Energy Policy 110 (2017) 365–374

Contents lists available at ScienceDirect

Energy Policy

journal homepage: www.elsevier.com/locate/enpol

Overview, issues and prevention of energy theft in smart grids and virtual power plants in Indian context

Sampath Kumar V.[a,*,1], Jagdish Prasad[b], Ravi Samikannu[c]

[a] Amity Business School, Amity University Rajasthan, Jaipur, Rajasthan, India
[b] Amity School of Applied Sciences, Amity University Rajasthan, Amity Education Valley, Kant Kalwar, NH-11C, Jaipur-Delhi Highway, Jaipur, Rajasthan 303007, India
[c] Department of Electrical Engineering, Botswana International University of Science and Technology (BIUST), Private bag 16, Palaype, Botswana

ARTICLE INFO

Keywords:
Technical loss
Advance metering infrastructure
Attack tree
Vigilant energy metering systems
Electrocution

ABSTRACT

This paper is an excerpt and a comprehensive research on Non-Technical losses during T & D. In developing countries, the utility companies are finding it difficult to address losses due to theft, meter tampering and allied problems which affect the quality of supply, increase on generation load and has a significant economic impact on the functioning of the utility company and its genuine consumers in the form of an excessive tariff. As the single largest contributor to T & D losses, various aspects and methods used for theft and detection mechanisms are discussed. This article also highlights the components of AMI and how a simple method of two smart meters equipped with harmonic generators could be used in conjunction to detect theft.

1. Introduction

The socio-economic growth of a country lies in its ability to harness energy. But this is hampered by inadequate resources or supplies. However, this scenario is changing. Energy sector across the globe is changing fast at an unprecedented scale and pace. The need for this is due to the fact to mitigate climate change and reduce carbon print across the globe. The Governments are playing a vital role in encouraging private bidders and new technologies. Technologies like renewable energy system for generating electricity storage has far reaching socio-economic benefits. Transformations depend on deployment of Virtual power plants, smart grids using smart technology. However, these digitization strategies have both pros and cons. All these techniques, smart energy system is therefore created through the significantly greater use ICT digitization of power production and distribution. The increasing decentralization of the energy system which includes the consumer, who is also a prosumer across the energy value chain poses a greater threat to the energy sector as a whole (David et al., 2016).

Smart Grid is an advanced modernized holistic concept where a broad range of ICT resources is put to use to reduce electricity wastage and energy costs. Smart Grid facilitates efficient two-way delivery system which is reliable from end-to-end, intelligent from source to sink, smart transmission and distribution through the integration of renewable energies. The combined power of IT + Power (Smart Grid) enables real-time monitoring and control of power system. It helps in reduction of demand response and demand side management, AT & C losses, power quality management, outage management, smart home energy system etc. Virtual Power Plant, “As its name implies, a virtual power plant doesn’t exist in the concrete-and-turbine sense. Rather, it uses the smart-grid infrastructure to tie together small, disparate energy resources as if they were a single generator. Just about any energy source can be linked up, and the energy that's used can also contribute to virtual power, not plant's capacity” (Kumagai, 2012) “Virtual power plants essentially represent an 'Internet of Energy,' tapping existing grid networks to tailor electricity supply and demand services for a customer," (Peter, n.d.) While virtual power plants act as pools of autonomous generation units for producing both heat and electricity, the solar cells can only be provided to the consumers locally. In principle, virtual power plants are suited for long-distance transfer (Markus et al., 2012). Numerous issues are associated with ”Smart Technology”. The system is subjected to vulnerabilities both from within and outside. Since the grid is a data hub of information, comprising of customer data, consumption, it is critical to protecting them as it is very vulnerable to reveal the customer's information (Ramyar et al., 2014). As data is transmitted over long distances, it opens up the grid for several

Abbreviations: VPP, Virtual Power Plant; SG, Smart Grid; AMI, Advanced Metering Infrastructure; DSM, Demand Side Management; DER, Distributed Energy Resource; NTL, Non-Technical Losses; TL, Technical Losses; T & D, Transmission & Distribution; CT, Current Transformer; VEMS, Vigilant Energy Metering System; PKI, Public Key Infrastructure; VPN, Virtual Private Networks; DG, Distributed Generation; ELM, Extreme Learning Machine; OS-ELM, Online Sequential Extreme Learning Machine; DG, Distributed Generators

* Corresponding author.
E-mail addresses: sampathkumaris123@gmail.com, sampathkumaris123@outlook.com (S. Kumar V.), jprasad@jpr.amity.edu (J. Prasad), drravieee@gmail.com (R. Samikannu).
[1] Current address: Botho University, Gaborone, Botswana, PO Box 501564, Botho University, Kgale KO, Near Game City, Gaborone, Botswana.

http://dx.doi.org/10.1016/j.enpol.2017.08.032
Received 2 June 2017; Received in revised form 30 June 2017; Accepted 13 August 2017

vulnerabilities regarding data theft or manipulation, thus invading consumer's privacy due to increased connectivity facilitating personal information collection. End-user data is also potential areas for cyber security threats that may be used for damaging infrastructure, power theft, espionage and other purposes. Failure to eliminate these risks will obstruct the modernization of the existing power industry. Intrusion Detection Systems (IDS), Anti-virus software's, Public Key Infrastructure (PKI), Virtual Private Networks (VPN), Firewalls that are contemporary security technologies used to protect the IT infrastructure, will still not be very effective source of defense, if directly deployed on the smart grid due to their inherent differences in application. Infrastructure privatization, new power policies requires the business to operate efficiently to optimize profits in rapidly changing environment (Patterson, 2001; Flavin and Lenssen, 1994).

The smart grid is a complicated system that uses many smart components. A smart grid uses automated methods for monitoring, distribution of electricity across the grid. As the system is complex, it will enable the utility companies to measure the energy consumption at a micro level creating better flow patterns and empowering different ways to analyze demand in the energy sector, thereby facilitating the generating companies to understand and meet the demand and close the gap between demand and supply. This development comes with adherent opportunities and challenges at multiple levels, since in a smart grid even the consumer may be a prosumer. A smart meter, in this case, identifies the energy consumption in detail. Since it is a two-way communication technology, it can securely communicate the data back to the utility company. Advanced software tools using sophisticated algorithms compute and monitor the grid components, and it is difficult to tamper with (McLaughlin et al., 2009). The Electricity boards and power utility corporations in India are in the process of installing smart meters and sensors over the next 20 years.

There are numerous methods to control the electricity theft in a normalized environment as in the case of India. Several technical and non-technical tactics need to be enforced for controlling theft. Although, like in many other countries, India treats electricity theft as a criminal offense, since it is not like any other theft, the detention of the culprits makes it more difficult. In most cases, the theft is committed in connivance with that of licensee's employees and political interference. While it is crucial to detect the point of theft, the solution lies not in controlling the theft but adopting technical measures to educate and ensure that the consumers feel at ease to pay for the services rendered by the providers. Many states in India typically follow a model of slab system for the consumers. This model could be put to use more efficiently by lowering tariff.

This paper primarily highlights the challenges due to energy theft in India. It stresses the importance on well-known emerging concepts, systems and technologies of smart grids and how it can contribute to meet the growing demand of electricity needs while mitigating the risks due to power theft. The organization of the paper is as follows: the first section presents analytical framework highlighting the fundamental problem of how power theft can be dealt with and what is the effect of power theft in Smart Grids and Virtual Power Plants? The second section discusses the effects of electricity thefts. While addressing these questions this paper will critically assess the methods and methodologies in use in the already existing power systems in Section 3 followed by Section 4 which presents the insights from the demonstration activity; Section 5 offers discussion, recommendations, while Section 6 contains the concluding remarks.

2. Analytical framework

2.1. Losses

Generation, Transmission, and Distribution (Soma Shekara Sreenadh Reddy Depuru et al., 2011a, 2011b) of electricity involve many losses. The losses can technically be classified as direct losses and indirect losses, in short, technical and non-technical losses (NTL). These losses are difficult to be quantified precisely and are unavoidable. The total combined losses in transmission and distribution across the globe is more than the sum of countries in Europe put together. The theft loss according to US consensus is between 0.5–3.5% of the annual gross revenues. It does look like a small amount, but the economic impact was termed at $280 billion in 1998. Technically that is anywhere between $1 and $10 billion (Nesbit, 2000; Thomas, 2004). On average, the losses due to theft is more than 25 billion dollars every year. India alone loses about 4.5 billion dollars every year due to electricity theft. These losses on the generation are not environment-friendly and add to the carbon footprint across the globe. Even if say 10% recovery is tabulated it conserve about 83,000 GW h of electric energy and reduce carbon emissions (Aditya Pyasi, 2008; 19–22 May 2008; Soma Shekara Sreenadh Reddy et al., 2011a, 2011b).

Typically losses are computed as follows

$$\text{Total Losses} = \text{Technical Losses (TL)} + \text{Non}-\text{Technical Losses (NTL)}$$

Where TL includes - Corona, Leakage Current, Dielectric, Open Circuit, Measuring elements, Joule, impedance and other variable losses. NTL includes energy theft, metering faults, metering inaccuracies, billing problems, unmetered supply, etc. The main contributor to NTL is Energy theft. Hence NTL can be computed as follows

$$\text{Non}-\text{Technical Losses} = \text{Total Energy} - \text{Bills Received (Paid)} - \text{TL}$$

It is difficult to detect NTL losses during T & D due to various components involved thus complicating to compute and prevent and becomes a bottle-neck for utility companies. However, TL is considered as an inherent component of losses and is catered. An alarming loss in TL will trigger an alarm which may be caused due to faulty equipment's, degraded components, etc.

2.2. Technical losses

Technical losses occur naturally due to power dissipation in transmission lines, transformers etc. (Oliveira and Barioni, 2009). Technical Losses in T & D (Transmission and Distribution) is normally computed based on the information about the load on the grid and the energy billed to the consumer (Oliveira and Barioni, 2009). Technical losses comprises of transmission lines, the energy dissipated in the conductors, equipment used for transmission and distribution like ACSR conductor, cables, transformers, relays etc. These losses are inherent to the system and cannot be eliminated. Technical losses are generally computed at 20–22.5% (See Fig. 1, Table 1) depending on various factors including delivery systems, networks etc. However, this varies with the technology used. That is Loss at 20% of the generated capacity

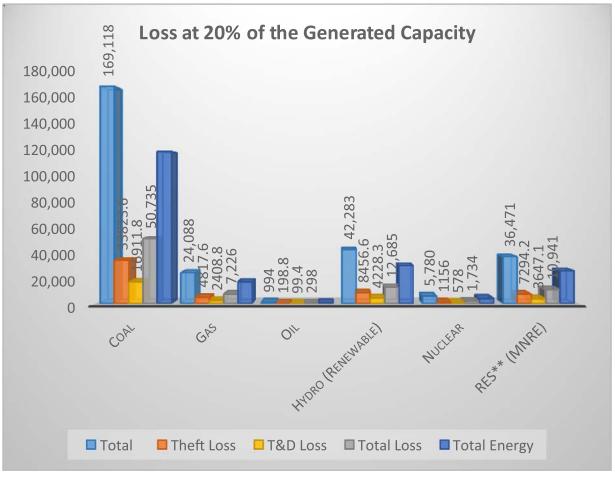

Fig. 1. Source MOP, GOI, [14,15].