A Survey of Energy Theft Detection Approaches in Smart Meters

Chapter · December 2020

DOI: 10.1007/978-981-15-8820-4_2

2 authors, including:

Arjun Choudhary
Sardar Patel University of Police, Security and Criminal Justice, Jodhpur
41 PUBLICATIONS **140** CITATIONS

SEE PROFILE

Chapter 2
A Survey of Energy Theft Detection Approaches in Smart Meters

Divam Lehri and Arjun Choudhary

1 Introduction

Since last decade numerous efforts have been made by the governments and distribution companies to counter electricity theft but it still remains a challenge. The entire loss suffered by the power sector is known as Transmission and Distribution Losses (TD Losses) which comprises an aggregate of Technical Losses (TL) and Non-Technical Losses (NTL). TD losses represent the difference between the electricity generated and the electricity consumed. Technical losses are those losses which are internal to the system such as energy dissipation by the electrical equipments used in distribution lines, transformers, transmission lines, and iron losses in transformers. On the other hand, NTL constitutes losses arising due to defective meters, errors in billing, flaws in supply, unmetered connections, and malicious activities by the consumer such as tampering of meter. Table 1 provides an overview of different types of electricity losses caused by different components of power sector.

The easiest way to determine the amount of non-technical losses (NTL) is by merely calculating the technical losses (TL) in the system and subtracting it from total losses (TD).

We can evaluate it as follows:

$$\text{NTL} = \text{Total Energy Losses(TD)} - \text{TL} \tag{1}$$

$$\text{Total Energy Losses} = \text{Energy Supplied} - \text{Bills paid} \tag{2}$$

D. Lehri (✉) · A. Choudhary
Sardar Patel University of Police, Security and Criminal Justice, Jodhpur, India
e-mail: lehridivam@gmail.com

A. Choudhary
e-mail: a.choudhary@policeuniversity.ac.in

M. Shorif Uddin et al. (eds.), *Intelligent Energy Management Technologies*,
Algorithms for Intelligent Systems,
https://doi.org/10.1007/978-981-15-8820-4_2

Table 1 Classification of methods of electricity theft

Elements	Methods of theft
Meters	Bypassing the meter Deliberately damaging the meter seals or removing of the meter
Wires/Cables	Illegal tapping to bare wires or underground cables
Transformers	Illegal tapping of transformer terminals and junction boxes of overhead lines
Billing irregularities	Errors made by meter readers
Unpaid bills	Unpaid bills by individuals or institutions

Some of the losses such as TL are unavoidable. The energy theft in India is majorly due to unmetered usage of electricity. The concept of Transmission and Distribution (TD) losses has been extended further to Aggregate Technical and Commercial losses (AT&C).

$$\text{AT \& C Losses} = \{1 - (\text{BE} \times \text{CE})\} \times 100 \tag{3}$$

$$\text{T \& D Losses} = \{1 - (\text{BE})\} \times 100 \tag{4}$$

where

$$\text{Billing efficiency (BE)} = \text{Total unit Billed/Total unit Inputs} \tag{5}$$

$$\text{Collection efficiency (CE)} = \text{Revenue collected/Amount Billed} \tag{6}$$

TD loss is the difference in input energy and energy billed. There is no account for the losses arising due to low collection. AT&C loss is the difference in input energy and energy for which revenue has been collected. Simply stated AT& C Loss can be aggregated as

$$\text{AT \& C Losses} = \text{TL} + \text{CL} \tag{7}$$

Statistics on electricity losses in India shows that around 10–12% of AT&C losses amount to technical reasons, while remaining 18–20% comprises commercial reasons [1] known as commercial losses (CL). According to U.S. Energy Information Administration (EIA) [2] in the countries with low rate of theft and optimal technical efficiency TD losses generally span between 6 and 8%. Figure 1 shows graphical representation of AT &C loss percentage of different Indian states.

In such scenarios adoption of smart meters by the government of India could prove as a game changer to curb electricity theft. There is also a grave need to develop a common framework in the country where governments, manufacturers, research institutions, Distribution system operators (DSOs) and academia work with mutual

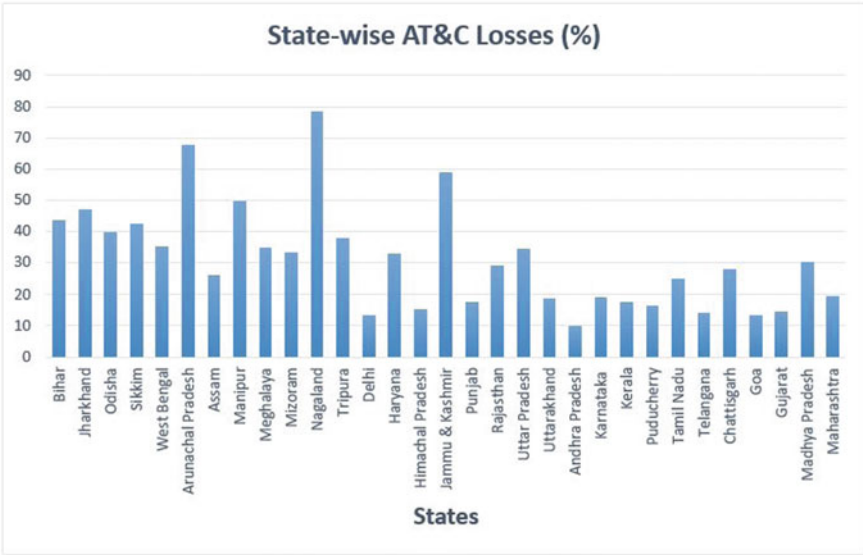

Fig. 1 A visual representation of state-wise AT&C losses (%) for the period Apr'14–Mar'15, According to catalog available on Open Government Data Platform (OGD), India [3]

cooperation to ensure resiliency, privacy and security of smart grid. A paradigm of one such framework is SEGRID Project [4] for European Digital Grid. While smart meters may not be completely theft resistant but they are capable of minimizing the number of theft cases due to their immunity against traditional electricity theft methods as well as the real-time monitoring of data between the utility companies and the consumers.

Due to the complex architecture and large attack surface of Advanced Metering Infrastructure (AMI), Smart Meters are vulnerable to tampering thereby requiring effective theft prevention and detection techniques. In this paper, we present a survey of available energy theft detection techniques.

2 Meter Tampering Methodologies

There are various mechanisms through which an adversary can tamper Smart Meters. Methods of meter tampering can be divided into four classes:

- Current related tampering methods.
- Voltage related tampering methods.
- Mechanical tampering methods.
- Tampering by hacking and altering the memory.

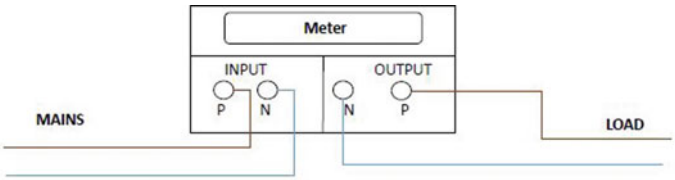

Fig. 2 Actual connection

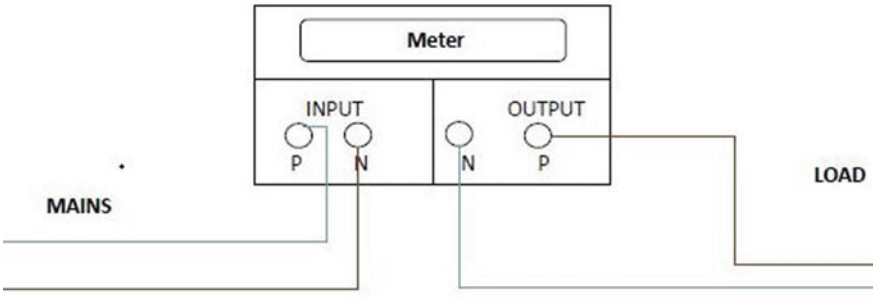

Fig. 3 Swapping of phase and neutral lines

A summary of mechanisms that are generally used to tamper smart meters is presented in this section.

2.1 Swapping of Phase and Neutral Lines

In this method of tampering the adversary interchanges the phase and neutral lines. This swapping of phase and neutral lines reverses the energy flow thereby effecting the billing calculation (Figs. 2 and 3).

2.2 Double Feeding

Double feeding as the name suggests is a meter bypassing technique where an additional feeder is connected to the meter in such a manner that meter gets bypassed and the energy consumption is not accounted for. Under such scenario the consumption for the load affixed to the supplementary feeder won't be recorded by the meter even if the connection is legitimate. This type of tampering is generally done to connect any heavy electric appliance so that it's consumption remain unnoticed (Fig. 4).

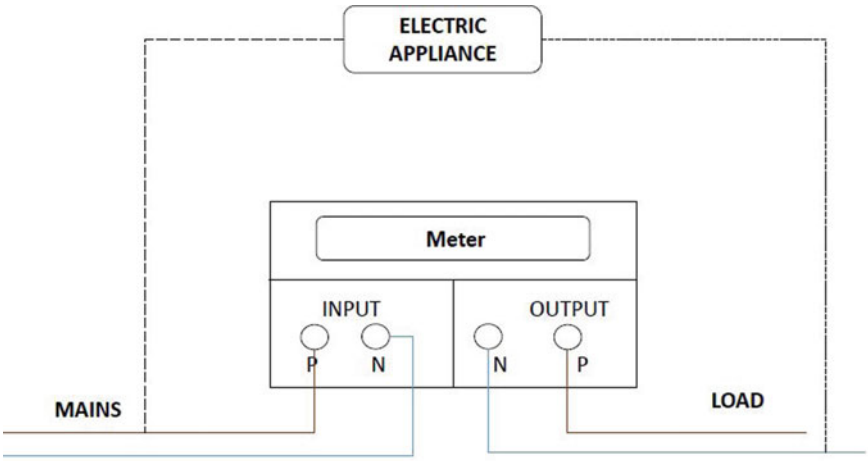

Fig. 4 Double feeding

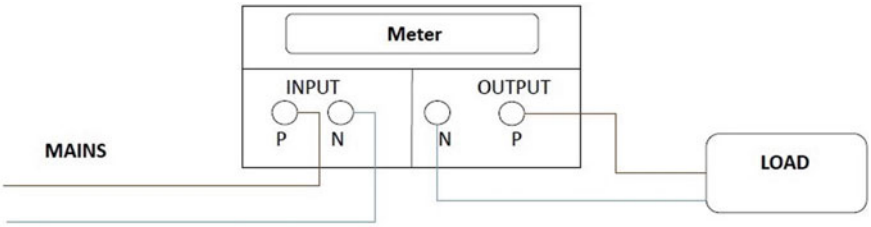

Fig. 5 Actual condition

2.3 Neutral Missing

In this method of meter tampering, the neutral line is completely cut-off from the meter thereby resulting in zero input voltage. Hence the power computed by the meter is zero (Since P = V * I and for given condition V = 0, therefore P = 0) This tampering method is also referred to as single wire operation [5] (Figs. 5 and 6).

2.4 Neutral Disturbance

In this method of tampering some noise (High-Frequency voltage signals) is added to the neutral line of the meter by connecting it through diode/variable resistance/capacitor. The neutral of the meter gets deviated from its original point and becomes unbalanced leading to less voltage recording by the meter and therefore less energy consumption is recorded by the meter (Fig. 7).

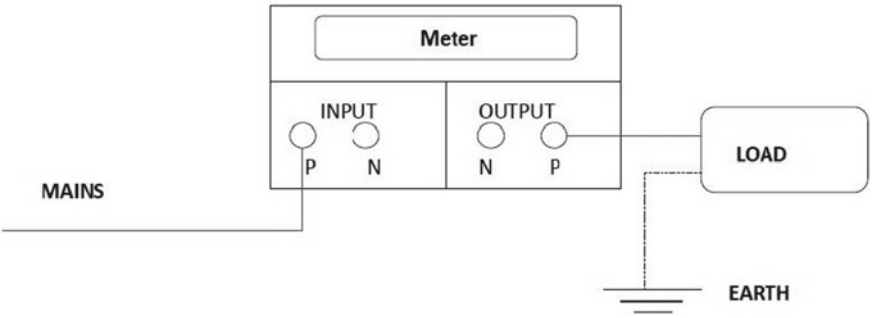

Fig. 6 Neutral missing

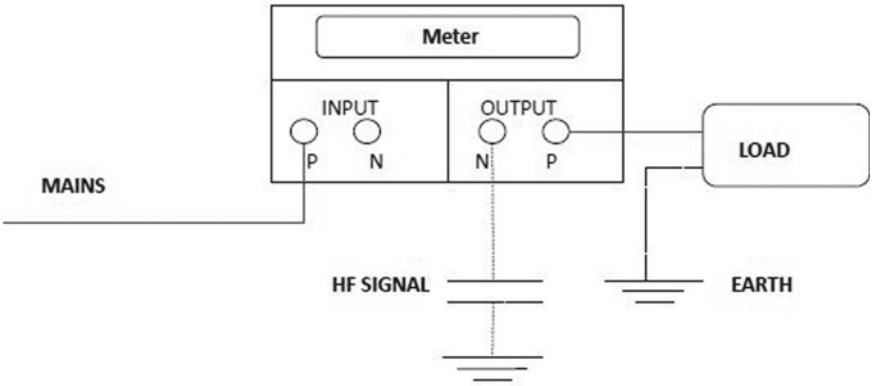

Fig. 7 Neutral disturbance

2.5 Current Reversal by Connecting Input and Output in Reverse

In this tampering event, the adversary connect the phase and neutral wires to the wrong inputs. This causes the current to change direction from it's original path in which it was intended to flow. The intention of this kind of tampering is to dupe the billing computation by reversing the route of current flow [6] (Fig. 8).

2.6 Partial Earth Fault Condition

It is a tampering method in which the load is connected to the earth due to which the return current going back to the meter is reduced. This generates a difference in the current stream flowing through the neutral wire and phase wire leading to current in

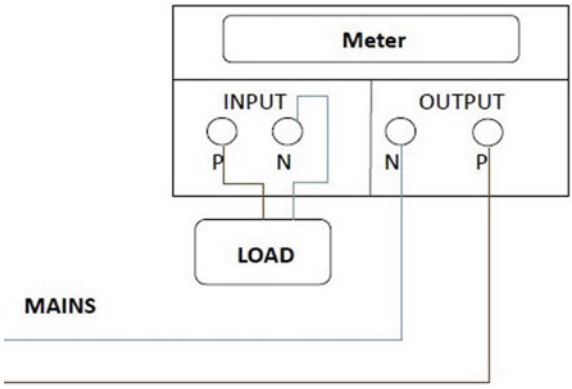

Fig. 8 Current reversal

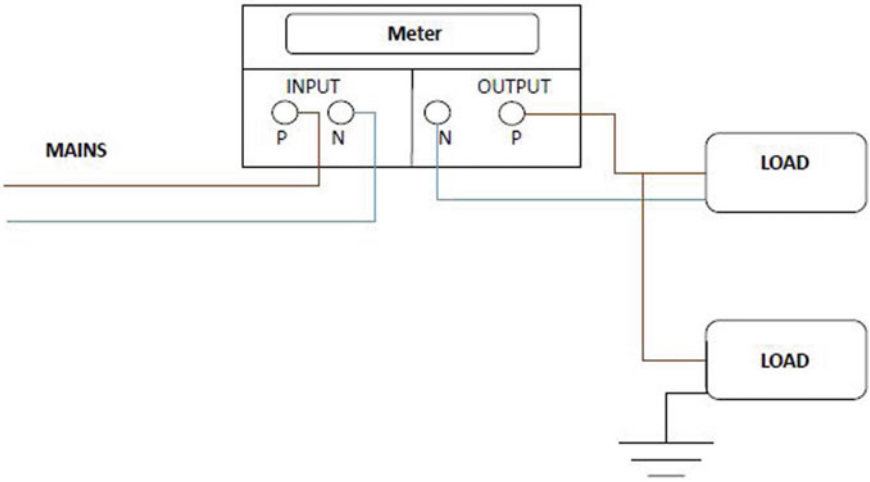

Fig. 9 Partial fault connection

neutral wire become less than the current in the phase wire. Under normal conditions, the current in the phase wire and the neutral wire is equal (Fig. 9).

2.7 Tampering Using High Frequency/Voltage

In this type of meter tampering a remote-controlled device is placed in close proximity to the meter. The device is capable of generating high-electrostatic discharge. The discharge so generated causes a spark in the meter thereby thwarting the meter from recording the electricity consumption. Such method of theft is a concern as it does not leave any trace or evidence.

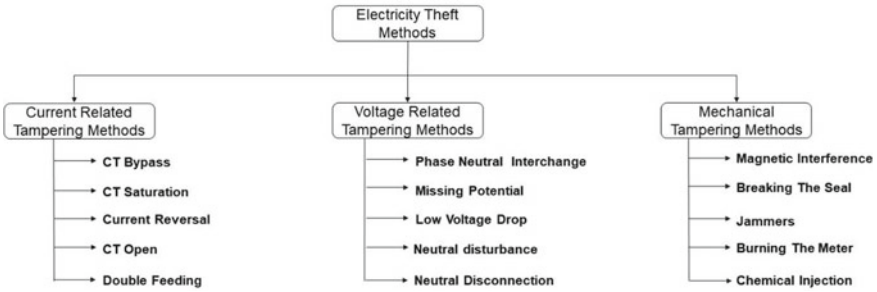

Fig. 10 Classification tree for energy theft methods

2.8 Mechanical Tampering

Mechanical tampering includes methods where the meter is physically damaged in order to record less or no energy usage. In such type of tampering the electrical characteristics of the components of the meter are altered. Some of the conducts that amount to such type of tampering are (Fig. 10)

- Opening of the meter covers by fracturing the meter seals.
- Subjecting meter body to chemicals.
- Subjecting meter to external magnetic field.
- Burning the meter.
- Using jammer devices.

3 Countermeasure Approaches Against Energy Theft

Along with the adoption of new technologies such as smart grid, a new era of attacks are expected to emerge. The government and the utilities are now becoming aware of these scenarios and are taking steps toward mitigating next generation of threats. Rapid developments in the AMI have captured the attention of research organizations and scholars from academia all around the sphere and a range of approaches have been proposed to curb the menace of electricity theft. In this section, we will provide a survey of the available approaches for energy theft detection.

3.1 Game Theory Based Detection Technique

In this technique, the stealing of electricity is represented as a play-off sandwiched amidst the adversaries involved in electricity thief and the distribution utility. It is a model projected on the concept of game theory where the main objective of the adversary is to whip a predetermined amount of electricity and at the same time

minimizing the possibility of being identified, whereas the electricity utility desires to augment the chance of detection of adversary and the level of operative price it will sustain in administering this anomaly recognition operation [7]. However, it still remains a challenge to construct a potential game plan and all players that include regulators, thieves, and distributors.

Moreover, game theory is based on assumption that the number of players participating in the game is finite. In country like India which is one of the largest in terms of population, equipping smart meter in every household simply means a drastic increase in number of players which makes game theory difficult to implement.

3.2 Supervised Learning Approach

In this approach load profiles for each customer is developed based upon the historical data which is used as a classifier dataset. A pre-selection is made on the subset of smart meters which are straightforwardly confirmed by the technicians within a specified region and time. This process is carried out by the utility company and is referred to as campaign [8]. Information such as consumption, profile, and external information along with other parameters is used to design the profile. In general, a classification problem of fraud identification is formulated which employs supervised learning approach over the historical dataset of fraud cases that occurred in the past [8]. The main criterion for evaluation is the (Odds Ratio) OR. OR may be computed between the falsified clients against all the clients not incorporated in any campaign, called as ORPG or between falsified clients and the non-falsified clients known as ORPN. The ratios obtained from the campaign are mentioned in Table 1 in [8] and are based on some of the characteristics obtained from the campaign. Based on probability a fraud score is computed for each customer according to which the customer can be classified as Fraudulent, Non-fraudulent, and Absent. However, this methodology has performance challenges in scenarios where rate of campaigns is excessively high or the size of campaigns is on a large scale.

3.3 Linear Error Correction Block Codes

Linear error-correcting block codes have a linear dependency between the bits of input message and the parity bits. In other words, the resultant of sum of any two codewords is also a codeword. At the receiving end, these bits are utilized to detect and correct errors in the transmission. A computation of the total amount of power in distinct combinations of the cables is computed repetitively and then these readings are utilized to detect and correct errors in the meter readings [6]. In this approach, the concept of syndrome decoding is applied where a generator matrix (G) is used by sender to generate the codeword and decoding matrix, also called parity check matrix (H) is used by the receiver to detect and correct the errors. If $G.H = 0$, then

the received codeword is correct. In case G.H $\neq$ 0, we can determine the error using the position of non zero bit and correct it. Additional meters, called check meters are used to detect and correct single-bit errors in meter readings. It is assumed that there are M check meters, which are capable of computing the sum of energies of desired cable combinations [6]. However, this Linear block code detection mechanism is prone to magnetic interference and can only detect that there is an error but could not identify the actual meter on which the error exists.

3.4 Dynamic Programming Algorithm Based on Probabilistic Detection

A novel algorithm based on dynamic programming which utilizes the tree structure of the distribution network has been proposed. It makes use of Feeder Remote Terminal Unit (FRTU), which is capable of measuring analog and digital signals and transmitting energy usage data back to the control unit wirelessly. The power consumption in the downstream network commencing from FRTU can be tracked down by means of the information gathered from FRTU. If the power consumption varies notably compared to the aggregate of the readings of smart meters in the downstream network than it is concluded that at least one of the meters has been compromised [9]. The algorithm aims to install FRTUs in minimal quantity in power distribution networks due to cybersecurity concerns. Moreover the algorithm is optimized to increase efficiency by utilizing solution pruning techniques. The main parameters that the algorithm uses to determine theft are the Attacking Probability and the Anomaly Score which are defined in [9]. Based on the anomaly score it is decided whether a meter is anomalous or not. The proposed algorithm works under the supposition that the adversary can only attack the smart meter equipped in her/his own apartment. It may not provide a fruitful solution in situations where adversary uses advanced techniques such as remotely attacking meter in Neighborhood Area Network (NAN). Another probabilistic approach has been proposed in [10] which provides an estimate of Technical and Non-Technical Losses in a segregated manner.

3.5 Temperature-Dependent Predictive Model

"Temperature-Dependent Technical Loss Model (TDTLM)" is the advancement of the "Constant Resistance Technical Loss Model (CRTLM)" [11] by making the resistance temperature dependent. To estimate NTL, TDTLM utilizes the property that there is a linear dependency between the resistance of material and its temperature in. The power consumption values along with other instantaneous measurements are aggregated and sent back to the utility repeatedly after a fixed interval of 30 min for calculation of NTL. Based on the threshold value of NTL cases are classified as theft

and non-theft. To train the predictive model data from the first two days (no theft) is utilized. Whenever NTL estimate exceeds the threshold value, it is suspected that a power theft has occurred in the user group.

3.6 Current Bypass Anti-Tampering Algorithm

A single-chip solution has been developed where an anti-tampering algorithm has been implemented on an "ARM Coretext-M3 (STM32L152VB)" microcontroller. It is a low power microcontroller operating at 32 MHz using "ADE7953 (Single Phase Smart Meter)" and "ADE7878 (Three Phase Smart Meter)" Analog Devices [12]. The unbalance current difference (Irr) is calculated by extracting data values from IRMSA (I_a) and IRMSB (I_b) registers of ADE7953, where current in phase line is denoted as I_a and current in neutral line is denoted as I_b. The unbalance current difference (Irr) is expressed in Eq. (1) of [12] as

$$|\text{Irr}| = I_a - I_b \div (I_a + I_b) \tag{8}$$

Verification of current bypass tampering event by the smart meter is done by comparing the calculated Irr value in (4) against the pre-defined threshold values which are 2.5% in case of three-phase meter and 1% in case of single-phase meter [12]. In case of any uneven event, an interrupt is sent to the MCU. The MCU verifies the tampering event by examining the status bits in the registers of ADE7953 and ADE7878.

3.7 Microprocessor-Based Theft Control System

The theft control system based on "ARM-Cortex M3 processor" has been implemented to prevent the energy meter from tampering attacks such as disconnections of phase/neutral lines, entire meter bypassing, and meter tampering. This approach utilizes the current difference in phase line and neutral line to detect tampering event. Two current transformers, one in each phase line and neutral line are inducted. In case of any disconnection of either of the lines from the meter, it would result in a significant drop in current measured by the each current transformer [13]. This difference is computed by the microcontroller by measuring current through ADC. In case of any irregular difference an SMS is sent to the electricity utility by the microcontroller. This functionality can be integrated into existing meters in addition to manufacturing it in new meters. The module uses GSM network for communication which is already well established in India.

3.8 AMIDS Framework

Advanced Metering Infrastructure Intrusion Detection System (AMIDS) is a framework developed using an amalgamation of a variety of approaches for detection and reporting of energy theft in smart meters. An attack graph-based data fusion algorithm is used by AMIDS to merge artefacts of on-going attacks from numerous sources [14]. The attack graph so composed is a directed graph based on state which consists of different stages from initial to final. To achieve information fusion online, the attack graph is considered as a Hidden Markov Model (HMM). AMIDS makes use of both a supervised learning methodology that can compute individual application usage and an unsupervised methodology that learns by clustering load events. AMIDS takes into account numerous information sources to collect adequate amount of artefacts regarding an on-going attack prior to identifying an activity as a malicious energy theft.

3.9 Model Based on Harmonic Generators

A model has been proposed in [15] which uses harmonic sensors to determine the uncertainty in smart meter readings. The proposed model consists of harmonic sensor, ICS, energy meter, circuit breaker, and communication system. The External Control Station (ECS) situated at the utility company receives instant values from end user side. The non-technical loss is calculated by ECS and in case of loss being more than 5% it would break the supply to the meter by indicating the control system to disconnect the customer. The core of the model is the harmonic sensor which compute the uncertainty in meter reading based on Total Harmonic Distortion (THD). In [16] this approach based on the harmonic generators is extended by placing two smart meters along with harmonic sensors and generators at either ends. One meter is placed at the consumer end and other one at the utility end which makes it possible to keep track of the generated power as well as the consumed power.

The difference in generated and consumed power is calculated to determine the theft.

3.10 MIDAS Framework

A novel framework MIDAS [17] is developed which is the integration of several techniques such as statistical analysis, data mining, and neural network. This framework is different from other approaches as it classifies not only suspected users but also classifies users without technical losses. Data mining is performed for fault and theft sensing and to analyze load profiles of individual customers. The neural network is trained with multiple methods. Different neural network topologies are developed

and at end of training the Root Mean Square (RMS) value for each model is computed. The model with minimum RMS value is presented as final neural network.

3.11 Measuring Voltage Drop Between Smart Meters

This approach utilizes the magnitude of the voltage drop between two smart meters to detect and decrease illegal consumption. The concept is to grab the voltage and power data from the meter. It functions on pre-condition that there should be more than two consumers involved in the powering of transformer, because detection of unauthorized spending is computed by comparing the drop of voltage of each measuring point to the transformer. In case if a drop of voltage occurs than it is deduced that the consumer is having unauthorized connection to the meter [18].

3.12 Energy Lens

Energy Lens system intelligently integrates electricity meter data with sensors on smartphones. It is expected that users using energy lens possess an android phone with the capability to sample microphone audio and WiFi signal strength. During initial phase users are required to turn on electricity appliances which they want to get recognized by the energy lens. Users wait for some time for its power consumption to reach a steady state and then turn it off. Based on this data acquired, it is identified that when, where, and by whom the activity is performed upon the execution of algorithm on the server [19]. However, energy lens faces several challenges such as acquisition of ground truth statistics for building up the precision, the effect of phone's direction and privacy of the customer.

3.13 FNFD ("Fast NTL Fraud Detrection and Verification")

FNFD is a mathematical method constructed on the notion of Recursive Least Square (RLS) to represent adversary behavior. Using FNFD the NTL fraud, in Smart Grid is detected in real time. FNFD is capable of verifying a fraud even with one single measurement, given that the historical data supplied to it is accurate [20]. FNFD employs linear functions to simulate the behavior of adversary. The main advantage of FNFD as compared to other schemes is that it requires much less data and supports NTL fraud verification, a unique feature that is not available in other schemes and it is much faster than the other similar frameworks.

4 Proposed Work

All the existing works available on energy theft detection in smart meters are dealing only with types of thefts where by some means either phase or neutral wires were swapped or removed which led to significant change in the voltage or current values or due to billing irregularities. Our work extends the existing approaches to a new threat scenario where theft detection in smart meter occurs due to tampering of the hardware chip of the meter itself. Our approach is mainly concerned with the chip-level tampering of smart meters. An adversary could Reverse engineer the meter and obtain the low-level assembly instructions of the meter. Further disassembling of the smart meter could be done, thereby attempting to read the firmware directly from the chip. Obtaining of the low-level assembly instructions would reveal the hard-coded cryptographic keys among other sensitive information that can be used in later attacks. Moreover, by exploiting the low-level assembly code the adversary could alter the consumption readings. The common methods of exploiting the hardware chip include:

- Logical Analyzer.
- Circuit Bending.
- JTAG Method.
- Hacking Over UART.

The logical analyzer is an instrument which sniffs the signals when placed on different test points on the circuit board thereby revealing potential information that could be interpreted into something useful, adding or removing circuit components such that the functionality of the circuit is affected, also known as Circuit Bending and using Joint Test Action Group (JTAG) method to read full memory hex dump.

We will begin with exploring the embedded hardware of the smart meter, examining individual components present on the circuit board. To get a better understanding of the working of each component we will probe the datasheets associated with each component. Extending our approach further we will examine the interconnections between different components using multi-meter. This will provide us insight of how data and signal transmission is taking place on the device. Now we will hunt for debug ports present on the device. JTAG and UART are the most common debug ports and we can easily identify them by monitoring the voltage levels using a multi-meter or with the help of oscilloscope. Once debug ports are identified we will start interacting with the device by making connections between the debug ports and any USB bridge. USB Bridge will provide us with the capability to interact with the device through console and finally we will begin the process of extracting data\firmware from the device. We will modify the data dump that we acquired and rewrite it to the device such that we can manipulate the device.

In continuation to this paper, we will be showcasing this kind of meter tampering using these mentioned method along with the experimental results. We will also propose mitigation measures for such type of chip-level energy theft approach such as assembly code obfuscation.

5 Conclusion

Curbing the energy theft menace is a huge concern for the governments and utilities. The scope of tampering comprises straightforward approaches like controlling live or neutral wires to more grave means like retrieving device firmware. Appliances like smart meters are part of critical infrastructure and any compromise to it would be causing chaos in the power sector and huge loss of revenue to the government. Most of the critical infrastructure devices are procured from global sources and may come pre-installed with hardware backdoors. Adversary can also intrude through the weakest point in the supply chain and compromise the device by installing hardware backdoor. This shows that attackers are now moving down the stack from application layer attacks to embedded hardware of the devices. The tools required to carry out physical attacks are also proliferating and becoming inexpensive. Such scenarios call for importance to hardware-level security which is not usually considered as important as application-level security. Organizations need to reshape their security approach from the viewpoint of attackers and conduct red team assessments to enhance the security of the assets. In recent years, the advancement of smart grid and adoption of smart meters has called for proposals from industry, universities, and governments to tackle the vulnerabilities existing in the AMI. In this paper, we have classified various ways of energy theft and detection techniques along with their challenges. However, it still remains a fresh topic and has a lot of room to be worked upon in the future.

References

1. Sharma T, Pandey KK, Punia DK, Rao J (2016) Of pilferers and poachers: Com-bating electricity theft in India. Energy Res Soc Sci 11:40–52
2. U.S. Energy Information Administration—Eia—Independent Statistics and Analysis. https://www.eia.gov/todayinenergy/detail.php?id=23452
3. Aggregate Technical & Commercial (AT&C) Losses in power sector. saumitra.cea@nic.in. https://data.gov.in/catalog/aggregate-technical-commercial-atc-losses-power-sector. Accessed Dec 17
4. Securing the smart grid of tomorrow. https://segrid.eu/
5. Warudkar D, Chandel P, Salwe BA (2014) Anti-tamper features in energy meters. Int J Electr, Electron Data Commun 2(5), May-2014. ISSN 2320-2084
6. Mesbah W (2016). Detection and correction of tampering attempts of smart electricity meters. In: PES innovative smart grid technologies conference Europe (ISGT-Europe), October, pp 1–6. IEEE
7. Cárdenas AA, Amin S, Schwartz G, Dong R, Sastry S (2012) A game theory model for electricity theft detection and privacy-aware control in AMI systems. In: Communication, control, and computing (Allerton), 2012 50th annual Allerton conference on, October, pp 1830–1837. IEEE
8. Coma-Puig B, Carmona J, Gavalda R, Alcoverro S, Martin V (2016) Fraud detection in energy consumption: a supervised approach. In: Data science and advanced analytics (DSAA), 2016 IEEE international conference on, October, pp 120–129. IEEE

9. Zhou Y, Chen X, Zomaya AY, Wang L, Hu S (2015) A dynamic programming algorithm for leveraging probabilistic detection of energy theft in smart home. IEEE Trans Emerg Topics Comput 3(4):502–513
10. Neto EAA, Coelho J (2013) Probabilistic methodology for technical and non-technical losses estimation in distribution system. Electric Power Syst Res 97:93–99
11. Sahoo S, Nikovski D, Muso T, Tsuru K (2015) Electricity theft detection using smart meter data. In Innovative smart grid technologies conference (ISGT), 2015 IEEE power & energy society, February, pp 1–5. IEEE
12. Tangsunantham N, Ngamchuen S, Nontaboot V, Thepphaeng S, Pirak C (2013) Experimental performance analysis of current bypass anti-tampering in smart energy meters. In: Telecommunication networks and applications conference (ATNAC), 2013 Australasian, November, pp 124–129. IEEE
13. Dineshkumar K, Ramanathan P, Ramasamy S (2015) Development of ARM processor based electricity theft control system using GSM network. In: Circuit, power and computing technologies (ICCPCT), 2015 international conference on, March, pp 1–6. IEEE
14. McLaughlin S, Holbert B, Zonouz S, Berthier R (2012) AMIDS: a multi-sensor energy theft detection framework for advanced metering infrastructures. In: Smart grid communications (SmartGridComm), 2012 IEEE third international conference on, November, pp 354–359. IEEE
15. Depuru SSSR, Wang L, Devabhaktuni V (2011) Electricity theft: overview, issues, prevention and a smart meter based approach to control theft. Energy Policy 39(2):1007–1015
16. Prasad J, Samikannu R (2017) Overview, issues and prevention of energy theft in smart grids and virtual power plants in Indian context. Energy Policy 110:365–374
17. Guerrero JI, Monedero Í, Biscarri F, Biscarri J, Millán R, León C (2014) Detection of non-technical losses: the project MIDAS. Advances in secure computing, Internet services, and applications, pp 140–164
18. Bula I, Hoxha V, Shala M, Hajrizi E (2016) Minimizing non-technical losses with point-to-point measurement of voltage drop between "SMART" meters. IFAC-PapersOnLine 49(29):206–211
19. Saha M, Thakur S, Singh A, Agarwal Y (2014) EnergyLens: combining smartphones with electricity meter for accurate activity detection and user annotation. In: Proceedings of the 5th international conference on Future energy systems, June, pp 289–300. ACM
20. Han W, Xiao Y (2016) FNFD: a fast scheme to detect and verify non-technical loss fraud in smart grid. In: Proceedings of the 2016 ACM international on workshop on traffic measurements for cybersecurity, May, pp 24–34. ACM