	98	98	0
television set, electric fan, radio	119	119	0
electric flat iron	599	610	1.84
electric flat iron, radio	620	626	0.97
electric flat iron, electric fan	651	654	0.46
electric flat iron, electric fan, radio	672	679	1.04
electric flat iron, television set	645	647	0.31
electric flat iron, television set, radio	666	664	0.3
electric flat iron, television set, electric fan	697	684	1.87
electric flat iron, television set, electric fan, radio	718	708	1.39
Lighting	298	296	0.67
lighting, radio	319	316	0.94
lighting, electric fan	350	348	0.57
lighting, electric fan, radio	371	372	0.27
lighting, television set	344	349	1.45
lighting, television set, radio	365	362	0.82
lighting, television set, electric fan	396	404	2.02
lighting, television set, electric fan, radio	417	409	1.92
lighting, electric flat iron	897	900	0.33
lighting, electric flat iron, radio	918	911	0.76
lighting, electric flat iron, electric fan	949	952	0.32
lighting, electric flat iron, electric fan, radio	970	971	0.1
lighting, electric flat iron, television set	943	955	1.27
lighting, electric flat iron, television set, radio	964	980	1.66
lighting, electric flat iron, television set, electric fan	995	1011	1.61
lighting, electric flat iron, television set, electric fan, radio	1016	999	1.67

The maximum error in measuring the magnitude of theft was 2.17 percent wherein the theft load is television. All the other loadings have errors below 2 percent. The error accounts for the 1 percent error of the energy monitor used. The maximum error is within the allowable range according to Institute of Electrical and Electronics Engineers standards [27].

Cost-Benefit of the System

Table 4. Quantification of Annual Cost

Cost Component	Annual Equivalent
Capital Cost	717.02
Maintenance Cost	10
Operating Cost	162.04
Total Annual Cost	889.06

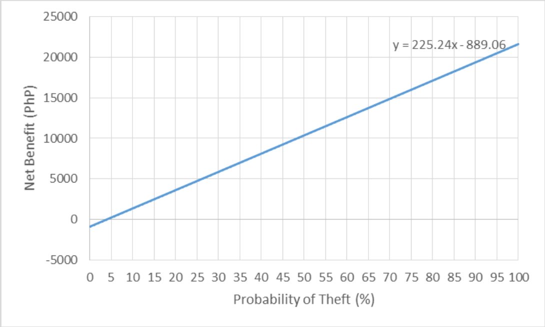


Figure 7. Net Benefit as a Function of Theft Probability

Since no data could be gathered to predict the probability of theft, the net benefit of implementing the system as a function of theft probability was determined. Based on Figure 7, the breakeven net benefit occurred at 3.94% probability of theft. This meant that the system has a positive net benefit at theft probabilities higher than 3.94%.

Perceived System Usability

The usability score was 82.083. Based on qualitative equivalence of usability score [24], the said score corresponded with excellent usability. This implies that the system was perceived as useful by the prospective users, implying that it was viewed as fit for its intended purpose. Second, it also implies that the system was perceived as user-friendly due to ease-of-use.

CONCLUSION

In order to enable unsupervised monitoring of the electrical service at elevated metering centers, a system for detecting electricity theft at service conductor of the elevated metering center was designed with two features – theft recognition and theft magnitude determination. A prototype was constructed to model the system using two devices that measure current and energy at both ends of the service conductor. After testing the prototype, the results were analyzed, and the following generalizations were obtained.

The sensitivity, specificity, and success rate of the theft recognition mechanism are all 100%. High sensitivity implies that all conditions when electricity theft exists can be recognized by the system. High specificity implies that it can accurately exclude no-theft cases and that it detects only as positive the condition of interest. The high success rate shows that the system can differentiate theft condition and no-theft condition. These data are indications of the technical viability of one function of the designed system – theft recognition mechanism.

The accuracy of the theft magnitude determination mechanism, expressed as percent error, ranges from 0 to 2.17 percent. The percent error is within the range allowed by the standards of the Institute of Electrical and Electronics Engineers. This indicates the technical feasibility of another function of the designed system – theft magnitude determination mechanism.

The system has negative net benefit at below 3.94 percent risk of illegal connection. Starting at 3.94 percent risk, the net benefit is positive and increases proportionally with risk.

The system has excellent usability as perceived by prospective end-users, suggesting excellent usefulness and ease of use, thus indicates the applicability of the designed system to the population of interest.

It is recommended for future studies to investigate using one master meter at the elevated metering center and several slave meters at each service that can also perform the functionality established by this study.

REFERENCES

[1] Northeast Group LLC, "Electricity theft and non-technical losses: global markets, solutions, and vendors," 2017.

[2] S. Nunoo and J. C. Attachie, "A methodology for the design of an electricity theft monitoring system," *J. Theor. Appl. Inf. Technol.*, vol. 26, no. 2, pp. 112–117, 2011.

[3] 9th Congress of the Philippines, *An act penalizing the pilferage of electricity and theft of electric power transmission lines/materials, rationalizing system losses by phasing out pilferage losses as a component thereof and for other purposes*. 1994.

[4] T. Fletcher, "BC Hydro downgrades smart-meter savings," *Kamloops This Week*, 2016. [Online]. Available: https://www.kamloopsthisweek.com/bc-hydro-downgrades-smart-meter-savings/.

[5] M. Mouton, "The Philippine electricity sector reform and the urban question: How Metro Manila's utility is tackling urban poverty," *Energy Policy*, vol. 78, pp. 225–234, 2015.

[6] M. Mouton, "Lighting up the urban poor in Metro Manila: How has the neoliberal reform of the energy sector impacted electricity distribution in low-income settlements of the Philippine capital city?" *Cah. Rech.du Program. Cities are Back T.*, 2014.

[7] M. U. Hashmi and J. G. Priolkar, "Anti-theft energy metering for smart electrical distribution system," in *International Conference on Industrial Instrumentation and Control*, 2015.

[8] T. B. Smith, "Electricity theft: a comparative analysis," *Energy Policy*, vol. 32, no. 18, pp. 2067–2076, 2004.

[9] Energy Regulatory Commission, *Rules to Govern the Installation and Relocation of Residential Electric Meters by Distribution Utilities to Elevated Metering Centers or Individual Residential Electric Meters to Other Elevated Service*. 2009.

[10] Institute of Integrated Electrical Engineers of the Philippines, *Philippine electrical code*. Quezon City: Institute of Integrated Electrical Engineers of the Philippines, 2009.

[11] N. Thakre, S. Vaidya, R. Pusadkar, and P. Damedhar, "Energy meter power theft detection in distribution system," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 5, no.III, pp. 1080–1082, 2017.

[12] J. Rong, R. Lu, W. Ye, J. Luo, C. Shen, and X. Shen, "Energy-theft detection issues for advanced metering infrastructure in smart grid," *Tsinghua Sci. Technol.*, vol. 19, no. 2, pp. 105–120, 2014.

[13] S. Mclaughlin, B. Holbert, A. Fawaz, R. Berthier, and S. Zonouz, "A multi-sensor energy theft detection framework for advanced metering infrastructures," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 7, pp. 1319–1330, 2013.

[14] Y. Lo, S. Huang, and C. Lu, "Non-technical loss detection using smart distribution network measurement data.," *IEEE PES Innov. Smart Grid Technol.*, 2012.

[15] V. Kamat, "Enabling an electrical revolution using smart apparent energy meters & tariffs," in *Annual IEEE India Conference*, 2011.

[16] H. Yuejun, L. Fubin, X. Jieqing, and M. Tingting, "Non-technical loss detection by multi-dimensional outlier analysis on the remote metering data," in *China International Conference on Electricity Distribution*, 2016.

[17] R. G. Balakrishna, "IoT based power theft detection," *Int. J. Innov. Eng. Technol.*, vol. 8, no. 3, pp. 111–115, 2017.

[18] Atmel, "AVR061: STK500 Communication Protocol." [Online]. Available: http://wwww.atmel.com/images/doc2525.pdf.

[19] Atmel, "ATmega48A/PA/88A/PA/168A/PA/328/P." [Online]. Available: http://www.atmel.com/images/atmel-8271-8-bit-avr-microcontroller-atmega48a-48pa-88a-88pa-168a-168pa-328-328p-datasheet.pdf.

[20] Philippine Statistics Authority, "Household Energy Consumption Survey."

[21] J. S. Atkari, S. A. Sutar, V. G. Birajdar, and M. A. B. Kanwade, "Electrical power line theft detection," *Int. J.Recent Innov.Trends Comput.Commun.*, vol. 5, no. 6, pp. 137–141, 2017.

[22] P.-H. Lin and C. van Gulijk, "Cost-benefit analysis of surveillance technologies," *Saf.Reliab.Methodol.Appl.*, pp. 409–414, 2015.

[23] M. G. Stewart and J. Mueller, "Cost-benefit analysis of airport security: Are airports too safe?" *J. Air Transp. Manag.*, vol. 35, pp. 19–28, 2014.

[24] A. Bangor, P. Kortum, and J. Miller, "Determining what individual SUS scores mean: adding an adjective rating scale," *J. Usability Stud.*, vol. 4, no. 3, pp. 114–123, 2009.

[25] I. Mamalikidis, "Machine learning methods for the analysis of data of an electricity distribution network operator," Aristotle University of Thessaloniki, 2017.

[26] J. Nagi, "An intelligent system for detection of non-technical losses in Tenaga National Berhad (TNB) Malaysia low voltage distribution network," UniversitiTenagaNasional, 2009.

[27] IEEE Standards Board, "IEEE standard procedures for measurement of power frequency electric and magnetic fields from AC power lines.".