

# Energy Theft Identification in Smart Grid

K. Govinda, Rishav Shav and Surya Prakash

**Abstract** Smart grid is a new generation of electrical grid communication with high management of power flow control, self-healing, energy efficiency, and security through the digital communication networks and technologies. To develop a smart grid from the existing power grid, we need to integrate ICT infrastructures with grid and management of grid has to be automated in the smart way, this requires sensing technologies, distributed communication, and pervasive computing frameworks to make the smart grid more efficient and secure. Theft identifying is one of the major issues faced by many service providers and this makes huge loss to the power management and the provider. This paper proposes a secure power management and theft identification in the smart grid.

**Keywords** Smart grid · Power theft · Infrastructure · Smart household meter  
Smart line meter

## 1 Introduction

Smart grid is the future power grid with the integration of electrical power grid and ICT which is developing all over world, it is a fully sustainable form of reliable and green electrical energy in existing network with advanced technologies and communication devices to manage the system in both sides [1]. These advanced methodology and frameworks provide a great flexibility and management, this also possesses a new class of risk [2]. Smart grid is one of the most critical infras-

---

K. Govinda (✉) · R. Shav  
SCSE, VIT University, Vellore, India  
e-mail: kgovinda@vit.ac.in

R. Shav  
e-mail: rishav2105@gmail.com

S. Prakash  
SITE, VIT University, Vellore, India  
e-mail: suryaprakash498@gmail.com

structures that are augmented by the large-scale ICT and renewable energy integration [3], even with all the crises, smart grid is the best infrastructure to handle a large set of management system that is distributed in the network. To provide grid monitoring and control capabilities, numerous power applications are necessary to exist [4]. Every year, the utility provider company fares their power theft from 20 to 30% and to that power, ministry loss is more than Rs. 125 billion [7], at this stage, service providers took several steps to manage the distribution system, but this is not enough to handle the power theft. This paper proposes a new model to handle power losses in distribution system.

## 2 Literature Review

In [1], the author has proposed a security framework using location-based security for protecting the SG infrastructure which is designed based on the algebraic code based cryptosystems, they chose it for smart grids to create location-based security applications.

In [2], the authors have done a study on threads on smart grid and solved it through system engineering and fault management concepts and expanded the range potential, range behaviors, and outcomes in the grid technologies with fault tolerance.

In [3], the authors have investigated challenges and security issues in smart grid, some important issues include privacy issue, identity spoofing, and so on and challenges such as mobility, scalability, deployment, and so on.

In [4], the author has discussed about the cyber security threats in smart grid and focused particularly on government grid infrastructures threats and measures to control and monitor the systems from cyber attacks for smart grid environments.

In [5], the author has done a survey on smart grid cyber security communications which elaborates the threats and vulnerabilities, solution proposed to these problems and relies on the system to make smart grid communication secured.

In [7], the authors have proposed a power theft monitoring system using GSM module and integrated the part used for the project and discussed about it briefly; the components used to implement for the projects such as sensors, circuits, etc., are discussed.

## 3 Proposed Method

Smart grid technologies are the future power grid that functions with the renewable energy, sensors, and smart meters to provide an efficient power usage and performance management [6, 8, 9]. Energy power resource has the highest priority in every field and thus it makes it as a huge resource and we provide a framework to manage it and identify the theft in the field of line as shown in Fig. 1.

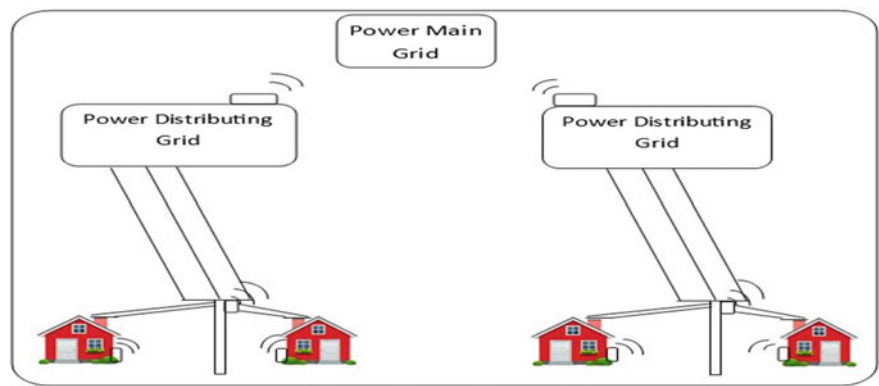


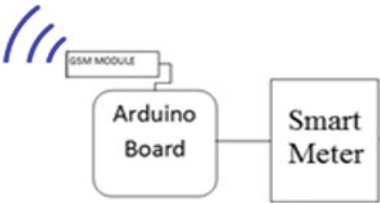
Fig. 1 System architecture

3.1 Smart House Holds Meters (SHHM)

This meter has the GSM module which has unique ID given for the customer and unique GSM number also, which is attached with Arduino board and the board is connected to the meter and communicates with sensors and sends signal from the house to the power distributing grid, the meter sends the power consumption level to power distributing grid in a particular interval of time (for example, every 1 h) and these values are stored in the server and to get processed, these values are indexed in the table on the customer id, every usage based on time is stored separately in another database table. In this way, we know how much power the customer consumes in a particular interval of time and monitor the power activity of customer Fig. 2.

Smart line meter which will be placed in the line post of the house where the connection coming from the line to house is through smart line meter and this meter communicates to the power distributing grid in the same interval of time as smart household meter[10, 11]. This SLM will consist of a number of sockets to get input from the line and output sockets to provide connection to the house, the line number denotes the customer connected to the concerned port which will be stored in the server (for example, 1 means the index will be stored), such that all the sockets readings will be communicated to the Arduino, Arduino will send signal to the GSM module and the power distributing grid will receive it and store it in database.

Fig. 2 Smart meter



### 3.2 Smart Line Meters (SLM)

Refer Fig. 3 for the basic structure of a Smart Line Meter.

### 3.3 Arduino

Arduino is a open source hardware and software architecture that is a microcontroller, it can control the smart devices connected to it such as sensors, GSM, Bluetooth, etc., this hardware is widely used all over the physical world and implements the hardware in an efficient way, it is of ATMEL 8-bit AVR microcontroller that is facilitated with complete components connected to its board [12]. Arduino is a preprogrammed device with boot loader that lets the user to upload the programs into the chip flash memory Fig. 4.

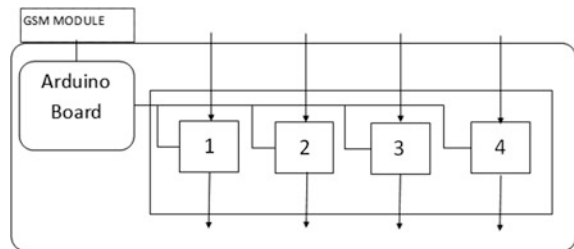
The Arduino board is connected to the digital smart meter and readings are sent to GSM module, this GSM signals the power distributing grid and processes the received signal based on the customer id and meter signal. These components work together as one device and manage the power grid and identify the power consumption at time intervals.

### 3.4 Power Distributing Grid

The power distributing grid which receives the signal from the SHHM and SLM stores the power values of the customers such that each power distributing grid support is providing the service to customer and the data from the smart household meters (SHHM) and smart line meters (SLM) are indexed in the server to process.

Here, the comparison is done between the received data of SHHM and SLM in which the line not equalized will be identified and forwarded to the admin where the line will be easily identified and theft can be prevented.

**Fig. 3** Smart line meter



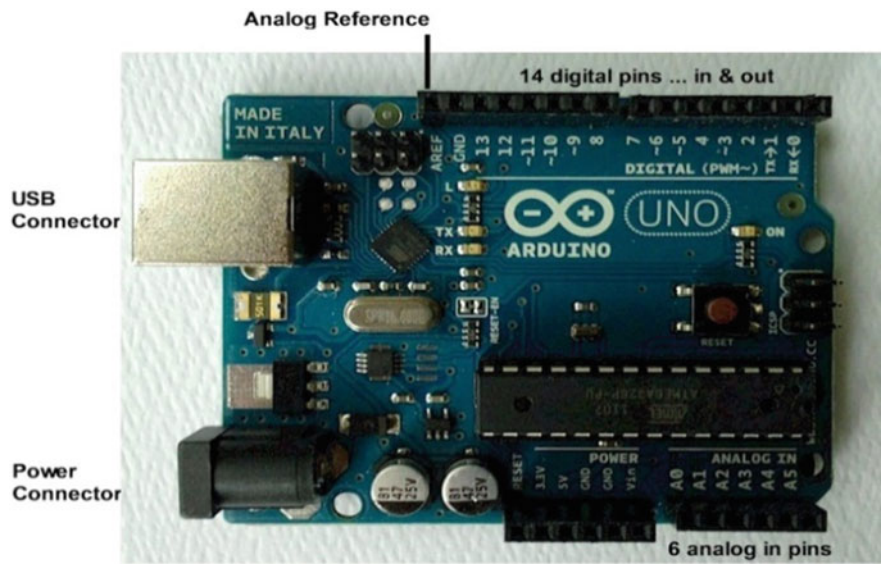


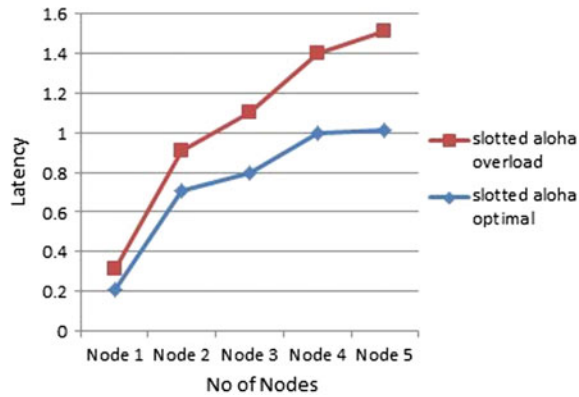
Fig. 4 Arduino board

The traveling of electricity loss is 2–5% of overall electricity and it is decreased in the comparison table. The loss indication of more than the 5% percentage will be denoted as theft status.

4 Results and Discussion

We have stimulated the GSM module in omnet++ by slotted aloha overload method and slotted aloha optimal method. While sending the packets to the server which is the local power distributing grid, the processing and sending time is calculated and derived in Fig. 5.

Fig. 5 Slotted aloha overload versus optimal



With the proposed model, power theft identification can be found imminently and can be stopped before the high loss of power. Here, the architecture gives the smart grid a flexible and scalable monitoring system and management system where all the processes are automated through the server and this reduces human power which is a benefit to the government.

## 5 Conclusion

The smart grid technologies are developing in many countries by establishing the infrastructure in their smart cities; smart grid power management system provides the information of all the connections in the networks and with technology, smart devices, sensors, and smart meter. Thus, managing the power grid in an efficient way and identifying the power theft imminently are the most important features of the architecture and the smart grid becomes more secure and managing the system will be flexible and scalable.

## References

1. Khan E, Adebisi B, Honary B (2013) Location based security for smart grid applications. The mediterranean green energy forum 2013, MGEF-13. Energy Procedia 42:299–307
2. Rice EB, AlMajali A (2014) Mitigating the risk of cyber attack on smart grid systems. In: Conference on systems engineering research (CSER 2014). Procedia Compute Sci 28: 575–582
3. Bekara C (2014) Security issues and challenges for the IoT-based smart grid. International workshop on communicating objects and machine to machine for mission critical applications (COMMCA-2104)
4. Ashok A, Hahn A, Govindarasu M (2014) Cyber-physical security of Wide-Area monitoring, protection and control in a smart grid environment. Dept Electr Comput Eng Iowa State Univ Ames IA USA J Adv Res 5:481–489
5. Yan Y, Qian Y, Sharif H, Tipper D (2012) A survey on cyber security for smart grid communications. IEEE Commun Surv Tutorals 14(4), Fourth quarter
6. Baig ZA, Amoudi A-R (Aug 2013) An analysis of smart grid attacks and countermeasures. J Commun 8(8)
7. Kalaivani R, Gowthami M, Savitha S, Karthick N, Mohanvel S (Feb 2014) GSM based electricity theft identification in distribution systems. Int J Eng Trends Technol (IJETT) 8(10)
8. Federal Energy Regulatory Commission (2013) Assessment of demand response and advanced metering staff report
9. Anderson R, Fuloria S (2010) Who controls the off switch? In: IEEE international conference on smart grid communications <https://doi.org/10.1109/SMARTGRID.2010.5622026>
10. Woody C (2013) Mission thread security analysis: a tool for systems engineers to characterize operational security behavior. INCOSE Insight 16(2):37–40

11. Liu Y, Ning P, Reiter MK (2009) False data injection attacks against state estimation in electric power grids. In: Proceedings of the 16th ACM conference on computer and communications security, CCS'09, ACM, New York, USA
12. Sridhar S, Manimaran G (2010) Data integrity attacks and their impacts on SCADA control system. In: Proceedings of power and energy society general meeting

Silicon Photonics & High Performance Computing

Proceedings of CSI 2015

Mishra, A.; Basu, A.; Tyagi, V. (Eds.)

2018, XIII, 138 p. 85 illus., 70 illus. in color., Softcover

ISBN: 978-981-10-7655-8