Algorithms for Intelligent Systems
Series Editors: Jagdish Chand Bansal · Kusum Deep · Atulya K. Nagar

Mohammad Shorif Uddin
Avdhesh Sharma
Kusum Lata Agarwal
Mukesh Saraswat *Editors*

Intelligent Energy Management Technologies

ICAEM 2019

Springer

Algorithms for Intelligent Systems

This book series publishes research on the analysis and development of algorithms for intelligent systems with their applications to various real world problems. It covers research related to autonomous agents, multi-agent systems, behavioral modeling, reinforcement learning, game theory, mechanism design, machine learning, meta-heuristic search, optimization, planning and scheduling, artificial neural networks, evolutionary computation, swarm intelligence and other algorithms for intelligent systems.

The book series includes recent advancements, modification and applications of the artificial neural networks, evolutionary computation, swarm intelligence, artificial immune systems, fuzzy system, autonomous and multi agent systems, machine learning and other intelligent systems related areas. The material will be beneficial for the graduate students, post-graduate students as well as the researchers who want a broader view of advances in algorithms for intelligent systems. The contents will also be useful to the researchers from other fields who have no knowledge of the power of intelligent systems, e.g. the researchers in the field of bioinformatics, biochemists, mechanical and chemical engineers, economists, musicians and medical practitioners.

The series publishes monographs, edited volumes, advanced textbooks and selected proceedings.

More information about this series at http://www.springer.com/series/16171

Mohammad Shorif Uddin · Avdhesh Sharma ·
Kusum Lata Agarwal · Mukesh Saraswat
Editors

Intelligent Energy Management Technologies

ICAEM 2019

Springer

Editors
Mohammad Shorif Uddin
Department of Computer Science and Engineering
Jahangirnagar University
Dhaka, Bangladesh

Kusum Lata Agarwal
Department of Electrical Engineering
Jodhpur Institute of Engineering and Technology
Jodhpur, India

Avdhesh Sharma
Department of Electrical Engineering
MBM Engineering College
Jodhpur, India

Mukesh Saraswat
Jaypee Institute of Information Technology
Noida, India

ISSN 2524-7565 ISSN 2524-7573 (electronic)
Algorithms for Intelligent Systems
ISBN 978-981-15-8819-8 ISBN 978-981-15-8820-4 (eBook)
https://doi.org/10.1007/978-981-15-8820-4

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Preface

Twenty-first century is the transition from fossil-fuel-based energy to renewable energy, and after Montreal and Kyoto Protocol, the world is inclined toward renewable energy sources. Intelligent energy management technologies are now appearing very cost-effective compared to the projected high cost of fossil fuels. In this context, numerous intelligent control schemes are proposed for developing smart energy management systems. With this background, the idea of the International Conference on Advances in Energy Management System (ICAEM 2019) is conceived to develop a platform for networking; disseminating; and exchanging challenges, ideas, concepts, and results among the researchers from academia and industry.

This book contains the good-quality research papers as the proceedings of this International Conference on Advances in Energy Management System (ICAEM 2019). ICAEM 2019 has been jointly organized by the Rajasthan Technical University (RTU), Kota, and Jodhpur Institute of Engineering and Technology (JIET), Jodhpur, Rajasthan, India. It was held on December 20–21, 2019 at JIET, Jodhpur, Rajasthan, India. The conference focused on the application of artificial intelligence, soft computing, optimization, machine learning, intelligent software, data science, data security, and big data analytics on advanced energy management systems.

We have tried our best to enrich the quality of the ICAEM 2019 through a stringent and careful peer-review process. ICAEM 2019 received 132 papers on four conference tracks. Among these 65 papers were selected through the peer-review process for presentation during the conference. However, the final proceedings contain only 38 papers after careful editorial reviewing.

The book presents the intelligent computing research results in reliable power systems, power quality, smart grids, energy management, conversion techniques, energy economics, etc. We believe that this book serves as a reference material for advanced research in the field of energy management.

Dhaka, Bangladesh	Mohammad Shorif Uddin
Jodhpur, India	Avdhesh Sharma
Jodhpur, India	Kusum Lata Agarwal
Noida, India	Mukesh Saraswat

Contents

About the Editors

Dr. Mohammad Shorif Uddin is a Professor of Computer Science and Engineering at Jahangirnagar University, Bangladesh. He completed his Bachelor of Science in Electrical and Electronic Engineering at BUET in 1991, Master of Technology Education at Shiga University, Japan, in 1999, Doctor of Engineering in Information Science at Kyoto Institute of Technology, Japan, in 2002, and an M.B.A. at Jahangirnagar University in 2013. He undertook postdoctoral researches at Bioinformatics Institute, Singapore, Toyota Technological Institute, Japan, Kyoto Institute of Technology, Japan, Chiba University, Japan, Bonn University, Germany, and Institute of Automation, Chinese Academy of Sciences, China. His research is motivated by applications in the fields of artificial intelligence, imaging informatics, and computer vision. He is the Editor-in-Chief of ULAB Journal of Science and Engineering and an Associate Editor of IEEE Access and has served as General Chair or Co-Chair of various conferences, including the IJCCI 2018 and 2019, EICT 2017, and IWCI 2016. He holds two patents for his scientific inventions, is a senior member of several academic and professional associations, and has published extensively in reputed international journals and conference proceedings.

Dr. Avdhesh Sharma is a Professor of Electrical Engineering at M.B.M. Engineering College, India. He completed his Ph.D. in Electrical Engineering at IIT, Delhi, M.Tech. in Computer Science & Data Processing at IIT, Kharagpur, M.Sc. at AMU, and B.Sc. in Electrical Engineering at D.E.I. Engineering College, India. He has over 33+ years of experience in teaching and research. He has published around 75 papers in international journal and conference proceedings. He guided a good number of PG and Ph.D. students. He is a Fellow of the Institute of Engineers, India.

Dr. Kusum Lata Agarwal is a Professor and Head of Electrical Engineering at JIET, Jodhpur, India. She completed her Ph.D., M.E., and B.E. degrees at M.B.M. Engineering College, India. She has over 18 years of experience in teaching and research. She published around 30 papers in journal and conference proceedings.

She supervised a good number of PG theses. She played a key role in organizing 4 national and international conferences and also achieved notable research grants. She is in the reviewer panel of many journals and conferences.

Dr. Mukesh Saraswat is an Associate Professor of Computer Science & Engineering at Jaypee Institute of Information Technology, India. He completed his B.Tech. in CSE at MJP Rohilkhand University, M.Tech. in CSE at UPTU, and Ph.D. in CSE at IIITM, Gwalior, India. He has more than 15 years of teaching and research experience. He has guided more than 72 UG & PG theses and presently guiding 4 Ph.D. students. He is a member of several academic and professional bodies and has published more than 35 papers in journals and conference proceedings in the area of imaging, pattern recognition, and soft computing.

Chapter 1
Solar PV-Based Electric Vehicle Charging System with Power Backup

Utkarsh Gupta, D. K. Yadav, and Dheeraj Panchauli

1 Introduction

With the rapid increase in technologies and popularity of EV, a need develops for the improved charging infrastructure for their successful propulsion [1].

The charging could basically be powered by electricity generated from either conventional or non-conventional source of energy. But to make the concept of EVs completely environment-friendly a charging station powered by a renewable source of energy is considered to be the best [2].

Out of many types of renewable sources present on earth like tidal, geothermal, solar, wind energy, etc., the use of solar PV array for the EV charging station is preferred the most due to its easy availability, ease of installation, and less maintenance due to the absence of moving parts [3, 4].

The solar-powered charging system with power backup provides various advantages to the infrastructure where it is installed as it provides free fuel for the EVs throughout its lifetime, 20–25 years approximately, after a single investment and also eliminates the need of the power backup sources like diesel generator, inverters, etc. as it can supply the load by the EV batteries under emergency conditions [5].

U. Gupta (✉) · D. K. Yadav · D. Panchauli
Rajasthan Technical University, Kota 324010, India
e-mail: Utkarshgupta3095@gmail.com

D. K. Yadav
e-mail: dkyadav@rtu.ac.in

D. Panchauli
e-mail: dheerajpanchauli777@gmail.com

M. Shorif Uddin et al. (eds.), *Intelligent Energy Management Technologies*,
Algorithms for Intelligent Systems,
https://doi.org/10.1007/978-981-15-8820-4_1

2 System Description

See Fig. 1.

2.1 PV Array

A solar PV array of 1 Soltech 1 STH-215-P is used with 10 series modules and 40 parallel strings. The PV and IV characteristics of the PV array are as follows (Figs. 2).

Characteristics of PV array
See Fig. 3.

2.2 Boost Converter

A boost converter is a DC–DC converter that steps up voltage (while stepping down the current) from its input to output. It is a category of SMPS (switch mode power supply) containing at least two semiconductors (a diode and a transistor) and at least one energy storage element, a capacitor, an inductor, or two in combination (Fig. 4).

2.3 Single-Phase Full Bridge Inverter for R-L Load Inverter

A single-phase square wave type voltage source inverter produces square-shaped output voltage for a single-phase load. Such inverters have very simple control logic and the power switches need to operate at much lower frequencies compared to switches in some other types of inverters (Fig. 5).

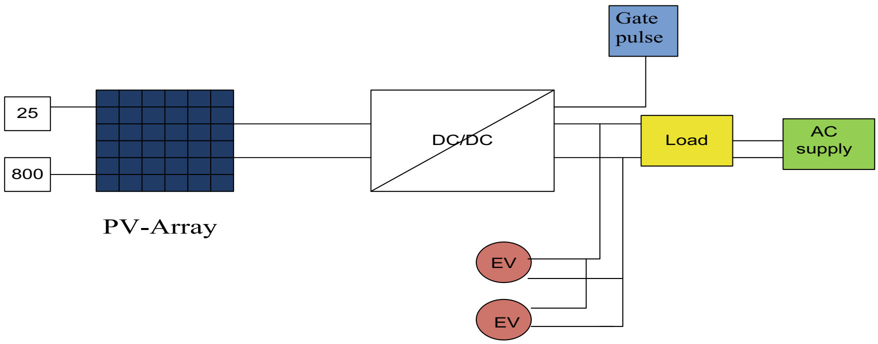


Fig.1 Block diagram of the system

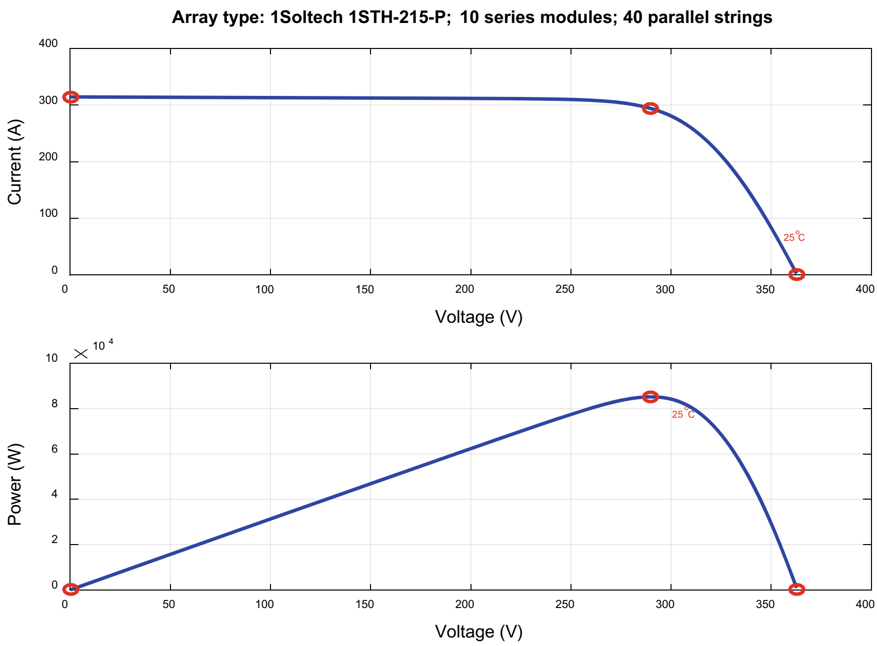


Fig. 2 The PV and IV characteristics of the PV array are as follows

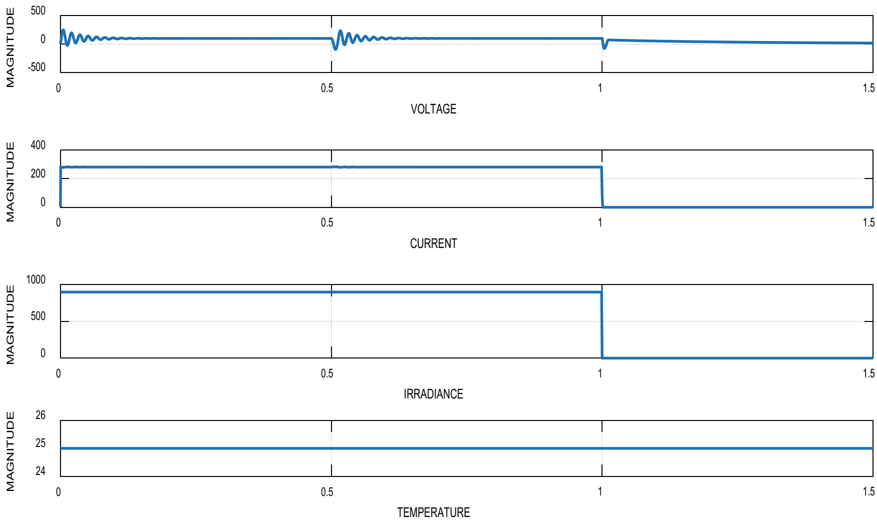


Fig. 3 The output waveform of the PV array used in this system

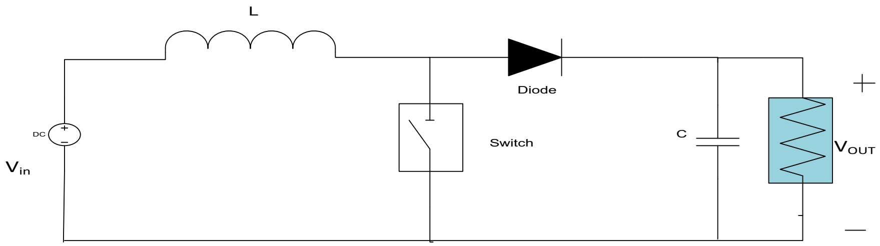


Fig. 4 Basic diagram of a boost converter

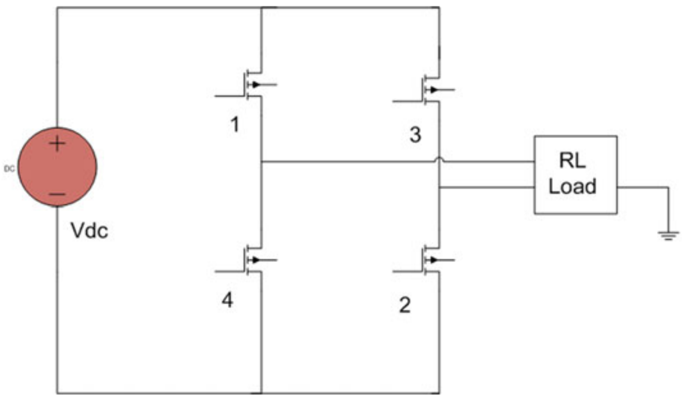


Fig. 5 Basic diagram of a single-phase inverter

2.4 Single-Phase AC Supply

A supply of peak voltage of 180 V and frequency of 50 Hz is used to supply the load under normal conditions.

2.5 Load

A resistive load of 5000 ohms is taken in this system.

3 Working of the System

The working of this system is explained basically in three modes.

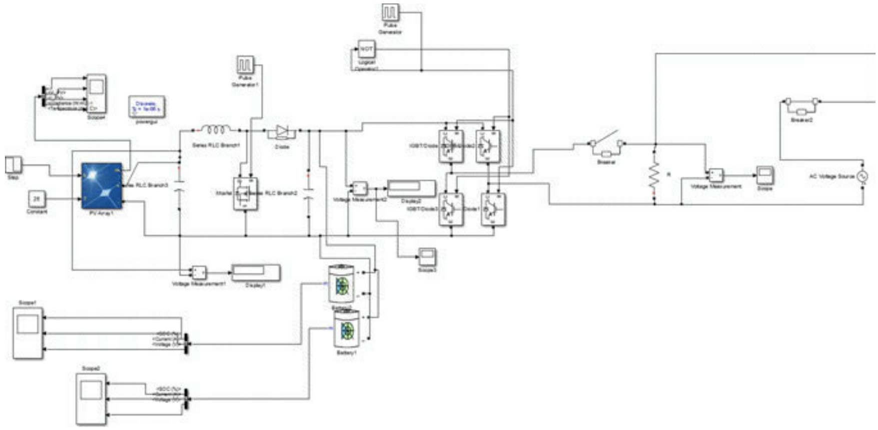


Fig. 6 Simulation model of the system in Matlab

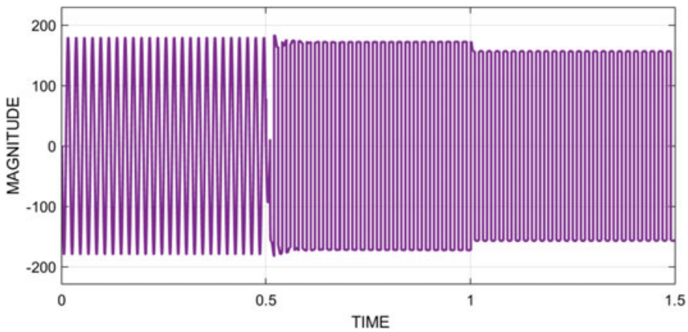


Fig. 7 Output waveforms across the load

MODE-I In this mode, both the grid and the SPV are ON where the grid supplies the load and the SPV charges the batteries of electric vehicles.

MODE-II In this mode, the grid is absent and the SPV maintains the supply across the load through a single-phase inverter and also charges the batteries of the EVs.

MODE-III In this mode, both the PV and the grid are absent and the batteries of the EVs supply the load and their discharging could be seen (Figs. 6, 7 and 8).

4 Simulation Model and Results

In Mode 1, i.e., from a time period of 0–0.5, the output waveforms across the load show sinusoidal waveforms as in this period of time the load is supplied by the grid

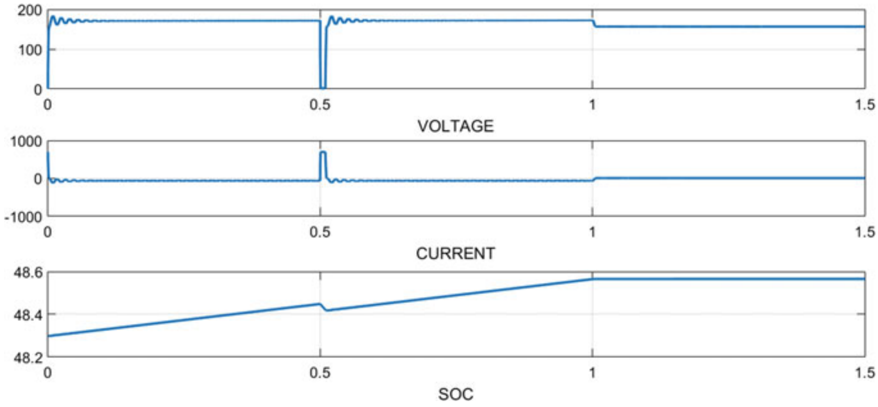


Fig.8 Output waveforms across the battery

and the output waveforms across the battery show an increasing value of SOC as it is getting charged by the solar PV array at this time.

In Mode 2, i.e., from time period of 0.5–1, the output waveforms across the load can be seen as a square wave as it is supplied by the solar PV inverter via a single-phase inverter in the absence of grid and the output waveforms across the battery show the increasing SOC as it is getting charged by the solar PV array.

In Mode 3, i.e., from time period of 1–1.5, the output waveforms across the load show the square wave of 144 V approximately which is supplied by the battery via a single-phase inverter due to the absence of both the sources (solar and grid) and discharging of the batteries can be seen in the output waveforms across the battery.

5 Conclusion

The charging station developed in this system proves to be a very economical system as with eliminating the requirements of expensive power backup sources. It also provides free fuel to the EVs throughout its life. The system could be further expanded and could be made more useful by applying some control techniques.

References

1. Suman N, Yadav DK, Jangid T (2018) Modeling and analysis of photovoltaic system with improved inverter technique. In: 2018 9th international conference on computing, communication and networking technologies (ICCCNT). https://doi.org/10.1109/icccnt.2018.8494168
2. Koduri N, Kumar S, Uday kumar RY (2014) On-board vehicle-to-Grid (V2G) integrator for power transaction in the smart grid environment. In: 2014 IEEE international conference on computational intelligence and computing research. https://doi.org/10.1109/iccic.2014.7238404

3. Chen J, Zhang Y, Su W (2015) An anonymous authentication scheme for plug-in electric vehicles joining to charging/discharging station in vehicle-to-Grid (V2G) networks. China Commun 12(3):9–19. https://doi.org/10.1109/cc.2015.7084359
4. Yang P, PengT, Wang H, Han H, Yang J, Wang H (2017) A single-phase current-source bidirectional converter for V2G application. In: 2017 IEEE 3rd international future energy electronics conference and ECCE Asia (IFEEC 2017 - ECCE Asia). https://doi.org/10.1109/ifeec.2017.7992125
5. Li Y, Yu G, Liu J, Deng F (2017) Design of V2G auxiliary service system based on 5G technology. In: 2017 IEEE conference on energy internet and energy system integration (EI2). https://doi.org/10.1109/ei2.2017.8245513
6. Han H, Lv Z, Huang D, Li Q (2017) Research on charge and discharge power tracking control for V2G system. In: 2017 IEEE 2nd information technology, networking, electronic and automation control conference (ITNEC). https://doi.org/10.1109/itnec.2017.8284928

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).

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

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

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

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

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

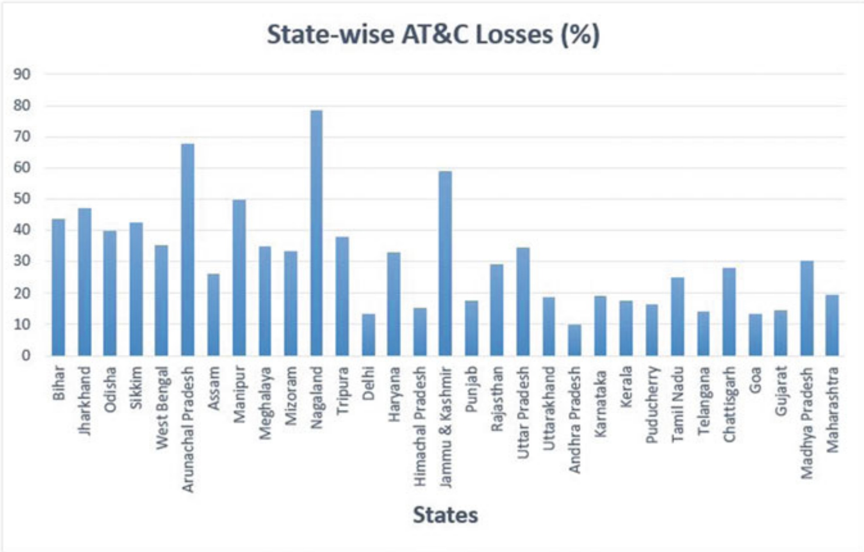


Fig. 1 A visual representation of state-wise AT&C losses (%) for the period Apr'14–Mar'15, According to catalog available on Open Government Data Platform (OGD), India [3]

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.

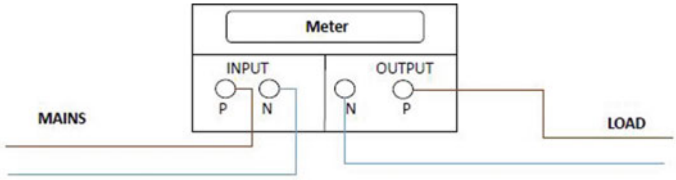


Fig. 2 Actual connection

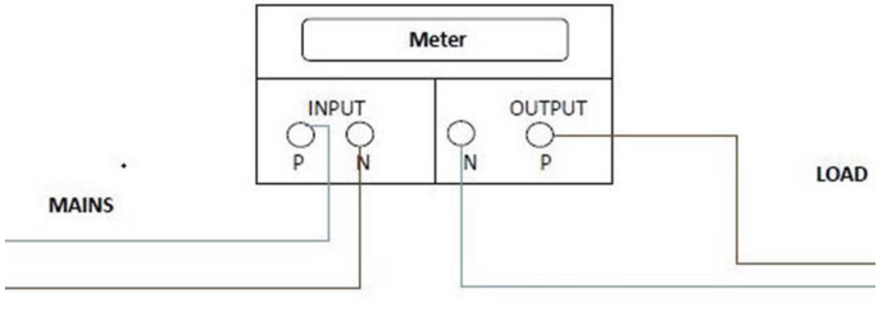


Fig. 3 Swapping of phase and neutral lines

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).

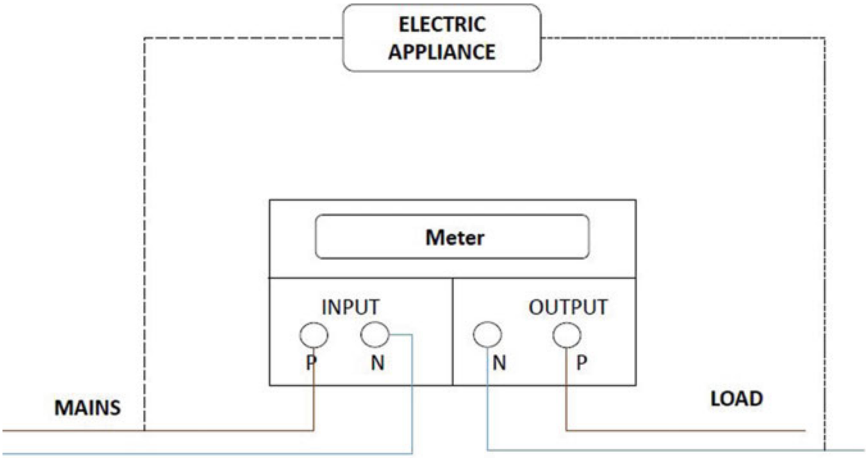


Fig. 4 Double feeding

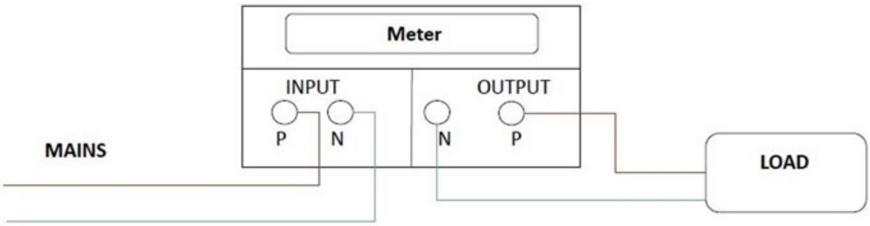


Fig. 5 Actual condition

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).

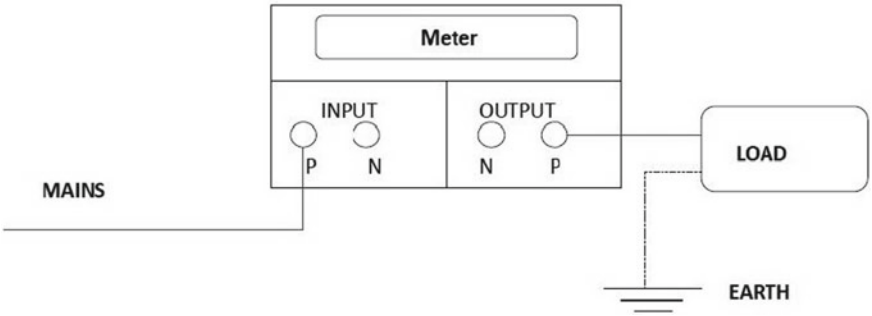


Fig. 6 Neutral missing

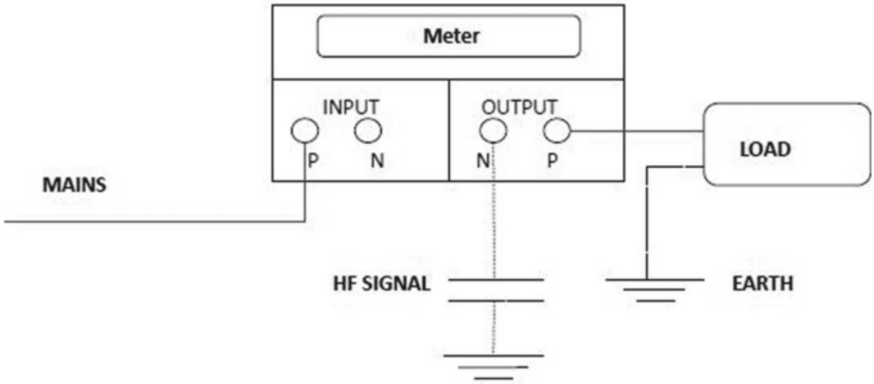


Fig. 7 Neutral disturbance

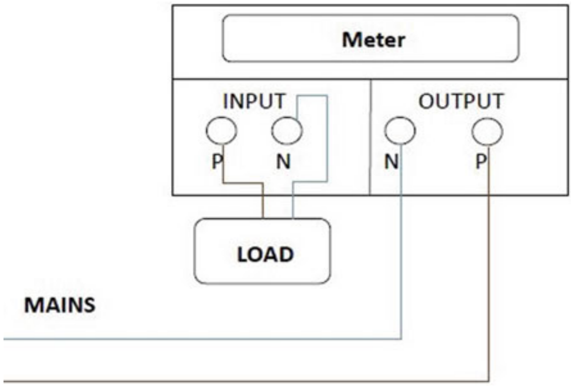
2.5 Current Reversal by Connecting Input and Output in Reverse

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



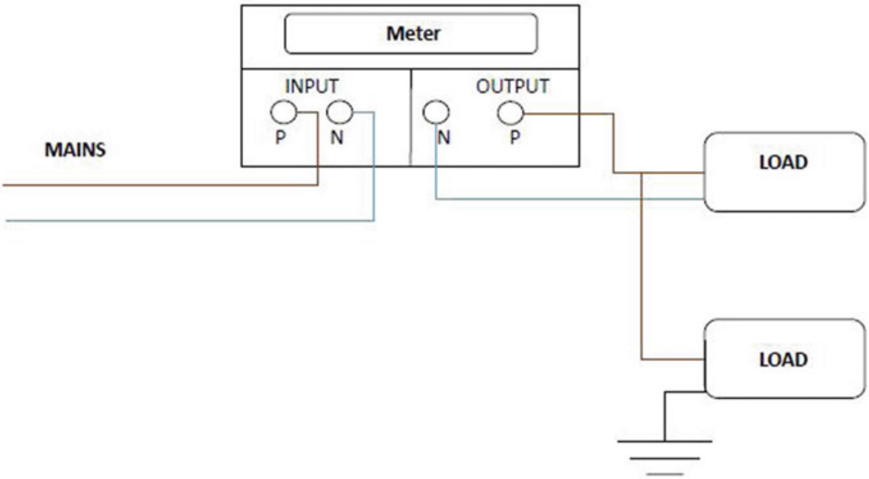


Fig. 9 Partial fault connection

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.

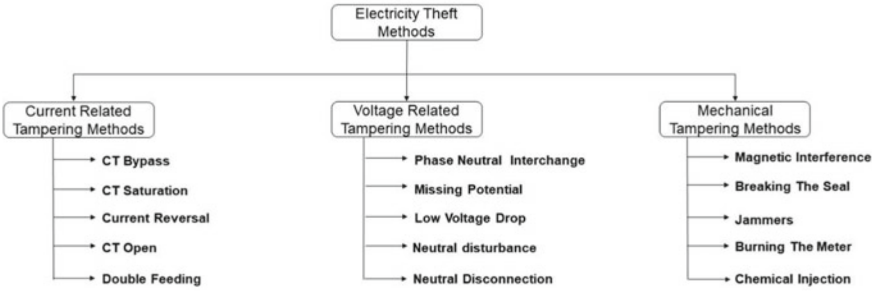


Fig. 10 Classification tree for energy theft methods

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

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

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.