International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6S2, August 2019

False Load Attack to Smart Meters by Synchronously Switching Power Circuits

Aarthi Suriya, S. P. Vijayaragavan, Anitha.S

Abstract*: In electric essentialness metering technique, flow and voltage are inspected discontinuously and simultaneously, and a while later used to find out the vitality utilization. This endeavor paper exhibits an essential yet incredible attack to the above metering framework with the ultimate objective that the learned imperativeness usage is made a long way from the genuine one. Specifically, an adversary switches on/off the power circuit at the meter's testing rate. If the meter tests the circuit at the circuit-off (or circuit-on) schedule, the vitality use is much lower (or higher independently) than the veritable one. Not in any manner like the top tier false load infusion assaults, the present strike safe to the eminent crypto-graphical counter measure that manufactures a safe and time-stepped channel between the meter and the central structure. We realized a simplicity contraption to attack a mimicked electric vitality meter. According to the examination results, the assault procedure is convincing. Furthermore, we propose a countermeasure on the present attack and display its practicality.

Key words: Metering system, Sampling rate, false load injection attacks, Energy meter, Energy consumption

I. INTRODUCTION

As a basic sort of equipment for electric administration associations, electric vitality meters are acquainted at customer's premises with measure the power usage. The meters are examined as often as possible to charge the customers at private, business and mechanical level. In early days, straightforward electromechanical imperativeness meter is the dominating shape. With the advancement of information and correspondence progresses, electric utilities are increasing predictable ground in upgrading their client's basic meters with modernized splendid meters. As keen meters can send the deliberate usage data remotely by methods for a client head correspondence channel, it supports the vitality estimation process, just as enables new applications, for instance, demand measuring, dynamic duty, and burden organization. [8],[10] ,[12]

The propelled meter is severely masterminded as the EB need to scrutinize the meter readings physically. An attacker can douse the yield current and exchange off the meter programming, or adjust the development of correspondence channel among meters and the utility's central structure. This paper demonstrates a novel false burden strike that is invulnerable to all the above countermeasures, and can effectively motivation a great deal of estimation goof of a keen meter. We propose a novel countermeasure that carries intervention into the meter's investigating timing to such a degree, that the attacker will experience issues to synchronize his circuit-trading with meter looking at. [1],[3],[5]

Manuscript published on 30 August 2019.
***** Correspondence Author (s)
Anitha.S Assistant Professor Department of EEE,Bharath Institute of Higher Education & Research,Tamil Nadu
Aarthi Suriya, Assistant Professor Department of EEE,Bharath Institute of Higher Education & Research, TamilNadu
S.P.Vijayaragavan, Associate Professor Department of EEE,Bharath Institute of Higher Education & Research,TamilNadu

II. SYSTEM DESIGN AND ARCHITECTURE

To give the foundation to the present attack, this area first quickly depicts the outline of a smart meter and the vitality estimation guideline. At that point it presents tampering detection, which is utilized to understand the present attack on energy meters. The voltage and current input is continuously measured using Sensors. [7],[9] ,[11]
The MCU is used to extract the sensor values. A current sensor is also placed before connecting the output to the loads. This checks for variation between input and output current. If variation obtained, then theft is detected. The values are displayed on the LCD connected with the microcontroller.
The proposed system is represented in simple in the block diagram representation as shown in the figure 1

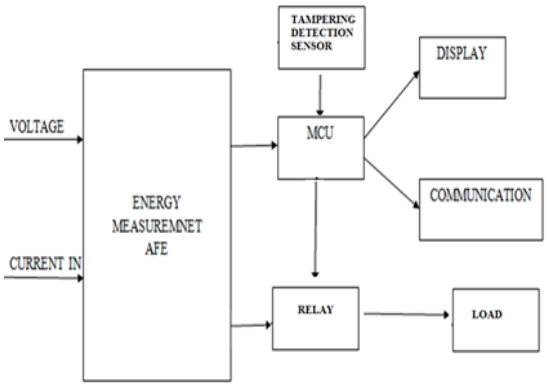


Fig.1. Block representation of System Architecture

III. BLOCK EXPLANATION

The microcontroller is used for the detection of Source voltage and current. The controller continuously detects the Source sensor data's and compares it with the load current extracted by the current sensor at the load output. As long as the load and source current is same, the driver circuit allows the source voltage to pass through to the load.

If the MCU detects a difference between the load and source current, then the driver circuit trips the output voltage from the source to the load. The values of the sensors are constantly updated to the LCD display module attached to the microcontroller. The communication here is displayed with the help of Virtual Terminal. The virtual terminal is used to display the incoming and outgoing data from the controller to the other communication device. [14],[16], [18]

IV. SMART METER

Fig. 1 shows the square of an Intelligent meter, which consolidates AFE, MCU, show, and correspondence module for remote scrutinizing. An AFE contains voltage information circuit, current data circuit and channel circuit, where the voltage information circuit reduces the genuine voltage to satisfy the estimation upper Boundary, the present information circuit changes over the current to a voltage through a present transformer or resistor, and the channel decreases the increase and mistakes displayed by the stage. Likewise, it may have ADC (Analog to Digital Converter) to test the current and Voltage, and figure the power, measure of vitality expended, etc. Through a submitted interface (e.g., Serial Peripheral Interface), a MCU talks with AFE and performs data handling. It furthermore coordinates the significant game plan of AFE, for instance, adjusting meter addition, and compensating stage mistakes. Additionally, the MCU yields the deliberate outcomes in plain view and sends the readings by methods for a correspondence. [19],[21], [20],

V. NEED FOR DRIVER CIRCUIT

The driver circuit used here is obtained an electromagnetic relay. The relays is activated whenever a voltage is transmitted from the microcontroller. When this is happened, then the input voltage is transmitted to the load. The driver circuit here acts as a switch which provides supply to the load whenever the microcontroller passes a control signal of 5voltage to the relay circuit. If the relay is not provided with any voltage, then the source voltage does not passes through to the load. This is done based on two conditions. The first condition depends upon the switch status. Then the next condition is based on the sensor values (The current sensor of the load and source). If the load current and the source current is different, then the controller restricts the output of 5voltage to the relay. Now it reverses the relay state to its initial state.

VI. RELATED WORK

Existing examinations on the security, receive constrained assault layouts that can't well describe who the attackers are. Reachability calculations have been utilized to check the presence of a power theft that will prompt the rupture of a power theftcondition. As opposed to subjective reachability examination, we register the base time until the network recurrence veers off to an inadmissible esteem, which gives a quantitative powerlessness metric in a most pessimistic scenario sense. The conditions for power theft assaults are detected by the sensor estimation. The FDI assaults can delude matrix activities. Develop a model checker to look for assault vectors that can expand the matrix's age taken a toll by a determined rate. The physical effect of assaults has gotten little consideration. In this paper, we break down this effect regarding disturbances of the lattice recurrence.

CIRCUIT DIAGRAM

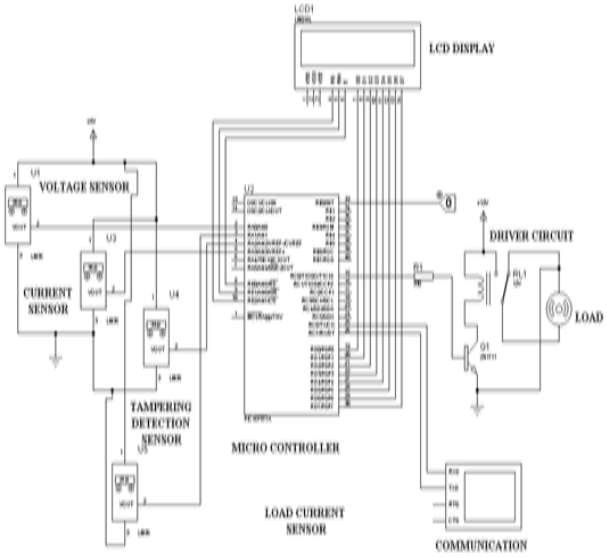


Fig.2. Circuit Diagram

SIMULATION SETUP

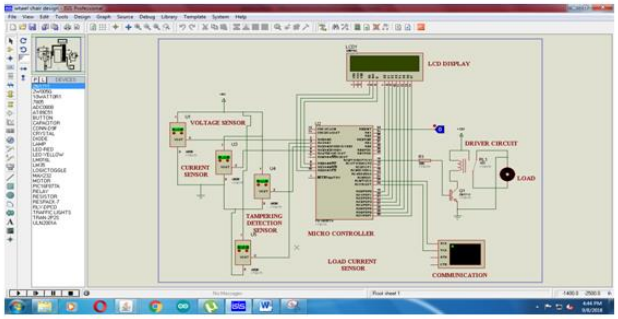


Fig.3. Simulation Setup

VII. CASE STUDIES:

TAMPERING THROUGH HOLES

Smart meters can communicate to the outside world through various wired and wireless communication methods. However, looking into the global landscape, the adoption of these improvements is inconsistent due to a lack of investments in grid infrastructure, challenging environments, and prioritized feature sets

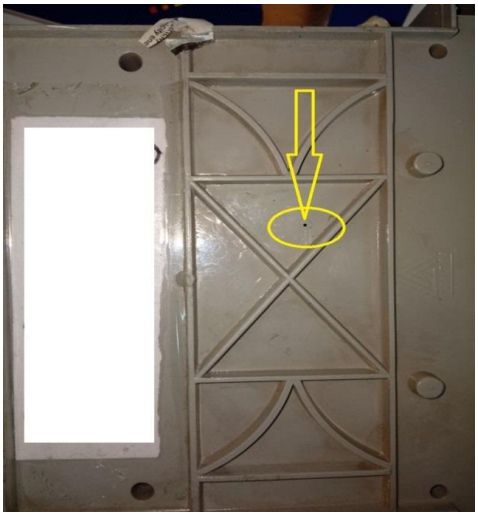


Fig.4 Tampering Through Holes

For example, most meters are electronic in India, but are far behind the concept of smart meters due to poor grid conditions. The image shows the tampering of meters through holes. [23],[22], [24]

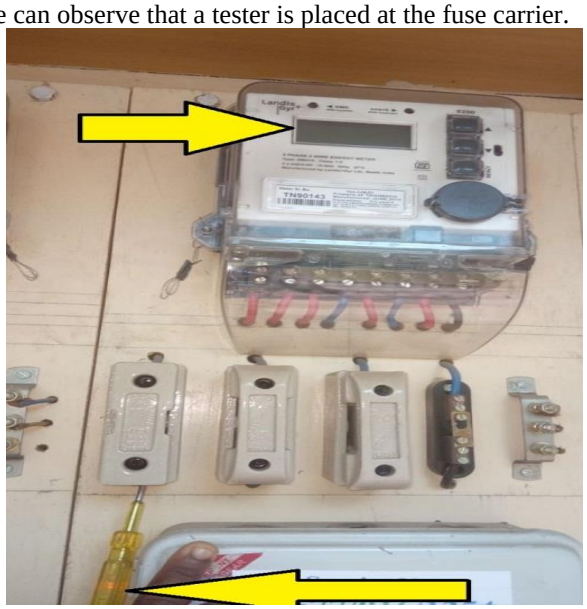
TAMPERING IN PHASE THROUGH HOLES

People will try to steal power by tampering with the meter itself. They will drill a hole in the meter phase coil and tamper through the hole to short-circuit the coil to interrupt the

Fig.4.2. Tampering In Phase Through Holes

4.(c) METER DISPLAY WHILE TAMPERING

We can observe that a tester is placed at the fuse carrier.



As the tester is placed, the load is being consumed, but the meter doesn't record the energy consumed. These causes the safety of the EB meters.

VIII. SIMULATION RESULT

The simulation presents the simulation connection for the proposed paper. The Controller is connected with peripherals. The LCD displays the Sensor values (Voltage Sensor, Current Sensor, Tampering Detection Sensor, Load Current Sensor etc).

Whenever the tampering is detected by the system, then the Power to the load is cut-off using the Driver Circuit. The figure below shows the simulation result. The current theft is displayed on the LCD display.

IX. CONCLUSION

The outcomes additionally show the right activity of the calculation with various control systems and a high unwavering quality and heartiness against false discoveries. The examination and coherent activities, bringing about a lightweight application that can be incorporated in the primary converter controller.

The framework proposed gives a proficient procedure where it confines the power stream from the source to the heap. This empowers a moment location of altering. [25],[27],[29]

REFERENCES

1. Sharma, R.K., Irusapparajan, G. & Periyaazhagar, D. 2019, "Three-phase symmetric cascading Z-source seven levels multilevel inverter excited by multi carrier sinusoidal pulse width modulation scheme", *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 10, pp. 4269-4274.
2. Velavan, R., Bharanidharan, S. & Sheeba, B. 2019, "EMF pollution - Causes, effects and protection", *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 9 Special Issue 3, pp. 1166-1168.
3. Saravana, S., Balaji, S., Arulselvi, S. & John Paul Praveen, A. 2019, "Reliable power quality monitoring and protection system", *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 9 Special Issue 3, pp. 644-645.
4. Tamil Selvan, S. & Sundararajan, M. 2019, "Performance Parameters of 3 Value 8t Cntfet Based Sram Cell Design Using H-Spice", *International Journal of Recent Technology and Engineering*, vol. 8, no. 2 Special issue 5, pp. 22-27.
5. Jac Fredo, A.R., Abilash, R.S., Femi, R., Mythili, A. & Kumar, C.S. 2019, "Classification of damages in composite images using Zernike moments and support vector machines", *Composites Part B: Engineering*, vol. 168, pp. 77-86.
6. Kathiravan, P. & Govindaraju, C. 2019, "Design and evaluation of ultra gain isolated DC-DC converter for photovoltaic system", *International Journal of Engineering and Advanced Technology*, vol. 8, no. 5, pp. 2646-2651.
7. Kripa, N., Vasuki, R. & Kishore Kanna, R. 2019, "Realtime neural interface controlled au-pair BIMA bot", *International Journal of Recent Technology and Engineering*, vol. 8, no. 1, pp. 992-994.
8. Mohanraj, Meenaa Kumari, M., Philomina, S. & Jasmin, M. 2019, "In-situ humidity measurement of hydrogen fuel cell car using MEMS sensor", *International Journal of Recent Technology and Engineering*, vol. 8, no. 1, pp. 41-43.
9. Velmurugan, T. & Prakash, S. 2019, "Artificial intelligent based distribution automation of swift fault detection isolation and power restoration for HT network", *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 6, pp. 1-6.
10. Dwarakesh, K. & Prem Kumar, G. 2019, "Five-level inverter based sequential boost system using fuzzy logic controller", *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 6, pp. 12-19.

11. Anne Gifta, A. & Hemavathi, G. 2019, "Analysis of grid tied solar PV system using ANFIS Algorithm", *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 6, pp. 312-316.
12. Jayavel, R., Rangaswamy, T.R. & Prakash, S. 2019, "Efficient grid management system with renewable and conventional power sources", *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 6, pp. 287-289.
13. Hemavathi, G. & Maheshwaran, S. 2019, "Proportional resonant controlled high gain step-up converter system with improved response", *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 6, pp. 317-323.
14. Periyaazhagar, D. & Irusapparajan, G. 2019, "Design and completion of asymmetric single phase 27 level cascaded mli for various pwm scheme", *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 6, pp. 792-797.
15. Mahalakshmi, V. & Vijayaragavan, S.P. 2019, "PV based power electronic converters for high voltage DC applications", *International Journal of Recent Technology and Engineering*, vol. 7, no. 6, pp. 670-674.
16. Irusapparajan, G., Periyaazhagar, D., Prabaharan, N. & Rini Ann Jerin, A. 2019, "Experimental verification of trinary DC source cascaded h-bridge multilevel inverter using unipolar pulse width modulation", *Automatika*, vol. 60, no. 1, pp. 19-27.
17. Sangeetha, G., Sherine, S., Arputharaju, K. & Prakash, S. 2019, "On Line Monitoring of Higher Rated Alternator using Automated Generator Capability Curve Administer", *Proceedings of the IEEE International Conference on "Recent Trends in Electrical, Control and Communication", RTECC 2018*, pp. 176.
18. Bycil, V.J. & Wiselin, M.C.J. 2019, "Modeling and analysis of vibration energy harvesting system using piezo stack", *International Journal of Mechanical and Production Engineering Research and Development*, vol. 9, no. Special Issue 1, pp. 523-533.
19. Sripada, A., Warrier, A., Kapoor, A., Gaur, H. & Hemalatha, B. 2018, "Dynamic lateral balance of humanoid robots on unstable surfaces", *International Conference on Electrical, Electronics, Communication Computer Technologies and Optimization Techniques, ICEECCOT 2017*, pp. 539.
20. Srinivasan, S., Thirumalaivasan, K. & Sivakumaran, T.S. 2018, "Performance evaluation of double-output luo converters", *Journal of Advanced Research in Dynamical and Control Systems*, vol. 10, no. 10 Special Issue, pp. 870-878.
21. Karthikayen, A. & Selvakumar Raja, S. 2018, "A skellam distribution inspired trust factor-based selfish node detection technique in MANETs", *Journal of Advanced Research in Dynamical and Control Systems*, vol. 10, no. 13, pp. 940-949.

AUTHORS PROFILE

Anitha.S Assistant Professor Department of EEE,Bharath Institute of Higher Education & Research,Tamil Nadu

Aarthi Suriya, Assistant Professor Department of EEE,Bharath Institute of Higher Education & Research, TamilNadu

S.P.Vijayaragavan, Associate Professor Department of EEE,Bharath Institute of Higher Education & Research,TamilNadu