A Novel Approach for Detecting and Mitigating the Energy Theft Issues in the Smart Metering Infrastructure

Pallab Ganguly¹ · Mita Nasipuri² · Sourav Dutta³

Received: 29 November 2017 / Accepted: 17 October 2018 / Published online: 27 October 2018
© Springer Nature Singapore Pte Ltd. 2018

Abstract

Smart meters are intelligent, responsive energy meters deployed for measurement and communication of energy consumption by the end consumer. This data is used for grid management, billing, fault detection, etc. So, it is paramount to ensure the availability and integrity of this data without compromising the privacy of the consumers. While the smart grid provides protection against amateur physical tampering techniques, it is vulnerable to hacking by malicious users or organized groups. With all the smart meters connected to the same network, security loopholes might have increased exposure to potential exploits resulting in revenue loss. We aim to provide an exhaustive list of all possible attacks on the smart meters including viable physical tampering and data hacking techniques and provide a novel approach to countering energy theft. To address the issue of energy theft, we propose a method which successfully detects and mitigates energy theft in the Smart Metering Infrastructure with attack exposure analysis including a Customized detection algorithm, Meter Data Tampering Algorithm (MDTA) and we suggest inserting a one-way function, named as Unique String Authentication Procedure (USAP) into the smart meter which is also stored in the Meter Data Management System (MDMS) database. The unique string generated at the meter end is authenticated with that generated at the MDMS. This novel method successfully detects and mitigates energy theft in the Smart Metering and Advanced Metering Infrastructure.

Keywords Advanced metering infrastructure · Energy theft · MDTA · One-way function · Smart grid · Smart meter · USAP

Introduction

With the advent of Advanced Metering Infrastructure [AMI], the traditional power grid today is transformed into the intelligent smart grid, and the analog meters are getting replaced by smart energy meters. Smart Grid is a next generation automated power generation and distribution system to provide a stable electrical power environment to support all functionalities of conventional and intelligent power systems that enhances the quality of power distribution maintaining a proper demand response system [1]. Smart meters are the most fundamental component which offers key functionalities like

remote readings of power consumption, and time of the day usage of tariffs; it facilitates a two-way information flow in infrastructure which integrates electricity generation and distribution [2] together with communication and provides high fidelity, power flow control, reliability and security [3] of the Smart Grid. It transforms the power grid from outdated, proprietary and legacy system to an advanced, intelligent communication technology [4].

Implementation of Smart Grid began with the United States of America, Nordic countries, Japan, Italy, UK and others. Increasingly more developing countries are acknowledging the benefits [5] which include increased grid resiliency and efficiency. Smart Grid involves an increased dependency on cyber resources, which may be a point of vulnerability for developing nations. Smart grid deployment in developing countries will bring its own challenges due to aggressive and hasty application, ageing infrastructure which is complex and ill planned, massive meter roll-out and limited budget. Within the present economic conditions in developing countries, a huge percentage of populations are involved in tampering the energy meters to save on their electricity bills.

✉ Pallab Ganguly
pallab.ganguly@rp-sg.in

¹ CESC Ltd, Kolkata, India

² Jadavpur University, Kolkata, India

³ IBM, Kolkata, India

In AMI, smart meters are installed within every user's premises. It measures the energy consumption at regular intervals and communicates it to a central Meter Data Management System (MDMS) using a private Radio Frequency (RF) mesh or public internet. While this data is extremely useful to the utilities, in the wrong hands it can prove to be extremely disastrous. However, more and more smart devices are being connected to the Home Area Network which can be remotely monitored and controlled through the Smart Grid Control Center. Smart meters not only need protection from outside attacks but also domestic and internal attacks. Since the entire billing is based on the readings provided by the smart meters to the Central MDMS, there is enough incentive for home owners and man-in-the-middle attackers to tamper the readings to reduce their electricity bills. On top of that the meters are installed in insecure locations within the user's premises with minimal safeguards. So, users have both the incentive and opportunity to tamper with smart meters [6, 7]. On the other hand, the utility will have a tendency to increase the units measured to charge the customer more.

Earlier researches have also demonstrated that inclusion of encryption in smart meters have degraded their performance in terms of computational processing and memory utilization. So, a security solution without a resource hungry function is needed to maintain the availability and integrity of the smart metering infrastructure.

To address this issue, we propose a novel method which successfully detects and mitigates energy theft in Smart Metering as well as Advanced Metering Infrastructure with attack exposure analysis including a Customized detection algorithm, Meter Data Tampering Algorithm (MDTA) and a mathematical one-way function, Unique String Authentication Procedure (USAP). Section II of this paper discusses the earlier research works related to data tampering and detection methods, and various limitations of these tampering techniques. Section III, introduces all possible tampering techniques, and a modular algorithm to detect tampering named as MDTA. Section IV, defines a mathematical model to implement an one-way function to detect and mitigate energy theft realistically. Section V, illustrates the simulation details with results.

Background

The conventional power grid was planned to distribute power from the generating stations to the commercial and domestic consumers. These were mostly government owned monopolies where consumer satisfaction was given top priority. Over time, a lot of users have been taking advantage of the minimal safeguards and irresponsibility of the government. In most of the localities resided by financially inconvenienced people, stealing power is not even shunned upon, and is a credit to the wits of the user. But with the privatization of utilities and advancement

in communication technology, one has an opportunity to put a check on energy theft.

According to a brochure on Emerging Markets Smart Grid: Outlook, 2015 [8], each year the world loses around 89.3 billion US\$, of which the highest losses were recorded in India followed by Brazil and Russia. If we look at India, most theft take place in Mumbai, Maharashtra, home to the third largest slum in the world, Dharavi. The theft techniques employed are very crude and amateurish, which can be easily countered but due to the ineffectiveness of the government and utility alike, perpetrators have been getting away with it. Implementation of smart meters might prove extremely potent, since they require more sophisticated theft techniques. But this will provide an opportunity to organized crime to make large-scale replicable products that can be used to steal electricity [9, 10]. Hence, protection against more advanced forms of tampering like data hacking will become more critical [11].

Previously many researchers have tried to hack into the AMI to find its security limitations [12]. A few of the architectural weak points that can be exploited by hackers to break into the AMI are 1) insecure data buses and serial connections, 2) data capture and injections, 3) stealing or replacing keys of the embedded devices memory, 4) firmware level vulnerabilities and 5) resetting of Joint Test Action Group (JTAG) fuses. While on the utility side, vulnerabilities exist in the form of buffer overflows, Structured Query Language (SQL) injection, credential hijacking, etc. Lawson [13] and Carpenter [14] had successfully identified the JTAG pins and dumped the program in the microcontroller through JTAG cable. They proved that the microcontroller code can be hacked easily and manipulated at any instance.

Another area of concern is the different communication standards and protocols used for smart metering [15]. If proper safety measures are not implemented the data can be caught on the fly and manipulated and then re-sent as credible data [16, 17]. With the advancement in telecommunication technologies faster and cheaper communication systems are being developed [18, 19] and due attention must be provided to firewalling and authentication protocols. Researchers have shown concern about how data privacy was not given as much importance as data security. Authors have proposed to use dedicated authentication servers in order to inhibit unauthorized nodes to gain access to sensitive information [20, 21]. Researchers have also proposed implementation of a key management system over existing infrastructure, but this incurs huge managerial costs and overloads the system due to the large deployment.

Smart Grid Attack Detection Techniques

Real Time Comparison Based Method

This method [22, 23] proposes to install two smart meters with one electric wire, connected to the consumer and utility

provider. Based on real time energy consumption of the user, if the disparities between the readings of the two meters pass a certain threshold then the consumer is adjudged as malicious. This method has a very high success ratio, because we can say with certainty whether theft is taking place or not. But it has two very major drawbacks; one is the requirement of a separate meter for every user which will be extremely cost incursive, and not worth compared to the number of malicious users caught. Also individual checking of each meter is computationally intensive and time consuming considering the huge number of meters deployed.

Binary-Coded Grouping Based Inspection

This is an optimization of the Real-time comparison based method [24]; it provides a grouping algorithm to greatly reduce the number of inspectors required and hence makes the procedure cost effective and faster. The meters are numbered numerically and encoded into binary and based on the positions of the 1's in the binary code, they are connected to the inspector meters. Depending on the malicious smart meter, the inspecting meters will give anomalous readings. We need to identify the anomalous meters from the inspector meter readings. This method is costly and complicated when the number of meters under inspection is huge, or the number of malicious meters is large. It also makes the network extremely complex.

Penetration Testing Using Attack Trees

When we consider attacking a smart meter there is always an adversarial goal which has to be achieved [25, 26]. If we go on dividing them into sub goals we will reach a set of attacks that achieve the original goal. This method includes:

- a) Using architectural description, design archetypal trees.
- b) Identify the system under test that may thwart archetypal attacks.
- c) Based on the vendor specific models design concrete trees.
- d) Attempt to achieve the concrete sub goals by performing penetration testing on the System under test (SUT).

This method is extensive but at the same time cumbersome and we must build individual trees based on different vendor specifications. And the accuracy is variable depending on the vendor.

Fuzzy Logic Based Attack Detection

In this technique, fuzzy logic is employed to estimate the most appropriate system values of a particular anomaly detection formulation. With the present system in place, it is very easy to generate malicious reading using an illegitimate device

impersonating the original one. Fuzzy logic allows us to assume values in $[0, 1]$. This optimization technique considers "Total Cost" and "Detection Rate", to get a low "Total Cost" for a high "Detection Rate". To get the best tradeoff between the two parameters, this technique can be effectively used to mitigate device implant attacks [27].

Machine Learning Based Algorithm

This algorithm is used to present an automated solution for rapid diagnosis of client device problems in private cloud. Clients are diagnosed with the aid of Transmission Control Protocol (TCP) packet traces, by (i) observation of anomalous artifacts occurring as a result of each fault and (ii) subsequent use of the inference capabilities of soft-margin Support Vector Machine (SVM) classifiers [28]. A consumer is deemed malicious if his current consumption differs abnormally from the predicted value, but this is highly unjust, as there can be several legitimate reasons for a change in a user's consumption patterns. Another major drawback is that for implementing machine learning one need to get historical data for old meter users, which is not available for new meter users. Even for service providers who have not kept digitized record of old users this is unviable. So, utilities need to wait for a couple of years to collect enough data. Still the results are not very convincing [29].

So, it may be concluded that the existing tamper detection techniques are neither exhaustive nor computationally intensive to be deployed for a large utility network. We need to devise a method that is fairly accurate and is cost effective to maintain a large network.

Identity Based Secured Communication

There have been multiple papers on identity number based encryption as a means to mitigate energy theft. Identity numbers based keys are generally preferred over randomly generated keys as they are unique to customers, but in case the private key is lost anyone can impersonate the user [30]. There have been few improvements with the use of physical unclonable functions, so that the hardware cannot be compromised and non-interactive distribution network between smart meters are geared with a secure and leakage free storage of keys [31].

Financial Impact

Utilities and governments incur huge losses due to widespread energy theft [32], while the theft from individual houses may not seem so much, but the amount of people practicing tampering makes it intolerable for the utilities. Energy theft not only affects utilities but also honest customers as they have to bear the cost of inflated bills raised by utilities to recover

losses. They live through frequent power cuts and low voltages which degrades the whole user experience. If the malicious users get caught they are forced to pay an exorbitant fine, which also hurts their social standing in the neighborhood.

We can visualize that in the long run, energy theft hurts everyone whether they realize it or not. Thus, we need to make people more aware about energy theft and make them feel the overall impact. This may act as a social deterrence to stop energy theft.

Smart Meter Attack Exposure Analysis

Communication System

The two major communication systems prevalent in the smart metering scenario [33]:

- Public Internet** –In this setup, the smart meters have an in-built GPRS supported modem to communicate with a Base Transceiver Station of the service provider. The data is routed through the internet to the Utility provider's network. Channelized through load balancer and filtered through the firewall, it reaches the core switch which performs role based access control and requisite files are sent to the metering server for processing and then sent to the billing server for consumer billing. The points of vulnerability are marked in Fig. 1 with arrows.
- RF mesh network**- It refers to the huge network of inter-connected smart meters, which serve as nodes. It is an adaptive intelligent communication network in which the signal hops from one node to another until it reaches its destination. The smart meters try to communicate using the access points and in case of failure there is a provision for cellular communication through public internet. Through the access point the signal reaches the corporate network which passes through a core switch and firewall and finally to the MDMS with the help of a trusted IPsec Virtual Private Network (VPN) channel. Then it reaches the billing server where the consumer is charged. The various points of vulnerability are marked in Fig. 2 with arrows.

When we need to uphold the safety and security of a system the following criteria should be met:

- Confidentiality** - It is the system of concealing sensitive information, for the sake of the privacy of the consumer or utility. This concerns both dynamically produced data like energy reading and static data like personal information of the consumer. We need to prevent snooping which may lead to violation of privacy of the

Fig. 1 Vulnerabilities in smart meter communication using Public Internet

consumer and at the same time needs to protect the utility from the consumer.

- Integrity** - This refers to the credibility or trustworthiness of not only the data but also the source of the data. This is very important because the entire billing is directly based on the units measured and sent by the smart meter. So, both the credibility of the data and the source is important.
- Availability** - It refers to the uptime of the system to use the data or resources required by it whenever it wants to. A major security threat in smart meters is Denial of

Fig 2 Vulnerabilities in smart meter communication using RF mesh network

Service (DOS). The data from the smart meter is acquired by polling so it is essential that it is always available.

- d) **Non-repudiation** - It means that both the sender and receiver cannot deny the accountability of any data transaction they have been party to. The non-accountability of members gives rise to a gray area that can be exploited by hackers.

Tampering Techniques

We have broadly classified tampering into two parts:

- 1) **Physical Tampering** – This encompasses any tampering scheme for which an individual needs to be physically in the close vicinity of the meter. In this type of tampering the consumer is mostly responsible and is a ploy to take advantage of the minimal safeguards of smart meter. No formal education is required to accomplish this, so it is hugely popular among members of lower middle economic class.
- 2) **Data Hacking** – A more sophisticated way of tampering; this is mostly related to organized crime. The motivation here is to monetize the whole process of energy theft, selling of hardware or software tools to compromise smart meters, or even worse to cause cyber war. Data can be manipulated in a number of ways - corrupting meter storage, system, on the fly spoofing and man in the middle attacks etc.

Physical Tampering

The various methods [34, 35] can be categorized as:

- 1) *Magnetic Interference* - One of the most vulnerable parts of a smart meter is the current and voltage sensors. The voltage can be easily replaced with a fixed value since it mostly remains constant but the entire load measurement depends on the current sensor value. If the current sensor is Current Transformer based it is very easy to saturate the core with a strong magnet and this may give erroneous readings.
- 2) *Bypassing meter or unbalanced current* - This technique involves connecting the load, like a metal plate, between the leads of the smart meter where live wires are connected. This gives a lower reading than the real consumption of the user. It is difficult to find this theft within the large pools of meters installed in an inaccessible manner. This gives a lower reading than the real consumption of the user. It can be easily detected by measuring the current through the live and neutral wires, normally they should be equal. If they are not, the meter should be flagged.

- 3) *Reversing current leads* - Reversing the current leads result in the smart meter measuring a negative value, so the smart meter in essence is counting backwards. This requires the consumer to swap the wires connected to live. With the newer meters, it is easy to flag them for single phase as it gives negative reading but for three phases, its reversing causes two phases to cancel out giving us a third of the total consumption. A possible counter measure is to secure the smart meter with a sealed enclosure.
- 4) *Electrostatic discharge* - Another method of tampering is to apply an Electro Static Discharge (ESD) to the meter using spark plugs or Cathode Ray Tube- Extra High tension (CRT-EHT) destroying the meters measurement capabilities. This can be avoided by providing proper shielding which has an adverse effect on the cost of meters.

Data Hacking

The various methods of data hacking [36] [37] [38] can be categorized as:

- 1) *Through smart meters hardware* – It is possible to figure out a smart meter programming by using pins on each side of the memory chip. Intercepting and analyzing the signals, the programmer can hack into it.
- 2) *Using Digital Radio* – The smart meter has its own communication network over which it sends and receives commands and information. So, it is possible to use a digital radio to get into the meter network and issue commands if the meters programming is known.
- 3) *Accessing the meter* – One can also use a software radio which can be programmed to mimic a number of communication system and snooping how the meter communicates with other meter and devices.
- 4) *Spreading malware in the network* – The attack can be more widespread. If the attacker has guessed the programming, he can create malware that would spread within the meters in the network and shut them down. This would have hard impacts, and can bring down the whole distribution network.
- 5) *Eavesdropping* - There are several communication protocols in use today by the smart meters. These are mostly insecure and are vulnerable to eavesdropping by hackers. These not only include a breach of privacy of the consumer but the stolen data can be used for more malicious activities. Stringent protocols must be implemented along with password verification, but again this would have an overhead cost.
- 6) *Meter Spoofing* - This problem is associated with the fact that the meters are installed in insecure locations,

by reverse engineering the consumer can use an adversarial device that impersonates the legitimate one.

- 7) *Password extraction* – Using optical port snooping, the password of any smart meter can be extracted.
- 8) *Man in the middle* – One of the most common forms of attacks, considering the whole smart network communication between systems is instrumental. But this allows hackers to intercept signal on the fly and transmit the manipulated data [39]. The system is not sophisticated enough to detect the small delay. There have been attempts to mitigate it using Intrusion Detection Systems (IDS) when a rogue node tries to steal information [40].
- 9) *Denial of Service* – To cripple the entire Advanced Metering Infrastructure, a hacker can overload the entire system beyond its capabilities so that legitimate devices cannot get access to essential services due to network congestion [41, 42]. One of the easiest ways to perform widespread Denial of Service (DoS) attacks is with Internet of Things (IoT) devices and has been studied in detail [43].
- 10) *False Data Injection* – One of the most studied attacks, False Data Injection causes false estimation of states which may lead to widespread power system failure [44].

In Fig.3, we have tabulated the entities of Data Hacking of smart meters and marked individually the data tampering techniques from H1 to H8.

In Fig.4, we have tabulated the entities of Physical Tampering of smart meters and marked individually the physical tampering techniques from P1 to P4.

MDTA Algorithm

We have tabulated all the possible forms of data tampering and are now in the process of developing a modular algorithm as mentioned below in Fig.5, which will individually counter each tampering techniques. The algorithm considers inputs from Feeder Remote Terminal Units [FRTU]. The power line goes from the FRTU through the pillar box into consumer households. A number of smart meters are connected to a single FRTU. So, from the FRTU we can get the total consumption in kilo watt hour unit drawn, by all the houses with smart meters under it. By excluding the transmission and

distribution losses, we get the total consumption of consumers. It is obvious that these two values must match. We have assumed that transmission and distribution loss are completely dependent on the specific utility. Depending on the network condition and utility, the range is generally between 11%–26%. The average is around 17% [45].

The first step is to match the value measured by the FRTU to the summation of consumption by all the meters connected to it through pillar box. A disparity in measurement suggests that one or more smart meters are sending aberrant values.

In case of disparity we need to identify the smart meter that is under-counting. If we consider both old meters and new meters, historic data about the consumption pattern of the consumer over the past few years is available to the utility. The energy value, load curve and events of these meters are available to the utility, so we can perform cluster analysis of the load curve with all the historical data set for the past years and months of that day, to find any abnormality in the reading. This gives us a preliminary idea of whether there is a possibility of tampering. However, for new meters, we don't have any historical data. For such meters, we propose to perform cluster other meters in the same network, having same maximum demand, this helps to separate households with possibly fallacious measurement.

Now we move on to the generally practiced cases, magnets can saturate transformer cores, so transformer based sensor gives reduced readings. Therefore, the smart meter produces lower energy consumption. While the current drawn depends on the load, the voltage reading should be always around standard value. So, we can verify magnetic interference by checking the voltage reading. A low voltage may be a sign of tampering, but we need to check with neighboring meters because it may also be caused by high demand.

Another method of tampering is bypassing the meter, but the difficulty with that is unbalanced current in live and neutral wires. So, we can easily catch a bypassed meter by matching the current in live and neutral wires.

If a user gets into the programming codes, he may attempt to change the passwords of the individual smart meters since all the passwords are stored in the central database. The passwords can be randomly checked with the database to find whether any password is manipulated or not. The smart meter itself generates events when it is physically tampered and reported to the MDMS and the utility can take appropriate action. The power factor of a household should vary between

Fig. 3 Tampering smart meter measurement through data hacking

Fig. 4 Physical tampering of smart meters

Fig. 5 Flowchart of the meter data tampering algorithm

0.8–0.9 depending on the utility allowance, if it is beyond range it may be a sign of passives being used to cause

interference. The algorithm mentioned below in Fig. 5 allows us to identify smart meters which have been possibly

tampered with and can also detect the type of tampering. But with limited data resource and huge computational complexity, it is nearly impossible to identify every tampered smart meter. The algorithm is not infallible but we need a more reliable solution that will detect and mitigate the problem without increasing computational cost. In the next section, we have used a Unique String Authentication Procedure (USAP) function to take care of data hacking.

Mathematical Model for Detecting and Mitigating Data Hacking

A cryptographic Unique String Authentication Procedure (USAP) is a kind of ‘signature’ for a text. USAP generates

an almost-unique signature for any text input. A USAP is not an ‘encryption’ – it cannot be decrypted back to the original text (it is a ‘one-way’ cryptographic function, having a fixed size for any size of source text). This makes it suitable when it is appropriate to compare USAP versions of texts, as opposed to decrypting the text to obtain the original version. Unlike other encryption techniques this will not increase the price of smart meters, nor will it consume more power and increase overhead for utilities while ensuring a fault proof system to catch data tampering. In Fig. 6, the Unique String Authentication Procedure is explained through a flow chart. Here the amount of consumed energy in the smart meter is considered as (UY). After applying USAP on the amount of consumed energy in the smart meter, a string H1 is generated in the smart meter which along with UY is sent to the MDMS

Fig. 6 Authentication procedure in MDMS using One-way function

database at every 15 min interval. At the server end again the USAP is applied on the amount of consumed energy and a string H2 is generated and stored in the database. At the Server level, every time the electronic meter sends the UY + H1, the H1 value is compared with the H2 value and in case of aberration, an error message is displayed. In case the value matches the data is saved into the database.

The activities in the smart meter end, the data transmission process and the server database end are mentioned below.

a. Activity in Electronic Meter End

Each subscriber device contains a built-in USAP function F (p), unique only to itself, where “p” is the variable amount of consumed energy (UY) measured by the smart meter at regular intervals. The USAP function F (UY) generates a result, say “H1”, having fixed number of bits for every “UY” measured.

b. Activity during Transmission

The energy measured by smart meter (UY) is jacketed with the function generated value “H” and sent using either public internet cloud or RF mesh network. Any attempted tampering attack is caught at the server end.

c. Activity at the Database & Server end

At the MDMS end there is a database of all the USAP functions for every smart meter, as it receives an unique “H1” for its respective “UY”, using the meter number and the USAP function from the database it itself generates “H2”.

A comparison of “H1” and “H2” is performed.

1. If the digit values are same then we can conclude that no alteration of measured energy consumption was performed on the subscriber end or on the fly.
2. If the digit values are not same then we can conclude that alteration of variable energy consumption was performed.

Table 2 Simulation results

32 bits Input (UY)	48 bits Output Result (H)
4321	129,032
6547	330,578
7896	634,934
4563	228,368
9871	789,587
8975	786,785
5973	493,091
3598	184,372
1989	106,982
5912	457,082

This results in generation of Interruption Indication message.

Simulation Result Analysis

Table 1 shows the comparison of the one-way function, USAP with the other popular algorithms like Message –Digest [MD4, MD5] and the different versions of Secure Hash Algorithm [SHA] on the basis of output size in bits, internal state size in bits, block size in bits, word size in bits, and rounds, which is the number of times the function is run to get the specified size of output data. The internal state size means the “internal hash sum” after each compression of a data block. A block size in cryptographic function is a chunk of data of a specified size. This chunk of data may be a set of decimal digits of specified length or a set of binary data of specified bit length.

“Word size” refers to the number of bits processed by a computer’s CPU in one go. Data bus size, instruction size, address size are usually multiples of the word size.

In the simulation setup, the proposed function is implemented in JAVA on a 1.8 GHz personal computer with 4 GB of main memory. As shown in Table 2, a set of random energy

Table 1 Comparison of one-way function with various encryption techniques

Algorithm	Output size (bits)	Internal state size (bits)	Block size (bits)	Word size (bits)	Rounds
MD4	128	128	512	32	3
MD5	128	128	512	32	64
SHA-224, SHA-256	224/256	256	512	56	64
SHA3-224	224	1600	1152	64	24
SHA3-256	256	1600	1088	64	24
SHA3-384	384	1600	832	64	24
SHA3-512	512	1600	576	64	24
USAP	Dynamic	1024	Dynamic	Dynamic	7

values were given as 32 bits Input (UY) and a set of 48 bits Output result (H) were obtained. The input value is present inside the string (one-way output cryptographic function). Here both the values are represented numerically.

Conclusion

There are two key contributions identified in this research that would enhance the security of the smart metering Infrastructure. First, it presents a novel technique in form of a modular algorithm MDTA to detect data theft in Smart meters. The research also focuses on Smart Meters from a security and privacy perspective. Security issues in the AMI are physical tampering and data hacking. The algorithm primarily compares the consumption values from the FRTU and the individual smart meters and then detects the thefts related to physical tampering.

Secondly, we have also proposed a new concept for solving the problems of data hacking which is mentioned in the Mathematical model through a unique 160 bit (20-byte) one way cryptographic function, USAP. The test data and simulation results along with the benefits of USAP with other cryptographic mechanisms are discussed in detail. A set of random energy values are given as input and a set of sample results are obtained. This result signifies that for any energy consumption value (UY), a string (H) is generated where the input value is present inside the string (one-way output cryptographic function). Here both the input and output values are represented numerically.

The results are found satisfactory as it yields a value of 20 byte crypto function where the energy value is embedded and cannot be tampered by any third party mechanism or man-in-the middle attack. We have also addressed the detection of energy theft through physical tampering or data hacking meticulously and also the mitigation of data hacking is addressed but the mitigation of the physical tampering is open to research.

References

- Peter Palensky, Dietmar Dietrich, (2011) Demand side management system: demand response, intelligent energy systems and smart loads, *IEEE Transaction on Industrial Informatics*, vol.7, no. 3, pages: 381–388, Aug, 2011, 7, 381, 388
- Pei W, Deng W, Shen Z, Zhao Z, Wang J (November, 2013) Design and implementation of energy hub in smart grid. *Inf Technol J* 12: 4797–4804. <https://doi.org/10.3923/itj.2013.4797.4804>
- Queen EE (2011) Smart meters and smart meter system: a metering industry perspective. In: *An EEI-AEIC-UTC White Paper*, published by: Edison Electric institute, 701 Pennsylvania avenue, N.W. Washington, D.C, USA, 20004–2696, march
- Jason Allen, Lasse Kari, Charlotte Raut and Carmen Uys, Realising the full potential of smart metering, *Accenture's Digitally Enabled Grid* program, April, 2016. [Online]. Available: <https://www.scribd.com/document/261125020/Accenture-Smart-Metering-Report-Digitally-Enabled-Grid-pdf>
- International Energy Agency, Technology Roadmap, SmartGrids, *International Energy Agency*, 9 rue de laFédération, 75739, Paris, Cedex, 15, France, April,2011. [Online]. Available: https://www.iea.org/publications/freepublications/publication/smartgrids_roadmap.pdf
- Sana Sardar, Sanaullah Ahmed, Detecting and Minimizing Electricity Theft: A Review, November, 2015. [Online]. Available: https://www.researchgate.net/publication/308207798_Detecting_And_Minimizing_Electricity_Theft_A_Review
- Jeff McCullough, Deterrent and detection of smart grid meter tapering and theft of electricity, water, or gas *Elster*, 208 S Rogers Lane, Raleigh, NC 27610–2144, United States, 2010. [Online]. Available: <https://www.elstersolutions.com/assets/downloads/WP42-1010A.pdf>
- Northeast Group, llc, Emerging Markets Smart Grid-Outlook 2015, 2014. [Online]. Available: <http://www.northeast-Group.com/reports/Brochure-Emerging%20Markets%20Smart%20Grid-Outlook%202015-Northeast%20Group.pdf>
- Rajiv K Bhatia, Varsha Bodade, Smart grid security and privacy: challenges, Literature Survey and Issues, *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 4, no. 1, January 2014
- Marek Jawaurek, Felix C. Freiling (2011) Privacy Threat Analysis of Smart Metering *INFORMATIK 2011- Informatik schafft Communities*, 41. Jahrestagung der Gesellschaft für Informatik, 4.-7.10.2011, Berlin
- Emiliano Palloti, Federica Mangiatordi, (2011) Smart Grid Cyber Security Requirements, *10th International Conference on Environment and Electrical Engineering (EEEIC)*, Rome, Italy, 8–11 May, 2011. <https://doi.org/10.1109/EEEIC.2011.5874822>
- Mike Davis, (2009) Smart Grid Device Security- Adventures in New Medium, *IOActive, Comprehensive Computer Security Services, Black hat, USA*, 2009. [Online]. Available: <http://www.blackhat.com/presentations/bh-usa-09/MDAVIS/BHUSA09-Davis-AMI-SLIDES.pdf>
- Nate Lawson, (2010) Reverse-engineering a smart meter, February15, 2010. [Online]. Available: <https://rdist.root.org/2010/02/15/reverse-engineering-a-smart-meter/>
- Mathew Carpenter, Travis Goodspeed and Josh Wright, (2008) Hacking AMI, *InGuardians, Inc.*, 2008. [Online]. Available: <https://rmccurdy.com/scripts/downloaded/Pen%20Test%20Perfect%20Storm/090202-SANS-SCADA-Hacking%20AMI.pdf>
- Fadi Aloul, A.R. Al-Ali, Rami Al-Dalky, Mamoun Al-Mardini, Wassim El-hajj, (2012) Smart grid security: threats, vulnerabilities and solutions, *International Journal of Smart Grid and Clean Energy*, vol. 1, no. 1, September, 2012
- Sophia Kaplantzis and Y. Ahmet Sekercioglu, (2012) Security and Smart Metering, *18th European Conference 2012*, April 18–20, 2012, Poznan, Poland
- Ye Yan, Yi Qian, Hamid Sharif and David Tipper, (2012) A survey on cyber security for smart grid communication. *IEEE Communications Surveys & Tutorials*, vol.14, no.4, January, 2012, 998–1010
- Taarek Khalifa, Kshirasagar Naik and Amiya Nayak, (2010) A survey of communication protocols for automatic meter Reading applications, *IEEE Communications Survey and Tutorials*, vol. 13, Issue. 2, January, 2010, pages: 168–182
- Stefan Feurhahn, Michael Zillgith, Christof Wittwer and Christian Wietfeld, (2011) Comparison of the communication protocols DLMS/COSEM, SML and IEC 61850 for smart metering applications, *IEEE International Conference on Smart Grid*

- Communications (SmartGridComm)*, Brussels, Belgium, 17–20 Oct 2011
20. Farid Morzalem, Security and Privacy of Smart Meters: A Survey, 2012, [Online]. Available: <https://doi.org/10.1109/JSYST.2013.22606977>
 21. Tanvi Mehra, Vasudev Dehalwar, Mohan Kolhe, (2013) Data communication security of advanced metering infrastructure in smart grid, *5th International Conference and Computational Intelligence and Communication Networks*, Mathura, India, 27–29 sept, 2013
 22. Jing Liu, Yang Xiao, (2014) Achieving accountability in smart grid, *IEEE Syst J*, vol. 8, no. 2, June, 2014, 493–508
 23. Zhifeng Xiao, Yang Xiao and David Hung-Chang Du, (2013) Exploring Malicious Meter Inspection in Neighborhood Area, *IEEE Transaction on Smart Grid*, Vol. 4, No.1, March, 2013, Page(s): 214–226
 24. Xiao fang Xia, Wei Liang, Yang Xiao and Meng Zheng, (2015) BCGI: a fast approach to detect malicious meters in neighborhood area smart grid, *IEEE International Conference on Communications (ICC)*, London, UK, 8–12 June, 2015
 25. Stephen McLaughlin, Dmitry Podkuiko, Sergei Miadvezzhanka, Adam Delozier and Patrick McDaniel, (2010) Multi-vendor penetration testing in the advanced metering infrastructure, *Proceedings of the 26th Annual Computer Security Applications Conference (ACSAC)*, Austin, Texas, USA, December, 2010, Pages: 107–116
 26. Rong Jiang, Rongxing Lu, Ye Wang, Jun Luo, Changxiang Shen and Xuemin Shen, (2014) Energy-theft detection issues for advanced metering infrastructure in smart grid, *Tsinghua Sci Technol* Volume. 19, Issue. 2, April 2014, Pages: 105–120
 27. Saif Ahmed, Zubair A. Baig, (2012) Fuzzy-based optimization for effective detection of smart grid cyber-attacks, *International Journal of Smart Grid and Clean Energy*, vol. 1, no. 1, September 2012: pp. 15–21
 28. Chaturanga Widanpathirana, Y. Ahmet Sekercioglu, Paul G. Fitzpatrick, Milosh V. Ivanovich, Jonathan C. Li, (2011) Diagnosing Client Faults Using SVM-based Intelligent Inference from TCP Packet Trees, *6th International Conference on Broadband Communication & Biomedical Application (IB2COM)*, Melbourne, VIC, Australia, 21–24 Nov. 2011
 29. J. Nagi, K. S. Yap, S. K. Tiong (December 2008) Detection of Abnormalities and Electricity Theft using Genetic Support Vector Machines, *TENCON 2008 - IEEE Region 10 Conference*, Hyderabad, India, 19–21 Nov, 2008
 30. Taimin Zhang, Xin Lu, Xiaoyu Ji, Wenyun Xu (2017) An Identity-Based Secure Communication Scheme for Advanced Metering Infrastructure in Smart Grid, *29th Chinese Control and Decision Conference (CCDC)*, Chongqing, China, 28–30 May 2017
 31. Vahe Seferian, Rouwaida Kanj, Ali Chehab, Ayman Kayssi, (2016) Identity Based Key Distribution Framework for Link Layer Security of AMI Networks, *IEEE Transaction on Smart Grids, (Early Access)*, November, 2016, Page: 1–1
 32. Salman Yussof, MMohd. Ezanee Rusli, Yunus Yousuf, Roslan Ismail, Azimah Abdul Ghapar, (2014) Financial impact of smart meter security and privacy breach, *International Conference on Information Technology and Multimedia (ICIMU)* Putrajaya, Malaysia, 18–20 Nov 2014
 33. Ye Yan, Yi Qian, Hamid Sharif and David Tipper, (2013) A survey on smart grid communication infrastructure: motivations, requirements and challenges, *IEEE Communication Surveys & Tutorials*, Vol 15, No. 1, First Quarter 2013, 5–20
 34. Stephen McLaughlin, Dmitry Podkuiko, and Patric McDaniel, (2009) Energy theft in the Advanced Metering Infrastructure, *Conference: Critical Information Infrastructures Security, 4th International Workshop, CRITIS 2009*, Bonn, Germany, September 30–October 2, 2009
 35. Robert Czechowski, Anna Magdalena Kosek, (2016) The Most frequent energy theft techniques and hazards in present power energy consumption, *Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG)*, Vienna, Austria, April, 2016
 36. Florian Skopik, Zhedong Ma, Thomas Bleier, Helmut Gruneis, (2012) A Survey on Threats and Vulnerabilities in Smart Metering Infrastructure *International Journal of Smart Grid and Clean Energy*, Volume: 1; Issue: 1; September 2012: pp. 22–28
 37. Dmitry Podkuiko, (2012) Vulnerabilities in advanced metering infrastructure, M.S. thesis, thesis in computer science and engineering, Pennsylvania State University, the graduate school, Dept. of computer science and Engineering, August, 2012
 38. Jing Liu and Yang Xia, (2012) Cyber security and privacy issues in smart grids, *IEEE Communication Survey and Tutorials*, Vol. 14, No. 4, , 2012, 981–997
 39. Pallab Ganguly, Sumit Poddar, Sourav Dutta, Mita Nasipuri, (2016) Analysis of the security anomalies in the smart metering infrastructure and its impact on energy profiling and measurement, *In Proceedings of the 5th International Conference on Smart Cities and Green ICT Systems (SMARTGREENS)*, Rome, Italy, Volume 1, April, 2016, pages 302–308
 40. Abhjeet Sahu, H N R Karthik Tippanaboyana, Lindsay Hefton, Ana Goulart, (2017) Detection of rogue nodes in AMI networks, *19th International Conference on Intelligent System Application to Power System (ISAP)*, San Antonio, TX, USA, 17–20 Sept. 2017
 41. Khaled Shuaib, Zouheir Trabelsi, Mohammad Abed-Hafez, Ahmed Gaouda, and Mahmoud Alahmad, (2015) Resiliency of smart power meters to common security attacks, *6th International Conference on Ambient Systems, Networks and Technologies (ANT)*, Volume 52, 2015, Pages 145–152
 42. Yonghe Guo, Chee-Wooi Ten, Shiyan Hu and Wayne W. Weaver, (2015) Modeling distributed denial of service attack in advanced metering infrastructure, *Innovative Smart Grid Technologies Conference (ISGT)*, 2015 IEEE Power & Energy Society, Washington, DC, USA, 18–20 Feb. 2015
 43. Yasin Yilmaz and Suleyman Uludag, (2017) Mitigating IOT-based cyberattacks on the smart grid, *16th IEEE International Conference on Machine Learning and Application (ICMLA)*, Cancun, Mexico, 18–21 Dec 2017
 44. Sandeep Kumar Singh, Kush Khanna, Ranjan Bose, Bijaya Ketam Panigrahi, Anupam Joshi, (2018) Joint transformation based detection of false data injection attacks in smart grid, *IEEE Transaction on Industrial Informatics*, Volume: 14, Issue: 1, Jan. 2018, 89–97
 45. Electric power transmission and distribution losses, IEA Statistics© OECD/IEA, 2014 IEA Statistics Accessed Nov 2017, [Online]. Available: <http://data.worldbank.org/indicator/EG.ELC.LOSS.ZS>