International Journal on Applications in Information and Communication Engineering
Volume 2: Issue 3: March 2016, pp 51-56. www.aetsjournal.com ISSN (Online) : 2394-6237

Electric Meter Monitoring and Theft Detection System

M. Muruganantham , Dr. G.Sathish Kumar

Abstract— Theft of electricity has a material impact on customers in terms of cost and safety. We consider that the existing regulatory framework does not adequately encourage suppliers to be proactive in detecting theft. In this document we are requesting views on proposed new supply license obligations to strengthen the arrangements for tackling theft and on the proposed role of Distribution Network Operators (DNOs) in tackling theft when it is not responsibility of suppliers. We are also consulting on additional policy measures and proposals to support suppliers in investigating, detecting and preventing theft. Theft of electricity increases the costs paid by customers and can have serious safety consequences. It leads to misallocation of costs among suppliers that can distort competition and hamper the efficient functioning of the market. The costs faced by an electricity supplier in detecting electricity theft by its customers may be greater than the costs to the industry as a whole. In particular, when it detects electricity theft by one of its customers, the supplier may incur liabilities relating to generation, network and balancing costs associated with the entry to the settlement system of estimates of the volume of electricity stolen by that customer. On the other hand, this action does not lead to an increase in costs at the level of the industry as a whole. Distribution and transmission network operators, and balancing and system operators, are subject to price controls set by of gem, and any increase in their revenue caused by unexpected additional volumes would result in lower unit charges for all suppliers in the following charging year. Energy charges paid by the supplier on the volumes entered into the settlement system would be treated as a reduction in unexplained losses, leading to lower unit charges for all suppliers. The smart grid refers to the modernization of the power grid infrastructure with new technologies, enabling a more intelligently networked automated system with the goal of improving efficiency, reliability, and security, while providing more transparency and choices to electricity customers. A key technology being widely deployed on the consumption side of the grid is advanced metering infrastructure (AMI). When a theft is detected, the supplier is expected to enter a reasonably accurate estimate of the volume of units that have been stolen into settlement, at which point the supplier becomes liable for the cost of electricity generation, network and balancing charges in relation to those units. The possibility that any theft is eventually detected means that a supplier is exposed to the financial risk of incurring charges relating to the volume of electricity stolen.

Index Terms— Distribution Network Operators (DNO's), Smart Grid, Power Grid Infrastructure, Security, Reliability, Advanced Metering Infrastructure (AMI).

M. Muruganantham (PG Student) Department of Electronics and Communication Engineering ,MNSK College of Engineering, Pudukottai, India

Dr. G.Sathish Kumar , Department of Electronics and Communication Engineering , MNSK College of Engineering ,Pudukottai, India

I. INTRODUCTION

Theft of electricity increases the costs paid by customers and can have serious safety consequences. It leads to misallocation of costs among suppliers that can distort competition and hamper the efficient functioning of the market. The costs faced by an electricity supplier in detecting electricity theft by its customers may be greater than the costs to the industry as a whole. In particular, when it detects electricity theft by one of its customers, the supplier may incur liabilities relating to generation, network and balancing costs associated with the entry to the settlement system of estimates of the volume of electricity stolen by that customer. On the other hand, this action does not lead to an increase in costs at the level of the industry as a whole. Detecting electricity theft has been traditionally addressed by physical checks of tamper-evident seals by field personnel and by using balance meters . Although these techniques reduce unmeasured and unbilled consumption of electricity, they are insufficient. Indeed, tamper- evident seals can be easily defeated, and although balance meters can detect that some customers are fraudulent, they cannot identify the culprits exactly. Despite the security vulnerabilities of smart meters, the higher-resolution data collected by them is seen as a promising technology that will complement traditional detection tools. They have clear potential to improve metering, billing and collection processes, and the detection of fraud and unmetered connections.

Common methods of theft range from compromising the physical security of meters to directly connecting loads to electricity distribution lines. Default of payments has been a major problem, due to suboptimal levels of monitoring and enforcement. The lack of technology and insufficient distributor incentives were the major contributors to this problem. CT (Current Transformer) Sensor is used to measure the incoming current from the Power meter and shown in LCD Display. If you add load to the Power Meter it consume some power this value is shown in lcd as well as computer via serial communication. Voltage Sensor is used to find the voltage level from main supply and shown in lcd .This voltage value is sent to computer using TTL-USB convertor. This alert message is received by owner instantly .The message contain Recent Current, Voltage and Usage values. Units are displaying in the 4 digit 7 segment Led Display. Once the meter is taken the unit reset to 0. If unauthorized person they

The smart grid being globally deployed today will forever change the way energy is used. This new infrastructure offers more efficient, lower cost, and more environmentally sound energy management than its antiquated predecessor. The advanced metering infrastructure (AMI) is a crucial piece of this new smart grid infrastructure. AMI provides a computer-based sensor system that extends from the homes and buildings that use power to the utilities that manage it. From a technology standpoint, AMI provides the necessary communication and control functions needed to implement critical energy management services such as fine grained pricing schemes, automatic meter reading, demand response, and power quality management. The smart grid has been widely deployed in Europe and Asia, with other parts of the world seeing more gradual but accelerating adoption

The smart grid, AMI in particular, introduces new security challenges. By necessity, AMI will consist of billions of low-cost commodity devices being placed in physically insecure locations. The equipment is under the control of the often disinterested, unsophisticated, or sometimes malicious users. Even in simple and/or low value services, such an arrangement would be extraordinarily difficult to secure.

Theft of service for electric meters is nothing new. Annual losses in the United States alone are estimated at $6 billion. Traditional theft in pre-AMI systems required the mechanical manipulation of analog meters. Conversely, in AMI, usage data may be tampered with after recording or in transmission to utilities. Moreover, software based attacks often require less expertise to execute and thus are likely to be more widespread. Precedence has shown and as we argue throughout, that these types of software attacks are quickly monetized by criminal groups that sell the hardware and software needed for theft of service. Examples include the descrambler boxes that lead to over $4 billion in cable theft per year and sites that sell SIM unlock codes for cellular phones. For these reasons, it is imperative for the AMI vendors, energy producers and distributors, governments, and customers to understand the potential scope and source of energy theft. This paper attempts to inform this need.

There is virtually universal agreement that it is necessary to upgrade the electric grid to increase overall system efficiency and reliability. Much of the technology currently in use by the grid is outdated and in many cases unreliable. There have been three major blackouts in the past ten years. The reliance on old technology leads to inefficient systems, costing unnecessary money to the utilities, consumers, and taxpayers. To upgrade the grid, and to operate an improved grid, will require significant dependence on distributed intelligence and broadband communication capabilities. The access and communications capabilities require the latest in proven security technology for extremely large, wide-area communications networks. This paper discusses key security technologies for a smart grid system, including public key infrastructures and trusted computing.

There is disclosed a method of monitoring an electrical network of the type having a feeder line connected to a plurality of distribution transformers, each distribution transformer being in turn coupled to a load which may be provided with a customer meter. The method includes the steps of recording an accumulated in-phase current at each of the distribution transformers over a time period and recording for the same time period an accumulated in-phase current at the feeder line. The sum of the accumulated in-phase currents recorded at the distribution transformers are then compared to the accumulated in-phase current recorded at the feeder line. The method may also include the steps of recording accumulated in-phase currents at the customer meters and comparing their sum with the accumulated in-phase current measured at the distribution transformers coupled to the customer meters. The method may further include a method of automatically detecting the configuration of the network to determine on which phase the customer meters are connected to, and to which distribution transformer said customer meters are connected to, and further, where on the network, relative to a plurality of feeder meters, each of the distribution transformers are connected.

II. RELATED WORK

The major part of the project development sector considers and fully survey all the required needs for developing the project. Before developing the tools and the associated designing it is necessary to determine and survey the time factor, resource requirement, man power, economy, and company strength. Once these things are satisfied and fully surveyed, then the next step is to determine about the software specifications in the respective system such as what type of operating system the project would require, and what are all the necessary software are needed to proceed with the next step such as developing the tools, and the associated operations.

More recent work has emphasized the need to consider consumption data anomalies as part of a diagnostic system, with the aim of enabling sensor fusion at the scale of an electricity distribution network, and reduce false positives

We present an attack tree for energy theft in the single requirement for energy theft is the manipulation of the demand data. There are three ways to tamper with demand data; a) while it is recorded (via electromechanical tampering), b) while it is at rest in the meter, and c) as it is in flight across the network. We discuss each of these ways in detail. The first class of attacks, which aim to prevent the meter from accurately measuring demand, is the only class that previously existed for analog meters. The other two classes are exclusive to AMR and AMI. AMI does increase the difficulty of executing this class of attacks by logging sensor data that determines when power is cut to the meter, or if reverse energy flow occurs. Thus, to execute attacks A1.1 or A1.2 undetected, it is necessary to also erase the logged events that indicate outage or reverse energy flow before they are retrieved by the utility

As these events are stored in the meter along with demand measurements, their removal falls under the second class of attacks on data stored in meters. Smart meters store a large range of data. This includes tariffs for TOU pricing, logs of both physical events and executed commands, recorded net demand and their own programs among others. Because effectively all aspects of a smart meter's behavior are controlled by the contents of its storage, the ability to tamper with that storage gives a customer complete control over its operation. An attack involving overwriting the meter's firmware, while powerful, is a significant reverse engineering task. Thus, this type of attack is limited to members of organized crime aimed at selling meter hack kits. For the purposes of energy theft, only a few select items in the meter's storage are of interest, namely, audit logs and the recorded total demand. Both of these values can be accessed through established administrative interfaces which require passwords. Their modification is usually limited to reset, clear in the case of an audit log and zero in the case of demand record. Consider the case in which a malicious customer has somehow obtained a meter password. The customer's electric bill may be reduced by X% by executing a demand reset operation after the first X% of the billing cycle. Because the administrative interface to the meter requires login credentials, a prerequisite to these attacks is extracting the necessary passwords from the meter. We explain one method that can be used for extracting the meter passwords and explain the far reaching consequences once they are no longer secret. The third class of attacks involves injecting forged values into communication between meters and utilities. These attacks contribute to the above described monetization of energy theft in that they may be executed by any node between the meter and utility, which is not necessarily at the site where the meter is located. Furthermore, because of the two tier architecture of AMI, (local networks and backhaul links), executing a network based attack at a collector node makes possible the modification of all demand recorded for the set of repeaters. In some commercially available AMI systems, this can be in upwards of 1,000 nodes depending on the particular metering system. The goal for subtree (3) requires two distinct types of actions, interposition of the attacker on the backhaul network and injection or modification of traffic between the meter and utility. Interposition is needed for any passive attack, including capturing the protocol between meters and utilities for reverse engineering. Network interposition can most easily be achieved close to one of the endpoints. For customers, tapping a line between the meter and the first backhaul link is the easiest. Utility insiders would have ready access to the links and routers leading up to the computers performing remote meter reads. The second task, traffic injection, requires the attacker to replace demand information from meters with forged data. In the event that an AMI system correctly uses cryptography for message integrity and authentication, this attack will require that the keys used for encryption first be extracted from meter storage.

If there is a flaw in the authentication or integrity protocols between the meter and utility, then a meter spoofing attack is sufficient for sending forged demand data and event logs. In this attack, a common device, such as a laptop computer, is used to receive calls from the utility in place of the meter and provides crafted values for specific fields. If the authentication mechanism is flawed but an encrypted channel is established between the meter and utility, a "man in the middle attack" (MIM) will be required. This involves a node on the backhaul link from the meter to the utility to impersonate one to the other while the secure session is established to obtain the key used for cryptographic message integrity.

III. PROPOSED SCHEME

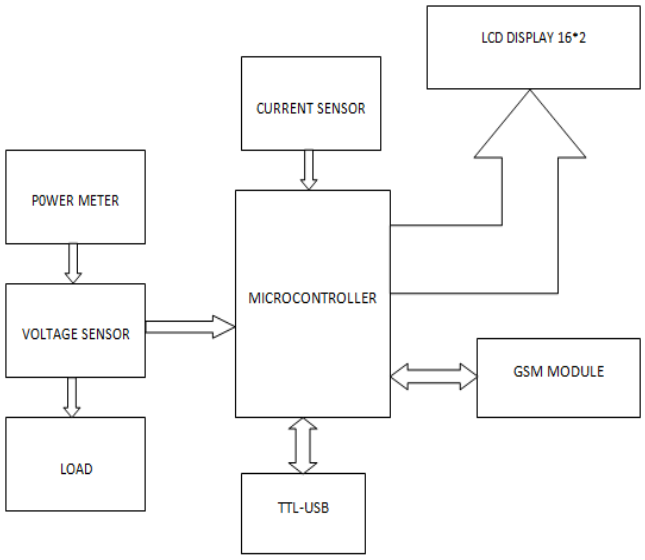

Fig.1 Block Diagram for Energy Meter Theft Detection

This System consists of Microcontroller unit, LCD Display, Sensors like Voltage and Current Sensor. The PCF8574 has a low current consumption and includes latched outputs with high current drive capability for directly driving LEDs or LCD Display. The I2C-bus is for 2-way, 2-line communication between different ICs or modules. The two lines are a serial data line (SDA) and a serial clock line (SCL). Both lines must be connected to a positive supply via a pull-up resistor when connected to the output stages of a device. Data transfer may be initiated only when the bus is not busy. One data bit is transferred during each clock pulse. The data on the SDA line must remain stable during the HIGH period of the clock pulse as changes in the data line at this time will be interpreted as control signals. The device consists of an 8-bit quasi-bidirectional port and an I2C-bus interface. CT (Current Transformer) Sensor is used to measure the incoming current from the Power meter and shown in LCD Display. If you add load to the Power Meter it consume some power this value is shown in lcd as well as computer via serial communication. Voltage Sensor is used to find the voltage level from main supply and shown in LCD .This voltage value is sent to computer using TTL-USB convertor. 74HC595 are 8-stage serial shift registers with a storage register and 3-state outputs.

The registers have separate clocks. Data is shifted on the positive-going transitions of the shift register clock input (SHCP). The data in each register is transferred to the storage register on a positive-going transition of the storage register clock input (STCP). If both clocks are connected together, the shift register will always be one clock pulse ahead of the storage register .Shift Register which controls the 4 digit 7 Segment Led Display.GSM Module is used to sent SMS to the Owner about billing Details and usage of Units. This alert message is received by owner instantly .The message contain Recent Current, Voltage and Usage values. Units are displaying in the 4 digit 7 segment Led Display. Once the meter is taken the unit reset to 0. If unauthorized person they are using power it gives instant SMS alert to the owner.

IV. CIRCUIT DIAGRAM

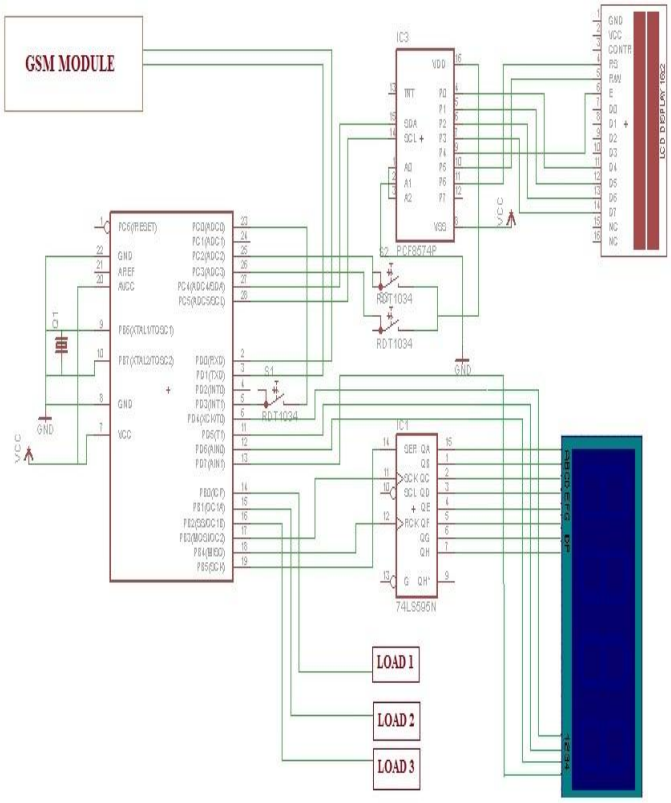

Fig.2 Schematic Diagram

CT (Current Transformer) Sensor is used to measure the incoming current. Shift Register which controls the 4 digit 7 Segment Led Display. The PCF8574 has a low current consumption and includes latched outputs with high current drive capability for directly driving LEDs or LCD Display. GSM Module is used to send SMS to the Owner about billing Details and usage of Units. If unauthorized person they are using power it gives instant SMS alert to the owner.

V.METHODOLOGY

1) ATMEGA 328

The ATmega328P provides the following features: 32K bytes of In- System Programmable Flash with Read-While-Write capabilities, 1K bytes EEPROM, 2K bytes SRAM, 23 general purpose I/O lines, 32 general purpose working registers, three flexible Timer/Counters with compare modes, internal and external interrupts, a serial programmable USART, a byte-oriented 2-wire Serial Interface, an SPI serial port, a 6-channel 10-bit ADC (8 channels in TQFP and QFN/MLF packages), a programmable Watchdog Timer with internal Oscillator, and five software selectable power saving modes. The Idle mode stops the CPU while allowing the SRAM, Timer/Counters, USART, 2-wire Serial Interface, SPI port, and interrupt system to continue functioning. The Power-down mode saves the register contents but freezes the Oscillator, disabling all other chip functions until the next interrupt or hardware reset. In Power-save mode, the asynchronous timer continues to run, allowing the user to maintain a timer base while the rest of the device is sleeping. The ADC Noise Reduction mode stops the CPU and all I/O modules except asynchronous timer and ADC, to minimize switching noise during ADC conversions. In Standby mode, the crystal/resonator Oscillator is running while the rest of the device is sleeping. This allows very fast start-up combined with low power consumption. The device is manufactured using Atmel's high density non-volatile memory technology. The On-chip ISP Flash allows the program memory to be reprogrammed In-System through an SPI serial interface, by a conventional non-volatile memory programmer, or by an On-chip Boot program running on the AVR core. The Boot program can use any interface to download the application program in the Application Flash memory. Software in the Boot Flash section will continue to run while the Application Flash section is updated, providing true Read-While-Write operation. By combining an 8-bit RISC CPU with In-System Self-Programmable Flash on a monolithic chip, the Atmel ATmega328P is a powerful microcontroller that provides a highly flexible and cost effective solution to many embedded control applications. The ATmega328P AVR is supported with a full suite of program and system development tools including: C Compilers, Macro Assemblers, Program Debugger/Simulators, In-Circuit Emulators, and Evaluation kits.

2) PL 2303 USB-TTL

Single-chip USB to Serial (RS232/RS422/RS485) asynchronous serial data transfer interface With Fully Compliant with USB Specification v2.0 (Full-Speed) Integrated USB 1.1 Transceiver and 5V to 3.3V Regulator. Integrated 96MHz clock generator (No external crystal required).Integrated OTPROM (One-Time Programming ROM) – no external EEPROM required. For writing and storing customer USB VID/PID, Serial Number, Product String, and other device startup configurations. (uses default

settings if OTPROM is empty) Supports USB to RS232 Serial UART Interface. Full-duplex transmitter and receiver (TXD and RXD) Six MODEM control pins (RTS, CTS, DTR, DSR, DCD, and RI) 5, 6, 7 or 8 data bits Odd, Even, Mark, Space, or None parity mode. One, one and a half, or two stop bits, Parity error, frame error, and serial break detection, Programmable baud rate from 75 bps to 12M bps. External RS232 driver power down control Independent power source for serial interface Supports RS-422/RS-485 like serial interface (TXD, DTR_N, and RTS_N pins should be externally pulled-up to 5V) Extensive Flow Control Mechanism Adjustable high/low watermark level. Automatic hardware flow control with CTS/RTS or DSR/DTR. Automatic software flow control with XON/XOFF Inbound data buffer overflow detection. Configurable 512-byte bi-directional data buffer, 256-byte outbound buffer and 256-byte inbound buffer; or 128-byte outbound buffer and 384-byte inbound buffer Supports Remote Wake-up from RS232 input pin signals (RI, RXD, DSR, DCD, CTS) Four (4) General Purpose I/O (GP0, GP1, GP2, & GP3) pins and Four (4) Auxiliary General Purpose I/O (RI_N, DSR_N, DCD_N, & CTS_N) pins. Supports Windows Selective Suspend by OTPROM configuration (Enable Remote Wakeup) Suspends power of chip when idle (COM port is closed) provides royalty-free USB to Virtual COM Port drivers for Windows, Mac, Linux, and Android.

3) LCD Display

Liquid Crystal Display which is commonly known as Alphanumeric Display can display Alphabets, Numbers as well as special symbols thus alphabets. Graphic display has embedded controller for controlling different modes. Controller accepts commands and data bytes from micro controller. LCD display has total 16 pins for interface with processor. RS is instruction or data select line. This pin is kept high or low by microcontroller to indicate command instruction or data bytes on data bus db0-db7. Special feature of this LCD module is it allows reading of data bytes stored in RAM. Pin no. 5 i.e. R/W is used for deciding read operation or write operation. Graphic display has RAM memory for storing characters codes to be displayed on LCD. We have used 16 x 2 Alphanumeric Display which means on this display we can display two lines with maximum of 16 characters in one line.

4) Current Sensor

A current sensor is a device that detects and converts current to an easily measured output voltage, which is proportional to the current through the measured path. When a current flows through a wire or in a circuit, voltage drop occurs. Also, a magnetic field is generated surrounding the current carrying conductor. Both of these phenomena are made use of in the design of current sensors. Thus, there are two types of current sensing: direct and indirect. Direct sensing is based on Ohm's law, while indirect sensing is based on Faraday's and Ampere's law. The IC has an internal filter resistance of 1.7 kΩ, and the carrier board includes a 1 nF filter capacitor, which produces a low-pass RC filter with a 90 kHz cutoff. You can improve sensing system accuracy for low-frequency sensing applications by adding a capacitor in parallel with the integrated 1 nF capacitor across the pads marked "filter" on the bottom silkscreen (this capacitor is labeled C2b in the schematic below). The frequency F that the filter will attenuate to half its original power is given by:

$F = 1 / (2\pi RC) = 1 / (11k\Omega * (1\ nF + Cf))$

Where Cf is the value of the capacitor added to the filter pads.

5) PCF8574

The I2C-bus is for 2-way, 2-line communication between different ICs or modules. The two lines are a serial data line (SDA) and a serial clock line (SCL). Both lines must be connected to a positive supply via a pull-up resistor when connected to the output stages of a device. Data transfer may be initiated only when the bus is not busy. One data bit is transferred during each clock pulse. The data on the SDA line must remain stable during the HIGH period of the clock pulse as changes in the data line at this time will be interpreted as control signals. The device consists of an 8-bit quasi-bidirectional port and an I2C-bus interface. The PCF8574 has a low current consumption and includes latched outputs with high current drive capability for directly driving LEDs. It also possesses an interrupt line (INT) which can be connected to the interrupt logic of the microcontroller. By sending an interrupt signal on this line, the remote I/O can inform the microcontroller if there is incoming data on its ports without having to communicate via the I2C-bus. This means that the PCF8574 can remain a simple slave device.

6) GSM Module

The SIM900 is a complete Quad-band GSM/GPRS solution in a SMT module which can be embedded in the customer applications. Featuring an industry-standard interface, the SIM900 delivers GSM/GPRS 850/900/1800/1900MHz performance for voice, SMS, Data, and Fax in a small form factor and with low power consumption. With a tiny configuration of 24mm x 24mm x 3 mm, SIM900 can fit almost all the space requirements in your M2M application, especially for slim and compact demand of design.

7) Shift Register 74HC595

74HC595 are high-speed Si-gate CMOS devices and are pin compatible with Low-power Schottky TTL. 74HC595 are 8-stage serial shift registers with a storage register and 3-state outputs. The registers have separate clocks. Data is shifted on the positive-going transitions of the shift register clock input (SHCP). The data in each register is transferred to the storage register on a positive-going transition of the storage register clock input (STCP). If both clocks are connected together, the shift register will always be one clock pulse ahead of the storage register. The shift register has a serial input (DS) and a serial standard output (Q7S) for

cascading. It is also provided with asynchronous reset (active LOW) for all 8 shift register stages. The storage register has 8 parallel 3-state bus driver outputs. Data in the storage register appears at the output whenever the output enable input (OE) is LOW.

VI. CONCLUSION

A second game-theoretic model, which is not fully covered here, assumes that all customers have the same initial preferences (utility function) and that they make a decision to become fraudulent, or stay genuine, depending on the probability of detection and the fine they would face if caught. Once the customers make their decisions about which type they will be (genuine or fraudulent), they could be viewed as if they are playing the game described in this article. Therefore, this second model could also be viewed as a leader-follower game, where relative to the first model; the customers have to make an additional decision, that is, to choose whether they will be honest or fraudulent. For any fixed fine and detection probability, it is possible to determine what fraction of customers will be fraudulent in equilibrium. Thus, it is possible to jointly solve the problem of the distributor's choice of security investment and find the corresponding fraction of customers that would choose to be fraudulent with a given security investment. Then, the problem becomes identical to the original formulation. This allows the distributor to compute expected profit as a function of security investment. Next, if the distributor is a monopolist, it maximizes its profit and chooses the equilibrium level of investment in monitoring fraud that achieves the highest profit.

REFERENCES

[1] S. McLaughlin, D. Podkuiko, and P. McDaniel, "Energy theft in the advanced metering infrastructure," in Proc. 4th Int. Conf. Critical Information Infrastructures Security, 2009, pp. 176–187.

[2] Guidelines for smart grid cyber security: Privacy and the smart grid, U. S. Dept. Commerce, Nat. Inst. Standards Technol., Interagency Rep. 7628, Aug. 2010, vol. 2.

[3] M. Lemay and C. A. Gunter, "Cumulative attestation kernels for embedded systems," IEEE Trans. Smart Grid, vol. 3, no. 2, pp. 744–760, 2012.

[4] E. de Buda, "System for accurately detecting electricity theft," U.S. Patent Application 12/351 978, Jan. 2010.

[5] A. W. Appel, "Security seals on voting machines: A case study," ACM Trans. Inform. Syst. Secure., vol. 14, no. 2, pp. 1–29, 2011.

[6] P. Antmann, "Reducing technical and non-technical losses in the power sector," World Bank, Washington, D.C., Tech. Rep., July 2009.

[7] S. McLaughlin, D. Podkuiko, S. Miadzvezhanka, A. Delozier, and P. McDaniel, "Multi-vendor penetration testing in the advanced metering infrastructure," in Proc. Annu. Computer Security Applications Conf., Dec. 2010, pp. 107–116.

[8] M. Davis. (2009, July). Smart grid device security. Adventures in a new medium. [Online]. Available: http://www.blackhat.com/ presentations/ bhusa09 /MDAVIS/BHUSA09-Davis-AMI-SLIDES.pdf