

Anti-Tampering Device for Residential Energy Meter



Ertie C. Abana, Marion James Ladia, Drexel Gil Balao, Joel Balunsat, Newel Dannug, Julius Rom Paguigan, Jovimar Torres

Abstract: In this study, an energy meter anti-theft device is designed in order to detect fully or partially-earthed tampering in energy meter of residential areas which contributes to non-technical loss (NTL). The device notifies the power company through Short Message Service (SMS) when it detects tampering from a particular residential area. The device detects tampering through the reading of the two current sensors that are connected to a microcontroller. The power company will get notified when one of the current sensors detects current while the other one has not or there is a difference from the reading of the two current sensors. From the testing conducted using the device, the result shows that the system is reliable in identifying the tampering in fully earthed condition and partially earthed condition. Moreover, the system also notifies the authority with an average time of 17.61 seconds. Upon notification, the power company can immediately disconnect the service line with an average of 20.71 seconds. When the problem is settled the power company can reconnect the line for an average of 7.6 seconds. The accuracy of the device in terms of sending notifications, receiving the commands, and cutting the service lines is 100 percent.

Keywords: Short Message Service, Energy Meter, Tampering, None-Technical Loss

I. INTRODUCTION

Losses in electricity in the energy sector can come under two sets: Technical and Non-Technical [1]. Technical losses of electrical energy are due to energy dissipated in the conductors, equipment used for a transmission line, transformer, sub-transmission line, distribution line and magnetic losses in transformers. Examples of this are the

dissipated power in transformers and transmission lines because of electrical resistance internally. On the other hand, Non-Technical losses (NTL) happened when there are external actions to the power system or by someone manipulating the loads. NTL occur as a result of metering inaccuracies, unmetered energy, and theft. Electricity theft [2] is energy delivered to customers that are not measured by the energy meter for the customer. It can be categorized in the form of billing indiscretions, meter tampering, unpaid bills, and illegal connections. Tampering in energy meter [3, 4] is done by people so that the meter will record a lower consumption reading. Tampering may range from simple techniques like manipulating live or neutral wires to more sophisticated ones like hacking the firmware and changing [1, 3] energy consumption records.

The amount of electricity theft in a sample of 102 countries from 1980 and 2010 only shows that power theft is increasing all over the world [5-6]. This problem posts a huge amount of revenue lost which results in a shortage of funds for investments to expand the existing power capacity [3-4]. A high percentage of income in electricity is lost due to power theft but this can be solved by technology [5, 7] without human interaction. In fact, some studies have already developed power theft detection devices [5-6]. However, these devices only detect on the source side of the energy meter and not on the load side of the energy meter. One of the examples of power theft in the load side of the energy meter is the fully or partially-earthed tampering.

This research project focused on how to reduce the non-technical losses specifically on power theft in the load side of the energy meter through fully or partially-earthed tampering. The device can locate where the tampering is being done. The device can also be used to sense the fault in the service line and notify the power company. The power company may cut/trip the service line through the use of a text message. In that case, the system can reduce NTL due to the tampering that is being done. As an additional feature, the device can allow the power company to reconnect the consumer line when the issue on tampering is cleared. The device developed in the study is proposed to be added in the existing energy meter so that consumers will not be aware that their energy meters have an anti-tampering feature.

Manuscript published on November 30, 2019.

* Correspondence Author

Ertie C. Abana*, Center for Engineering Research and Technology Innovation, University of Saint Louis, Tuguegarao City, Cagayan, Philippines. Email: ertie04@gmail.com

Marion James Ladia, Electrical Engineering Program, University of Saint Louis, Tuguegarao City, Cagayan, Philippines.

Drexel Gil Balao, Electrical Engineering Program, University of Saint Louis, Tuguegarao City, Cagayan, Philippines.

Joel Balunsat, Electrical Engineering Program, University of Saint Louis, Tuguegarao City, Cagayan, Philippines.

Newel Dannug, Electrical Engineering Program, University of Saint Louis, Tuguegarao City, Cagayan, Philippines.

Julius Rom Paguigan, Electrical Engineering Program, University of Saint Louis, Tuguegarao City, Cagayan, Philippines.

Jovimar Torres, Electrical Engineering Program, University of Saint Louis, Tuguegarao City, Cagayan, Philippines.

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an [open access](http://creativecommons.org/licenses/by-nc-nd/4.0/) article under the CC-BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>)

II. MATERIALS AND METHODS

A. Block Diagram of the Device

The device consists of current sensors, relay, GSM module, and Arduino as the microcontroller enclosed control unit as shown in Fig. 1. Arduino Uno was used because it is a well-established general-purpose microcontroller [8-9] that works well for this kind of device. The current sensor parameter can read input current going into the meter and output current that goes out of the meter.

The microcontroller uses low input voltage to function, it converts an analog signal from the sensors into a digital signal to observe the behaviour if the current is stable, rising or falling. The microcontroller will compare the input signals to check if there is a difference between the input and output current. The Global System for Mobile Communication (GSM) module will serve as a bridge between the input data and the power company.

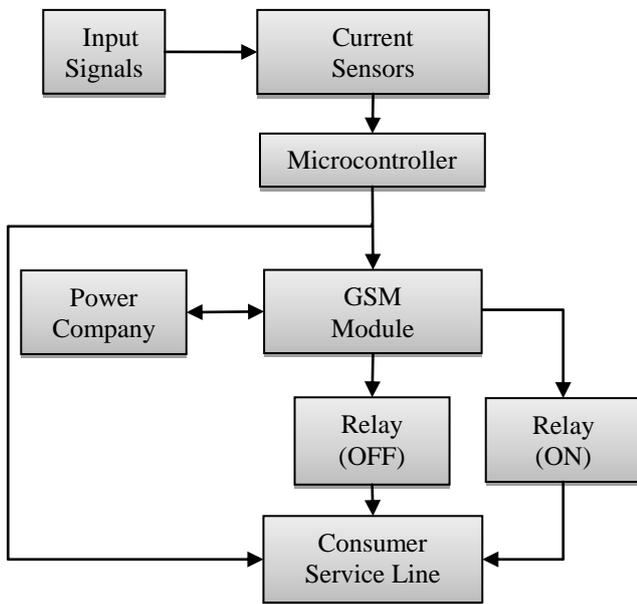


Fig. 1. The block diagram of the system.

When tampering is detected, the device notifies the power company through text message. The power company will then reply whether to cut the service line or not via text message. The service line is cut by the relay. If the power company wishes to reconnect the line, they can send a text message to the device to reclose the relay.

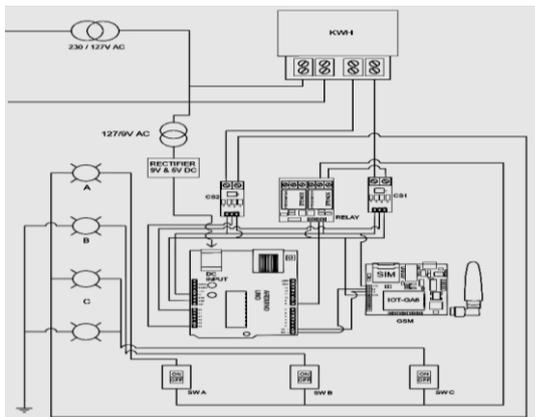


Fig. 2. The circuit diagram of the system.

The connection between the different elements of the device

is shown in Fig. 2. In the supply unit, the transformer serves as the main service line to produce a phase and ground terminals that are connected to the energy meter going to the loads. The series connection of Current Sensor 1 (CS1) and relay is placed in series between the energy meter and load phase terminal while the Current Sensor 2 (CS2) is placed in series with their ground terminal. To energize the microcontroller, the rectifier circuit is directly connected in the parallel connection going to the energy meter to step down the voltage at 9V. The working voltage of the two sensors, relay, and GSM module are 5V and they are connected as the bus going to the output voltage of microcontroller together with their common terminals. The pin A0 and A5 of analog pins of the microcontroller are connected to the first and second sensor input pin, respectively. Pin 9 and 10 of the microcontroller is connected to the pin RXD and TXD of the GSM module while the pin 12 of the microcontroller is connected to the input of the relay.

B. Tamper Conditions

Tampering of energy meters like changing the time, bypassing meter, magnetic interference, fully or partially-earth condition, and many more have been adopted by consumers [7] over time. The tampering from the source side has already been addressed by previous studies; therefore this study focused on the tampering on the load side particularly the fully or partially-earthed tampering. At normal condition, the connection between the source terminal to load terminal is the same, phase-to-phase and ground-to-ground terminal connection as shown in Fig. 3. However, consumers manipulated this by either changing the condition to fully or partially-earthed condition. In the fully-earthed condition shown in Fig. 4, the total load is earthed. In both cases, the current in the neutral wire IN, is less than that in the Phase wire (IP). For partially-earthed condition shown in Fig. 5, one of the loads is connected to earth and the other goes back to the neutral of the meter.

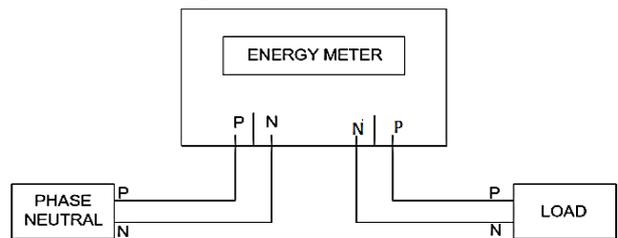


Fig. 3. No theft condition.

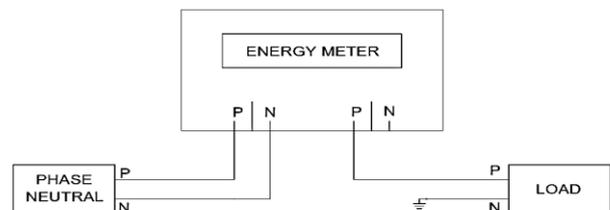


Fig. 4. Fully-earthed tampering condition.

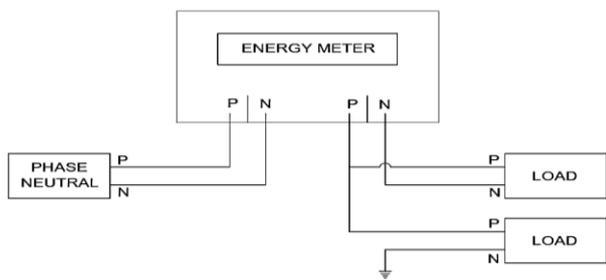


Fig. 5. Partially-earthed tampering condition.

In the device, normal condition happens when the reading of CS1 is equal to the reading of CS2. Fully-earthed tampering condition happens when the current reading on CS2 is zero amperes.

On the other hand, partially-earthed tampering condition happens when the current reading on CS1 is greater than the current reading on CS2.

III. RESULTS AND DISCUSSION

A. Testing Board

The testing board that is shown in Fig. 6 was made to check if the device works. The device itself is embedded at the back of the energy meter. The supply unit is rated 230/127 VAC to serve as the distribution line. The left switch represents an honest consumer where its loads are connected in normal condition. The middle switch represents a power theft that uses the fully-earthed tampering condition. The right switch also represents a power theft that uses the partially-earthed tampering condition. The light bulbs are the loads in the testing board. The first light bulb from the top is the load of the honest consumer; the second light bulb is the load of the power theft that uses fully-earthed tampering condition; and the third and fourth light bulb is the load of the power theft that uses partially-earthed tampering condition. When the middle switch or the right switch is turned on the device will automatically prompt the power company via text message that the consumer is stealing power and the power company can immediately act upon it by replying “Disconnect” to the earlier message from the device.



Fig. 6. Testing board of the device.

B. Testing of the Device

The device had undergone three testing procedures to determine how well it functions to its intended purpose. The testing was done with the supervision of a technical expert from a local power company. The mobile phone of the technical expert served as the receiver of the notification

when tampering is detected.

The first test was checking whether the device is capable of notifying the technical expert via text message when tampering is detected. The message latency was also recorded during the testing using a stopwatch. Message latency in this testing was the time elapsed between the time the middle switch or the right switch is switched on and the time the message is delivered to the technical expert. There were 20 trials during this testing wherein the first 10 trials were for the fully-earthed tampering condition while the next 10 trials were for the partially-earthed tampering condition.

Table- I: Notifying of Power Company

Trials	CS1 (mA)	CS2 (mA)	Message Latency (s)	Text Message
1	4.86	0	11.26	Received
2	4.87	0	11.66	Received
3	4.84	0	9.84	Received
4	4.85	0	18.86	Received
5	4.89	0	22.35	Received
6	4.86	0	17.3	Received
7	4.87	0	15.24	Received
8	4.87	0	15.05	Received
9	4.85	0	16.45	Received
10	4.86	0	12.31	Received
11	9.74	4.87	39.26	Received
12	9.74	4.87	20.19	Received
13	9.68	4.84	21.39	Received
14	9.72	4.86	17.03	Received
15	9.78	4.89	20.79	Received
16	9.74	4.87	26.53	Received
17	9.72	4.86	13.99	Received
18	9.74	4.87	12.62	Received
19	9.7	4.85	13.63	Received
20	9.74	4.87	16.36	Received

The results of the testing on the function of the device to notify technical expert via text message when tampering is detected is shown in Table I. It is evident from the results that the device was able to serve its essential purpose. It will help power companies to reduce their NTL which is also the main goal of other [5-7] power theft detection devices. The reduction of NTL will greatly benefit the majority of consumers as electric bills may also go down. For the power companies, they may now be able to spend more on their other facilities to improve their services.

The use of SMS by the device in notifying the technical expert about tampering was successfully done with an average message latency of 17.61 seconds. The use of SMS is more practical than the use of internet-based notification since the phone signal is easier to access than an Internet connection. Moreover, in developing countries like the Philippines where the study was conducted, the Internet connection is slow [10].

The second test was conducted to check the ability of the device to disconnect the service line when prompted by the technical expert via text message. The cut-off latency was also recorded during the testing.

Anti-Tampering Device for Residential Energy Meter

This latency was the time elapsed between the technical expert sending a message to the device and the moment the device disconnects the service line. The disconnection can be seen when the light bulb in the testing board switches off. A stopwatch was also used in this testing. A total of 20 trials were conducted wherein the first 10 trials were for fully-earthed tampering condition and the next 10 trials were for the partially-earthed tampering condition.

The device was able to disconnect the service line in the tampered energy meter as soon as the technical expert sends the disconnection text message as shown in Table II. An average of 20.74 seconds was recorded during the testing with 100% accuracy. This feature of the device was not incorporated in previous [5-7] power theft detection devices.

This will allow the power company to prevent the power thefts from stealing as soon as possible and take appropriate actions.

Table- II: Disconnection of Service Line

Trials	Cut-off Latency (s)	Light Bulb Status
1	26.28	Off
2	30.68	Off
3	12.37	Off
4	21.12	Off
5	18.81	Off
6	18.32	Off
7	22.24	Off
8	21.91	Off
9	36.60	Off
10	17.16	Off
11	38.4	Off
12	19.65	Off
13	17.2	Off
14	16.34	Off
15	20.33	Off
16	11.4	Off
17	10.56	Off
18	11.6	Off
19	21.47	Off
20	22.3	Off

The third test was conducted to check if the technical expert can reconnect the service line when the consumer dishonesty has been settled. This can be done by sending a text message "Reconnect" to the device. The reconnection latency was also recorded during the testing using a stopwatch. This latency is the time elapsed between the technical expert sending a message to the device and the moment the device reconnects the service line. The disconnection can be seen when the light bulb in the testing board switches on. There were 20 trials for this testing.

Table- III: Reconnection to Service Line

Trials	Reconnection Latency (s)	Light Bulb Status
1	7.01	On
2	9.71	On
3	6.48	On
4	6.24	On
5	11.42	On
6	8.66	On
7	10.08	On
8	7.3	On
9	6.17	On

10	7.64	On
11	6.13	On
12	7.17	On
13	5.29	On
14	6.23	On
15	9.14	On
16	9.27	On
17	7.56	On
18	7.43	On
19	6.22	On
20	6.77	On

Table III indicates that the device is 100% accurate in reconnecting to the service line when the technical expert sent the text message. The average reconnection latency is 7.6 seconds which is fairly fast. This reconnection feature that has not been embedded in previous studies [5-7, 11-12] can be very useful since the power company will no longer manually reconnect it.

IV. CONCLUSION

This research developed an anti-tampering device which may be one of many solutions in detecting the unlawful activity of residential consumers. The device was able to notify the power company when the energy meter is being tampered in fully-earthed and partially earthed condition. It can also allow control to the energy meter when remotely disconnecting service line via text message. Moreover, the service line can also be remotely reconnected via text message through the device. The results show that SMS can handle the notification, disconnection and reconnection of the line with minimal latency. The device can be further improved by adding features that will also detect other kinds of tampering.

REFERENCES

1. D. Warudkar, P. Chandel, & B. A. Sawale, "Anti-Tamper Features in Electronic Energy Meters," *International Journal of Electrical, Electronics and Data Communication*, vol. 2, no. 5, pp. 114-117, 2014.
2. R. Jiang, R. Lu, Y. Wang, J. Luo, C. Shen, & X. S. Shen, "Energy-theft detection issues for advanced metering infrastructure in smart grid," *Tsinghua Science and Technology*, vol. 19, no. 2, pp. 105-120, 2014.
3. S. S. S. R. Depuru, L. Wang, & V. Devabhaktuni, "Electricity theft: Overview, issues, prevention and a smart meter based approach to control theft," *Energy Policy*, vol. 39, no. 2, pp. 1007-1015, 2011.
4. J. P. Navani, N. K. Sharma, & S. Sapra, "Technical and non-technical losses in power system and its economic consequence in Indian economy," *International Journal of Electronics and Computer Science Engineering*, vol. 1, no. 2, pp. 757-761, 2012.
5. S. Anusha, M. Madhavi, & R. Hemalatha, "Detection of Power Theft Using GSM," *International Journal of Advanced Research Trends in Engineering and Technology*, vol. 1, no. 3, pp. 15-17, 2014.
6. C. P. Bidkar, P. R. Devale, P. D. Gawali & R. S. Bawane, "A Review on: GSM Based Electricity Theft Detection System," vol. 5, no. 1, pp. 337-339, 2017.
7. S. Sahoo, D. Nikovski, T. Muso, & K. Tsuru, "Electricity theft detection using smart meter data," In *2015 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference*, pp. 1-5, 2015.
8. E. Abana, M. Pacion, R. Sordilla, D. Montaner, D. Agpaao, & R. M. Allam, "Rakebot: a robotic rake for mixing paddy in sun drying," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 14, pp. 1165-1170, 2019.
9. E. Abana, C. V. Dayag, V. M. Valencia, P. Talosig, J. P. Ratilla, & G. Galat, "Road flood warning system with information dissemination via social media," *International Journal of Electrical & Computer Engineering*, vol. 9 no. 6, part 1, pp. 4979-4988, 2019.

10. E. Abana, "Usability of "Traysi": A Web Application for Tricycle Commuters," International Journal of Advanced Computer Science and Applications, vol. 10, no. 7, pp. 280-284, 2019.
11. A. S. Metering, S. Visalatchi, & K. K. Sandeep, "Smart energy metering and power theft control using arduino & GSM," In 2017 2nd International Conference for Convergence in Technology, pp. 858-961, 2017.
12. N. Mohammad, A. Barua, & M. A. Arafat, "A smart prepaid energy metering system to control electricity theft," In 2013 International Conference on Power, Energy and Control, pp. 562-565, 2013.

AUTHORS PROFILE



Ertie C. Abana received BS in Computer Engineering and Master of Information Technology degrees from the University of Saint Louis in 2011 and 2016, respectively, and is working for his PhD degree. He is a faculty of the School of Engineering, Architecture, and Information Technology Education, University of Saint

Louis, Tuguegarao City, Philippines since 2014.

He is also the head of the Center for Engineering Research and Technology Innovation in the same school. He has published papers in the areas of embedded systems, microcontrollers, fuzzy systems, data mining, and software usability.



Marion James Ladia received BS in Electrical Engineering from the University of Saint Louis in 2018. He is a faculty of the School of Engineering, Architecture, and Information Technology Education, University of Saint Louis, Tuguegarao City, Philippines since 2018. His research interests are in the areas of

renewable energy, smart grid, smart metering, power systems engineering, electronics circuits, and intelligent systems.



Drexel Gil Balao received BS in Electrical Engineering from the University of Saint Louis, Tuguegarao City, Philippines in 2019. His research interests are in the areas of renewable energy, smart metering, and power systems.



Joel Balunsat received BS in Electrical Engineering from the University of Saint Louis, Tuguegarao City, Philippines in 2019. His research interests are in the areas of renewable energy, power systems engineering, intelligent systems, and robotics.



Newel Dannug received BS in Electrical Engineering from the University of Saint Louis, Tuguegarao City, Philippines in 2019. His research interests are in the areas of smart metering, power systems engineering, intelligent systems, robotics, and solar thermal electric generation.



Julius Rom Paguigan received BS in Electrical Engineering from the University of Saint Louis, Tuguegarao City, Philippines in 2019. His research interests are in the areas of robotics, solar thermal electric generation, and vibrational energy harvesters.



Jovimar Torres received BS in Electrical Engineering from the University of Saint Louis, Tuguegarao City, Philippines in 2019. His research interests are in the areas of renewable energy, smart grid, smart metering, power systems engineering, electronics circuits, and intelligent systems.