International Journal of Academic Information Systems Research (IJAISR)
ISSN: 2643-9026
Vol. 6 Issue 5, May - 2022, Pages: 5-8

Testing of the Tampering Techniques on Prepaid Domestic Meters using GSM Modem

Kibirige David[1], Bob Rich Mwecumi [2], Namulawa Hawa[3], Kitone Isaac [4], Sserunjogi Solomon[5], Kayenga Tendo Joshua[6], Nelson Njubo[7], Nakitto Immaculate[8], Kanyana Ruth[9], Dr. Primrose Nakazibwe[10], Dr. Rita Makumbi[11]

[1-8]Department of Electrical Engineering, Ndejje University
Kampala, Uganda
semkibirige@gmail.com[1], abooki2014@gmail.com[2], hawanamulawa@gmail.com[3], kitonei@gmail.com[4], solomonsserunjogi29@gmail.com[5], kayengatendojoshua4991@gmail.com[6], tag.nnt@gmail.com[7], nakittoimmy@gmail.com[8]

Kanyana Ruth
Directorate of Research, Innovation, Consultancy and Extension, Kampala International University
Kampala, Uganda
ruth.kanyana@kiu.ac.ug

Dr. Primrose Nakazibwe
Directorate of research and innovations, Ndejje University
Kampala, Uganda
pnakazibwe@ndejjeuniversity.ac.ug

Dr. Rita Makumbi
Directorate of Quality Assurance, Ndejje University
Kampala, Uganda
barymaks@yahoo.co.uk

Abstract: *Rampant theft of electric power has been evolving over time. before the installation of prepaid meters, consumers were using manual methods of stealing power such as using a simple wire bypass and at the same time the distribution companies were using manual physical methods detecting power theft. As technology evolved in Uganda prepaid meters have been installed but there's still a big challenge in controlling power theft because customers have resorted to using electronic means of tampering. In this paper we address the different means of testing prepaid meter for tampering using GSM modem in order to come up with a real-time permanent solution to power theft.*

Keywords— Prepaid meter, Utility, GSM modem, Power theft, Tampering

1. INTRODUCTION

Over the years, the utility distribution companies in Uganda have had money losses through power theft. This has mainly happened due to tampering of the prepaid domestic meters that are installed at the top of the distribution pole which has led to launching of various operation such as operation "sigma" and "combowa" intended to net or capture consumers who are involved in power theft. In the end this has led to further losses on the side of electricity distribution company due to the high cost of sustaining the above mentioned operations [1]. Currently, Uganda is using prepaid meters for single-phase domestic consumers with a Dual In line rail mounting which is ideal for residential applications.it comprises of two elements, a measurement control unit (MCU), most commonly known as the meter and a Customer interface unit (CIU) which is the user's keypad interface. The meter is housed outside the consumer's premises, for example in a street kiosk or pole top box, which enables easy access for the utility [2]. This was also intended to reduce on power theft and death of clients. The prepaid meter has optional tamper protection, that is configured in production. If the tamper feature is enabled, any attempt to tamper with the meter can result in the consumer's supply being disconnected, if so configured. The supply is only reconnected when a Standard Transfer Specifications (STS) clear tamper token is entered into the meter. The STS tamper token is meter specific so it can only be used during installation and after that any tampering should be noticed [3]. However, there has been several was in which this meter has been tampered with.in this this paper we look at testing the different tamper techniques and use the GSM modem to communicate to the concerned personnel in the utility company to provide the most appropriate solution to the problem reported.

2. METHODOLOGY

The following block diagram was used in the testing.

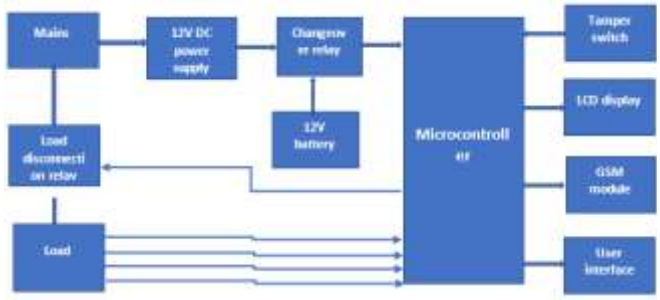

Figure 1: Block diagram of the project

In this Paper an energy meter which automatically dictates any form of tampering was designed from the above block diagram. it was created by programming an Arduino Uno microcontroller to track, measure, and record the amount of energy used by the load [2]. When a tampering attempt is detected, it is also programmed to disconnect the customer load and issue an alarm message.

Testing

Detection of tampering in case of battery failure.

If the battery fails for some reason, a thief can open the meter and install a measurement limiting resistor successfully which confuses signal wires from the load wire to the controller, as a result the microcontroller fails to be powered when the mains goes off. Therefore, the tamper switch cannot operate to cause customer load disconnection. A difference in currents reaching the microcontroller's pins will be detected by the microcontroller when the mains power is restored and the customer load will be disconnected immediately, and a tamper message sent using the GSM module to the concerned Utility personnel.

Detection of tampering and messaging

The first line of defense in the meter terminal compartment is the tamper switch connected to one of the pins of the microcontroller, it is designed to close when the terminal cover screw is opened, send a logic 1 message to the microcontroller as a meter tamper message. This will result in the transmission of a tamper alert message through SMS via the GSM module to the meter inspector's phone and followed by disconnection of the customer's load when the tamper is detected.

Testing different conditions

1. **Mains off condition**

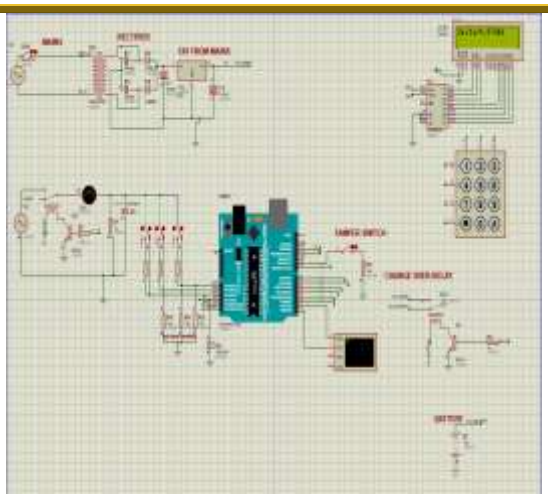

Figure 2: Load gets disconnected and meter is powered by the battery

Observation

The customer load was disconnected and the changeover relay turned on the battery to power the meter.

2. **Tamper switch closed during power outage.**

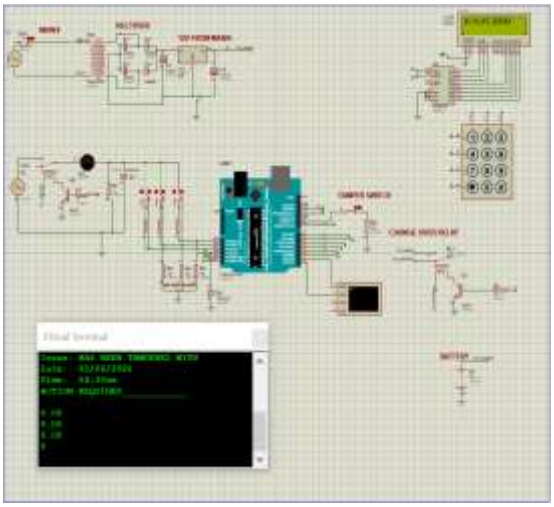

Figure 3: Tamper detected and message sent when tamper switch is closed

Observation

Customer load was disconnected and an alert message sent to the operator.

International Journal of Academic Information Systems Research (IJAISR)
ISSN: 2643-9026
Vol. 6 Issue 5, May - 2022, Pages: 5-8

3. Closing tamper switch with mains on

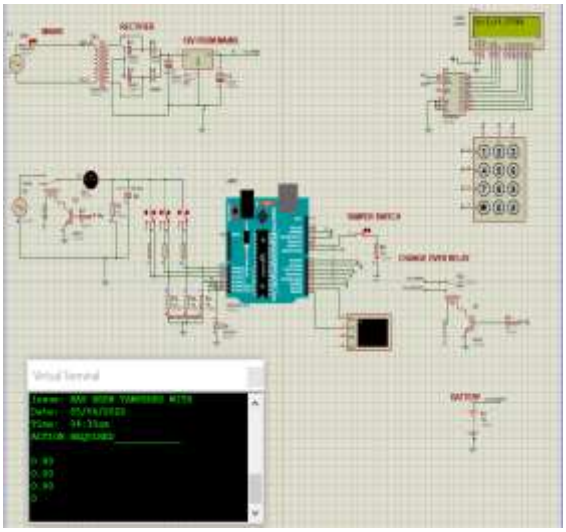

Figure 4: Closing tamper switch with mains on

Observation
The customer load was disconnected and an alert message sent to the operator, the meter continued to be powered by mains.

4. During a mains power outage or a battery supply failure, one measurement limiting resistor is added between signal wires from the load bar to the microcontroller.

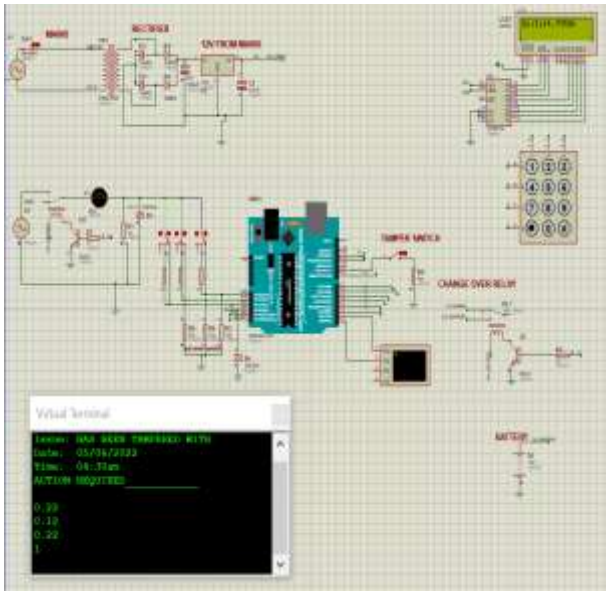

Figure 5: Testing condition 4

Observation
The meter generated an alert message when the mains supply returned.

5. Measurement Limiting resistors inserted in all the signal wires between load wire and microcontroller.

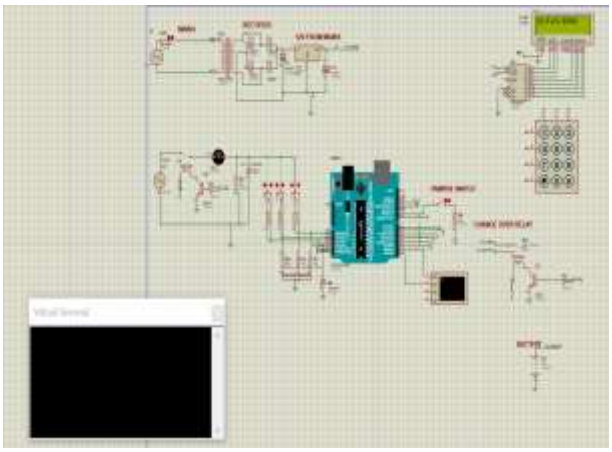

Figure 6: Testing condition 5

Observation
No tamper message displayed. When mains power comes back on, the load gets connected but the meter does not register consumption.

6. When the mains power is off and the battery fails to power the microcontroller, and MLRs are installed in all signal wires.

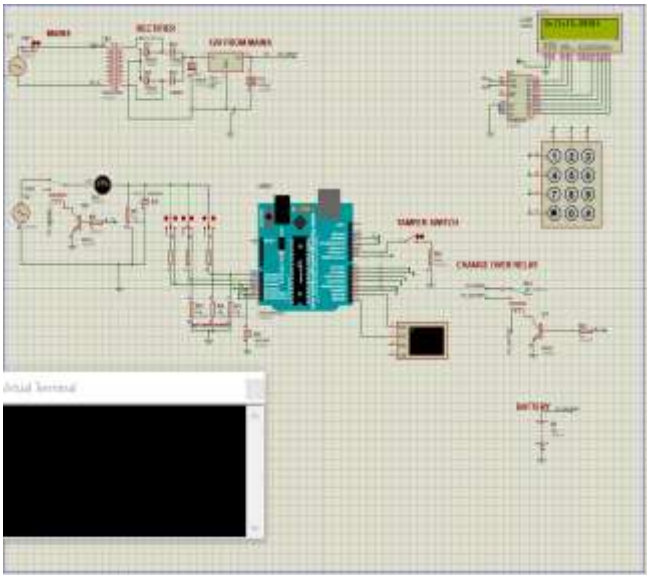

Figure 7: Testing condition 6

Observation
Customer load is not disconnected, and when mains power is restored, the load is powered, but there is no sign of energy use at the Customer Interface Unit.

Table 1: Summary of the testing

S.No	Tests	True positive	True negative	False positive	False negative
1	Mains off condition.	yes			
2	Tamper switch closed during power outage.		yes		
3	Tamper switch closed with mains on:		yes		
4	Inserting a Measurement Limiting Resistor (MLR) in a signal wire during power outage with battery functioning properly		yes		
5	MLR inserted in a signal wire when battery has failed and mains restored.		Yes		
6	Connecting MLRs in the signal wires when both mains and battery are out and thereafter restoring the mains.			Yes	

3. PERFORMANCE EVALUATION

Number of tests done: 6
Number of tests with true results: 5
Accuracy: (5/6) X 100 = 83.3%

True positive: is when the system indicates that the meter has not been tampered when it truly has not been tampered.
True negative is when the meter indicates that the meter has been tampered when truly it has been tampered
False positive is when the system indicates that the meter has not been tampered when it actually has been tampered
False negative is when the system indicates that the meter has been tampered when actually it has not been tampered.

4. CONCLUSION

The system was able to detect the different tampering techniques as discussed and shown above and send alert to the concerned utility personnel.

References

[1] J. M. van Leeuwen, T. Sekeramayi, C. Martell, M. Feinberg, and S. Bowersox-Daly, "A baseline analysis of the Katanga slums: Informing Urban public policy in Kampala, Uganda," *Etude la Popul. Africaine*, vol. 31, no. 2, 2017, doi: 10.11564/31-2-1057.

[2] S. S. Sable, Saurabh Padalkar, Akshay Rathod, Gaurav Tayade, and Vaibhav Bhadmukhe, "Smart Energy Meter," *Int. J. Adv. Res. Sci. Commun. Technol.*, 2022, doi: 10.48175/ijarsct-2888.

[3] Kannan P, A. Devaraj, Esakki Rajavel. S, Nisharni B, Sancta A, and Muthu Lakshmi M, "GSM Based Smart Energy Meter System," 2021. doi: 10.3233/apc210274.