World Academy of Science, Engineering and Technology
International Journal of Electronics and Communication Engineering
Vol:9, No:11, 2015

Smart Grids Cyber Security Issues and Challenges

Imen Aouini, Lamia Ben Azzouz

Abstract**—**The energy need is growing rapidly due to the population growth and the large new usage of power. Several works put considerable efforts to make the electricity grid more intelligent to reduce essentially energy consumption and provide efficiency and reliability of power systems. The Smart Grid is a complex architecture that covers critical devices and systems vulnerable to significant attacks. Hence, security is a crucial factor for the success and the wide deployment of Smart Grids. In this paper, we present security issues of the Smart Grid architecture and we highlight open issues that will make the Smart Grid security a challenging research area in the future.

Keywords**—**Smart grids, smart meters, home area network, neighbor area network.

I. Introduction

THE Smart Grid is a modernized electric grid that uses the Information and Communication Technology (ICT) to enable a variety of applications that aims to reduce energy consumption and losses, integrate distributed energy resources and deploy infrastructures of electronic vehicles charging [10], [17]. For example, put off heating or air conditioning if a home is unoccupied or even adjusts the temperature will reduce significantly unnecessary energy consumption. Additionally, electricity requires long distance transmission lines that cause power losses averaging 26% of power generation [3], [8]. Sensors and intelligent devices in the power grid will be able to control and detect circuit outages. This will help in reducing transmission and distribution losses [8], [11]. Smart Grids provide also the flexibility to integrate different types of Distributed Energy Resources (DER) such as wind and photo-voltaic [5], [6]. Therefore, consumers will not act as passive receivers of power, but can take instead charge of their energy production [6]. Moreover, Smart Grids challenges will be to manage the infrastructures of Electronic Vehicles (EV) charging and to control the load balancing in order to avoid blackouts and energy peaks when charging EV [1]. For example, the grid allows the charging of EVs using the Plug-in Hybrid Electronic Vehicle (PHEV) only when energy consumption is lower.

In order to deploy Smart Grid networks, organizations for standardization (NIST, IEEE, IEC, ETSI…) issued many works. Most of these works focused on advanced metering, transmission and distribution systems, distributed energy resources and electronic vehicles. The National Institute of Standards and Technology (NIST) coordinated with some groups to harmonize a global architecture for the Smart Grid framework [15]. The European Telecommunications Standards Institute (ETSI) based its work on this architecture, but introduced some modifications taking into account European requirements [16]. The IEEE developed the IEEE 2030-2011 guide for Smart Grid interoperability that defines three levels of the Smart Grid architecture: power systems, communications technology, and information technology [2], [14].

Nowadays, security has become a crucial factor for the success and wide deployment of Smart Grid networks. The Smart Grid introduces new security issues due to network architecture characteristics and the critical nature of applications in terms of delay, sensitive and personal data being exchanged. Many works, in the literature addressed security issues and vulnerabilities of Smart Grids [18], [20], [29]. In this paper, we give an overview of works and standards dealing with security issues and attacks that can be performed on the Smart Grid architecture. This overview is presented as a classification of attacks that can be performed according to criteria determined from the characteristics of the Smart Grid. We also highlight attacks that can be performed on Smart Grid and not identified in previous works. The paper is organized as follows. In Section II, we describe standardization works and we introduce the NIST and European architecture. In Section III, we identify, in a first step, characteristics that can have an impact on security. In a second step, we propose a classification of security issues and attacks identified in the literature. In Section IV, we present Smart Grids security requirements identified in some works and we highlight security service requirement for each proposed class. Section V highlights security issues and attacks that are not yet explored in the literature. In the Section VI, we discussed future security challenges of the Smart Grid and the end-to-end security architecture.

II. Smart Grids: Standardizations Works

In order to ensure the interoperability of Smart Grids, various standards are currently under development by several international organizations.

The NIST has defined a global architecture for the Smart Grid divided into seven domains (customers, Distribution, Transmission, Market, Service Providers, Bulk generation, operations) as shown in Fig. 1. Each domain covers many actors (Smart meter, substations, control center…) that interact to provide several Smart Grid applications.

Imen Aouini and Lamia Ben Azzouz are with the University of Manouba, Ensi Cristal Laboratory Manouba, Tunisia (e-mail: imen.aouini@ensi-uma.tn, lamia.benazzouz@ensi.rnu.tn).

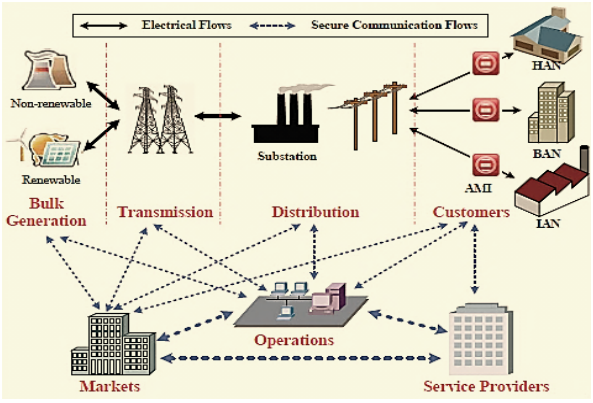

Fig. 1 Domains of NIST architecture

The Smart Grid Coordination Group (SGCG) was established by the European Standardization Organizations CEN, CENELEC and ETSI) to ensure a coherent work for the deployment of Smart Grids in Europe. In 2012, the SGCG established a European conceptual model that extends the existing NIST Model to address the European Distributed Energy Resources (DER) specificities. The Distributed Energy Resources domain is integrated into the NIST Model and has interactions with operations, market, services provider and distribution NIST domains as shown in Fig. 2. These distributed electrical resources are connected to the public distribution grid and may be directly controlled by the service provider.

The IEEE Std 2030–2011 Guide for Smart Grid Interoperability [7] was developed by IEEE standardization organism that is based on the NIST framework. It elaborates a Smart Grid Interoperability References Model (SGIRM) that considers three levels (power system, communication and information technologies). The power system represents a view of the production, delivery, consumption of electrical energy. The communication technology provides the relationship of various sub-networks of the Smart Grid such as Home Area Network (HAN), Neighbor Area Network (NAN) and Field Area Network (FAN). The information technology describes the data flows associated with Smart Grid applications.

The IEEE Std 1547 provides physical interconnection, specifications and requirements for distributed energy resources that include both distributed generators and energy storage systems [2].

III. Attacks on Smart Grids Network

Smart Grid is a complex infrastructure that covers a growing number of heterogeneous electronics nodes, including smart meters, sensors in Home Area Network (HAN) and intelligent electronic devices. These nodes communicate through several networks (HAN, NAN, FAN, WAN) and use different communication technologies. This introduces security challenges for each interface involved in the communication with other nodes. IEEE specified Nodes exchange commands, messages and energy information for a variety of applications. This information is critical and personal which increases vulnerabilities of Smart Grids. Also, the Smart Grid has diverse characteristics (time constraints, data rate, etc.). It is vulnerable to malicious attacks of varying types that can severely obstruct its widespread deployment. Many research works were interested in identifying attacks and threats on the Smart Grid and proposed classification of these attacks based on different criteria. Works of [20] showed that attacks can be classified into three types: Attacks targeting availability, integrity and confidentiality. Attacks targeting availability also called Denial-of-service have an impact on the performances because some Smart Grid features are delay-constrained. According to [30], Attacks on the confidentiality and integrity of the information will concern the smart meter. Authors of [24] addressed four types of attacks (Device attack, Data, Privacy, Network availability) that can be performed on Smart Grid communication. Device attacks aim to compromise grid devices. Data attacks attempt to alter or delete data of the network traffic. The Privacy attack aims to learn users' private information by analyzing the network traffic. Network availability attacks aim to use resources of the smart grid to make an online service unavailable. These classifications have not taken into account the type of network where node is involved. We can notice that attacks targeting confidentiality have more impact on the privacy when they are performed on the HAN while the NAN is more concerned by modification attacks. Moreover, these works does not discuss the impact of attacks on the Privacy particularly in the HAN. In addition, other critical nodes (PMU, Concentrator…) are also vulnerable to attacks that can have serious affect in the entire of network. For these reasons, we propose, in this work, a new classification for attacks on the Smart.

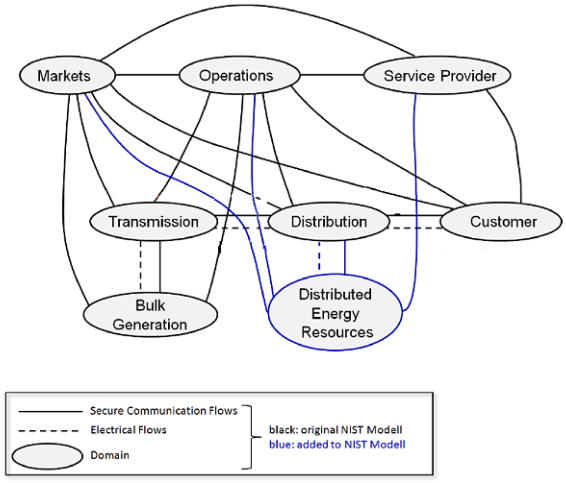

Fig. 2 European extension of the NIST

In this section, we identify, firstly, the criteria that have an impact on the security of the Smart Grid. Second, we present a classification of works investigating threats and attacks according to these criteria.

A. Classification Criteria

We present below the most important criteria for the proposed classification of attacks.

- **The type of node:** Due to heterogeneity of nodes involved in *the* Smart Grid and specific attacks related to, we defined the criteria type of node. So, we distinguish two types of nodes: components (smart meter, Phasor Measurement Unit (PMU), Plug in Hybrid Electronic Vehicle (PHEV)…) and system (Distributed Management System (DMS), Advanced metering infrastructure (AMI)…).
- **The location of node:** Smart Grids span large geographical areas and could incorporate several networks (HAN, NAN, FAN etc.). Communications among nodes in the same network may have similar characteristics and requirements. Each network presents particular security issues and raises specific security requirements.

B. Attacks Classification

Based on criteria described above, we classify attacks on three groups (components, systems and networks).

1. Components Security Issues

J. Liu and Y. Xiao [29] showed that attacks can be performed on different types of devices such as consumer devices (smart meter, PHEV…) and distributed automation devices. In fact, several constraints for Smart Grid devices such as limited bandwidth, storage, memory and intermittent connections increase their security issues.

Many works [21], [25], [30] evaluated the security issues of smart meters. Malicious node can disrupt normal operations of smart meters by performing several types of attacks. Jamming attacks can be launched to prevent the legitimate smart meter from communicating with other nodes (distributed substations, neighbors smart meters, the control center). Moreover, an unauthorized node can perform eavesdropping to detect sensitive information about the customer energy usage (energy consumption, energy bills, types of home electronic devices…). In addition, an attacker can perform a false data injecting attack against smart meters by sending an error control command. In [27], authors described an application of the smart meter called Remote Connect Disconnect (RCD) that allows connecting a smart meter and delivering the energy after maintenance operations or the payment of a bill without the presence of a service agent. In order to prevent a customer from energy, an attacker can achieve a remote disconnect attack by sending disconnect commands to shut down the customer's smart meter. We can note that attackers may also use this application to connect a smart meter and benefit from an illegal energy.

Message time stamping or the use of the nonce is normally considered sufficient against replay attack. However, real-time clocks in smart meters have some fundamental issues while, they cannot be synchronized within communication networks. On the other hand, messages of smart meters or the control center take more time to achieve their destinations. These two factors make opportunistic replay attacks highly possible. Authors of [30] showed a replay attack of control commands that necessary impact smart meters. For example, an attacker can replay an old peak energy alert transmitted by the control center. As a result, the smart meter turns off some devices while energy is available.

Some works focused on a device called a home gateway that receives the power consumption data from the smart meter and displays it on householder's devices (e.g., laptop, tablet, Smartphone). The home gateway or the smart meter may send the power consumption data to a service provider to manage energy use for financial benefit (e.g. Efficiency advice, pricing choice…). Hence, authors of [25] show that gateway communications can be affected by eavesdropping and modification attacks. For example, a malicious node can modify the energy consumption data to affect the marketing purposes of the service provider.

Phasor Measurements Units (PMU) are able to collect field measurements of voltages and electrical quantities and send it to the Phasor Data Concentrator (PDC) [33]. The PDC reads the data from multiple PMUs, merges it as a single message, and communicates with the operations domain [15]. Authors of [30], [31] illustrate that malicious node can perform PMU spoofing attacks, modify PMU messages that contain energy measurement data and can also replay messages in transit between the PMU and the PDC. These attacks affect critical decision operations such as fault detection and event location and impact the transmission network. For example, when an attacker replays an old PMU message that contain energy measurement losses or line outages, the operation systems may take a decision to turn off electricity for an area.

2. Systems Security Issues

The operations domain has several control systems which have similar objectives and requirements [15]. The Energy Management System (EMS) and Distribution Management System (DMS) are responsible for the control of transmission and distribution of energy [4]. Supervisory Control and Data Acquisition (SCADA) support controlling applications that detect problems on the electrical power grid [11].

Several papers [21], [24], [29] highlighted that control and management systems are performing critical operations (regulate voltage, define outages, transfer of power…) for the energy distribution and transmission and need to be protected against attacks. A malicious node can perform DoS attacks on control systems and affect their availability. In addition, a false-data attack against control systems can affect their decisions. For example, sending false measure energy will have an impact on the distribution and transmission operations while systems make control decisions based on false PMU information. A malicious node can replay PMU transmission measurement data, then, the control center takes decision based on old data.

Wide Area Monitoring, Protection and Control (WAMPAC) system will exchange transmission data with other control systems to provide real-time monitoring and alarm functions and ensure efficient energy transmission, generation and aggregation in the electric grid [32]. In [31], the classification of attacks showed that WAMPAC system is also vulnerable to timing based attack (DOS attack) while

applications provide real time operation and performance. Denial of service attack can be performed at different communication layer. For example, a malicious node can launch jamming that fills the wireless medium with noise signals and can have severe impact on time-critical messages. Jamming attack is able to damage the availability of the system, and legitimate node cannot recover messages. Furthermore, other types of attacks such as spoofing and man-in-the middle attacks can be launched only when the full or partial communication channels can be jammed.

In AMI system (communications between smart meters and the control center), messages are delivered in multi-hop. Man-in-the-middle attacks can be possibly launched, and energy consumption information can be modified before transmitting messages. In addition, by eavesdropping on the wireless communication channel, an attacker could gain information exchanging between the smart meter and the control center.

3. Network Security Issues

The Neighborhood Area Network (NAN) covers and manages communications between smart meters in a specific geographic area [13]. The Routing Protocol for Low power and lossy networks (RPL), the Minimum Transmission Energy (MTE) protocol and the Adhoc On-Demand Vector Multipath (AODVMP) are routing protocols that can be used on NAN networks [9], [24], [25]. Work in [26] demonstrates that the most available attacks against WSNs (e.g. Selective-Forwarding Attacks…) can affect the RPL routing protocol for the Internet of Things (IoT). We note that, while the particular characteristics of Smart Grid networks, the RPL routing protocol for NAN networks can fail under other types of attacks. The work in [25] showed that Wireless Sensor Networks attacks are also applicable to the Minimum Transmission Energy (MTE) protocol. For example, an attacker can perform a black hole or a selective forwarding attack to drop incoming packets. Simulation results show that a small number of compromised smart meters can severely alter network connectivity and packet delivery measures.

Works described in [19], [20], [28], show that network communication protocols of the Smart Grid are also an important source of vulnerabilities. Some of the wireless protocols to be used in Smart Grid networks (e.g. Zigbee, Wimax, Wifi, LTE, UMTS, GPRS, etc.) have well known attacks (Jamming, message modification, eavesdropping…). In [28], authors discussed security issues and attacks of WIMAX, LTE, PLC in a NAN environment.

The Home Area Network (HAN) manages communications between HAN devices (e.g. PHEV, programmable communicating thermostats…) and the smart meter. HAN can use different communication technologies such as Zigbee, Bluetooth, WiFi [5], [12], [15]. [19], [21], [28] pointed that some existing security solutions (e.g. IDS, IPsec, VPN, PKI…) can be applied in the context of Smart Grid but they are not sufficient to secure it for its special features. Table I summarizes attacks for each group.

TABLE I
ATTACKS AND SECURITY REQUIREMENTS

	Node/protocol	Attacks
Components	Smart meter	Jamming, Eavesdropping, Tracking, False data injecting, Replay attacks
	PMU and PDC	Spoofing, Modification, Replay,
	Gateway	Modification, Eavesdropping,
Systems	AMI system	Modification, Man in the middle, Eavesdropping,
	WAMPAC system	DoS attacks,
	Control system	DoS attacks, False data injecting
Location (HAN,NAN,WAN)	Communication protocols	Replay, Jamming, Eavesdropping
	Routing protocols	Selective forwarding, Black hole

IV. SECURITY SERVICE REQUIREMENTS

We review, in this section, security service requirements identified by the NIST guidelines and research works. Then, we highlighted security services required by groups described in our classification.

NIST issued Guidelines for Smart Grid Cyber Security [18] where it identified security requirements necessary to protect the modernizing power grid from attacks. This guideline identified first all network interfaces of nodes involved in Smart Grids. For example, the smart meter has a lot of interfaces with other equipment such as with electronic vehicle or distributed energy resource sub-meters and MDMS (Meter Data Management System), etc. Then, NIST categorized these interfaces based on their security needs. This classification addressed twenty two categories similar in their security related characteristics. For example, the multiple smart meter interfaces were classified in different categories such as the category for interfaces between metering equipment (smart meter, EV and DER sub-meter…) where integrity and confidentiality are important, but availability is not critical. In addition, another category, for interfaces with systems, requires the integrity of data and availability; but, where data do not need to be confidential. NIST evaluated so the impact level (low, moderate or high) of security service requirements (confidentiality, integrity and availability) for each category.

Additionally to Smart Grid security needs characterized by the NIST guideline, [21], [25] and [30] highlighted that the non-repudiation service is also necessary for the traffic of smart meters. A compromised smart meter may transmit an incorrect meter reading to the control center, and claim that it did not send this information. Therefore, the basis for billing in the grid will be shattered.

The intensive personal information, being exchanged by the Smart Grid applications, details the energy usage of the customer (the type of home devices, meter reading, electricity bill…) and presents new privacy considerations. Several

works [21], [20], [25] and [29] showed that malicious attacks can obtain information about usual energy consumption. These data may be used by a malicious node to track activities of home appliances. For example, recharging the electric vehicle provide information on the number of kilometers traveled in one day and Heaters-off in winter can provide information about the occupation or not of the home.

Some works [22] and [23] proposed mechanisms to protect the privacy for the traffic of smart meters. In fact, [22] suggests a method that creates two different ID for the smart meter. Those ID are high-Frequency ID for often metering data (e.g. Meter reading every few minutes) and Low-Frequency ID for scarcely metering data (e.g. Bill reads every week or month).

We show in Table II, the security services required by each group described in the previous section.

TABLE II
SECURITY SERVICES REQUIREMENTS OF SMART GRID NETWORK

Groups \ Security Services	Confidentiality	Privacy	Integrity	Availability	Non-repudiation	Authentication
Smart meter	×	×	×	×	×	×
PMU and PDC			×		×	×
Gateway	×	×	×			×
AMI system	×	×	×			
WAMPAC system				×		
Control system			×	×		
Communication technology				×		
Routing protocols			×	×		

V. DISCUSSIONS AND REMAINING SECURITY ISSUES

Works in the literature showed that attackers can perform several types of attacks on devices and systems. In addition, communications and routing protocols can fail under other types of attacks. However, these works lack serious study of security issues on HAN, NAN and WAN. Furthermore, some attacks are missing on devices and systems.

Few works in the literature studied security issues of electronic devices on home area networks. Besides, several attacks can be performed on HAN devices and mechanisms, and have a serious impact on the home energy management. Demand Response (DR) is a mechanism that manages customer consumption of electricity to reduce energy peak demands and consumption according to market prices. The energy demands of some home devices including dishwasher, washing machine, Plug-in Hybrid Electric Vehicle (PHEV), etc. are based on energy consumption information delivered by the smart meter to schedule their load between low and high demands and prices. An attacker can spoof the smart meter identity and send false response to those devices in order to cause a peak energy demand, increase the electricity bill or to shut off devices.

Concentrators are deployed on the electronic grid to aggregate data from intelligent electronic devices and communicate information to the control center. The data concentrator collects energy usage data of smart meters. The Phasor Data Concentrator (PDC) receives transmission data from multiple Phasor Measurement Units (PMUs). The communication of concentrators with a lot of devices must be protected against attacks. We address that concentrators are vulnerable to many types of attacks such as spoofing and flooding that can isolate several devices from the control center. In addition, concentrators must ensure the integrity of data since the modification of these data may result in wrong reconfiguration actions, the possibility of money loss and the power failure affecting multiple countries.

Distribution automation devices (closers, automated feeder switches, voltage regulators…) allow automatic decisions on the energy distribution network in order to avoid failure situations and reduce peak loads. A wide range of attacks such as the false data injecting, the replay and the spoofing attack may be performed on distribution automation devices and its operations. For example, automation distribution devices are used to manage the transfer of energy from one substation to another to equilibrate the total load and avoid circuit outages. Therefore, an attacker can spoof the identity of an automatic distribution device and send false messages to route power around a fault.

Each NIST architecture domain (Markets, service providers, customer, operations…) has intelligent devices that exchange critical information. Therefore, the different types of interfaces and protocols required for exchanging information between each of these domains need to be protected against malicious operations.

VI. FUTURE SECURITY CHALLENGES

Securing the Smart Grid, from the control center to the distributed substations, Intelligent Electronic Devices (IED) and even to customer meters, requires a global end-to-end security infrastructure. This infrastructure must deploy security solutions for networks (HAN, NAN and FAN) and endpoints (Smart meters, IED, substations, control center) that tier network together.

Smart Grid communications infrastructure may support multiple access technologies such as Zigbee, Wimax, WI-Fi. The Home Area Network (HAN) manages several electronic devices using the Zigbee protocol. Zigbee specification [34] presents a number of security provisions for devices in a Zigbee network. Studying the performance of Zigbee security

mechanisms for the management of Zigbee applications in the home area network stays an open research topic. While Zigbee specifications have been designed for simpler tasks like remote controls, the Zigbee Alliance works actually to provide a standard for the NAN mesh network. The Field area network can establish communications between distributed devices and substation based on Wimax. In order to deploy an end-to-end security infrastructure, the set of access technologies involved in the Smart Grid must be secured to protect the flow of Smart Grid operations. On the other hand, [35] pointed out the use of IPsec protocol to provide an en-to-end security architecture for the Smart Grid network. In this case, a study of IPsec over Zigbee and Wimax has to be considered. Zigbee was designed for local networks, it does not directly communicate with devices on the Internet. However, some devices in the home area network and smart meters need to communicate information through the Internet. The IPv6 over Low power wireless Personal Area Networks (6LowPAN) allows the exchange of IPv6 packets over and from the IEEE802.15.4 based networks [34]. If the 6LowPAN is used in the home area network, extended security requirements must be addressed. Moreover, the security of IP based Wimax for the FAN network has to be studied. The deployment of IPsec in the Smart Grid network may introduce some issues while Smart Grids present particular constraints (real-time data, delay…).

VII. Conclusion

Securing the Smart Grid is essential since the information exchanged is sensitive and management operations are critical (turn off the electricity, shut down smart meters…). The Smart Grid is organized in many domains and each domain involves heterogeneous devices and systems. Therefore, it is difficult to study vulnerabilities of the whole network. In the literature, most of works focused on identifying threats and attacks on domains and even on devices and systems. The smart meter is a critical component and is vulnerable to many types of attacks (Tracking, eavesdropping, false data injecting and replay attack). In addition, we highlighted that an attacker can spoof the identity of the smart meter to get access to all home devices. Control systems (DMS, EMS) can be affected by DOS attacks that make systems unavailable for grid requests. Some works were interested in determining attacks that can be performed on networks and especially on the NAN network. Man-in-the-middle attack on the AMI system and selective forwarding attack on routing protocols may isolate a legitimate node that will not be able to reach its neighbors and the control center. However, there are very few works investigating the security of domains like service providers, markets, bulks generation, etc. while, many attacks can be launched against them and deserve a study in future works. To secure the Smart Grid, an end to end security architecture has to be addressed. Two ways can be envisaged securing all communication protocols involved in the Smart Grid or by using IPsec.

References

[1] Z. Qiqi, S. Gang, L. Puming, Smart City Grid: The Start to Develop Smart Grid, International Conference on E-Product E-Service and E-Entertainment (ICEEE), pp.1-4, 2010.

[2] IEEE Standards Coordinating Committee, 'IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads' 2011.

[3] C. Selvam, K. Srinivas, G. S.Ayyappan, M. V.Sarma, Advanced Metering Infrastructure for Smart Grid Application, International Conference on Recent Trends In Information Technology (ICRTIT), pp.19-21, 2012

[4] Y. Yan, Y. Qian, H. Sharif and D. Tipper, A Survey on Smart Grid communication Infrastructures: Motivations, Requirements and challenges, IEEE Communications surveys & tutorials, Vol.15, No.1, pp.5-20, 2013.

[5] Guizani, M., Anan, M., Smart grid opportunities and challenges of integrating renewable sources: A survey, International Wireless Communications and Mobile Computing Conference (IWCMC), pp-1098-1105, 2014.

[6] B. H. Chowdhury, C. Tseng, Distributed Energy Resources: Issues and Challenges, Journal of Energy Engineering, Special Issue: Distributed Energy Resources-Potentials for the Electric Power Industry, pp.109-110, 2007.

[7] IEEE Std 2030, 'IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads', 2011.

[8] J. Dickert, M. Hable, P. Schegner, Energy Loss Estimation in Distribution Networks for Planning Purposes, International Conference on Bucharest PowerTech, pp.1-6, 2009.

[9] Binod Vaidya, Dimitrios Makrakis, Hussein Mouftah, Secure Multipath Routing for AMI Network in Smart Grid, IEEE 31st International Performance Computing and Communications Conference (IPCCC), pp.408 - 415, 2012.

[10] B. P anajotovic, M. Jankovic, B. Odadzic, ICT and Smart Grid, 10th International Conference on Telecommunication in Modern Satellite Cable and Broadcasting Services (TELSIKS), pp.118-121, 2011.

[11] D. J. Dolezilek, S.Schweitzer, Practical Applications of Smart Grid Technologies, Published By Schweitzer Engineering Laboratories, Inc. (SEL), 2009.

[12] C. Bennett, D. Highfill, Networking AMI Smart Meters, IEEE Energy 2030 Conference, pp.1-8, 2008.

[13] Yifeng He, Mohammad Shams Yazdi, Differentiated service for Smart Grid neighbourhood area networks via optimal resource allocation, International Journal of Sensors and Sensor Networks; pages: 55-60; 2013.

[14] Kenneth C. Budka Jayant G. Deshpande Marina Thottan, Communication Networks for Smart Grids Making Smart Grid Real, Computer Communications and Networks, Springer,pp.1-377, 2014.

[15] NIST Special Publication 1108 NIST, Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0, 2010.

[16] CEN-CENELEC-ETSI Smart Grid Coordination Group, CEN-CENELEC-ETSI Smart Grid Coordination Group – Sustainable Processes, 2012.

[17] J. O. Petinrin, Mohamed Shaaban, Smart Power Grid: Technologies and Applications, IEEE International Conference on Power and Energy (PECon), pp.892 - 897, 2012.

[18] NISTIR 7628 Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements, The Smart Grid Interoperability Panel – Cyber Security Working Group; 2010.

[19] Fad iAloula, A. R. Al-Alia, Rami Al-Dalkya, Mamoun Al-Mardinia,Wassim El-Hajj, Smart Grid Security: Threats, Vulnerabilities and Solutions, International Journal of Smart Grid and Clean Energy; vol. 1 No.1, 2012.

[20] Wenye Wang, Zhuo Lu, Cyber security in the Smart Grid: Survey and challenges, In Computer Networks, vol.57 no.2013, pp.1344–1371; 2013.

[21] Xinxin Fan and Guang Gong, Security Challenges in Smart-Grid Metering and Control Systems, Technology Innovation Management Review; pp.42-49, 2013.

[22] C. Efthymiou and G. Kalogridis, Smart Grid Privacy via Anonymization of SmartMetering Data, First IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 238-243, 2010.

[23] L. Sankar, S. Raj Rajagopalan, S. Mohajer, H. Vincent Poor, Smart Meter Privacy: A Theoretical Framework, IEEE Transactions on Smart Grid, vol.4, No.2, pp.837-846, 2013.
[24] X. Li, X. Liang, R. Lu, X. Shen, X. Lin, and H. Zhu, "Securing smart grid: Cyber attacks, countermeasures, and challenges," IEEE Commun. Mag., vol. 50, no. August, pp. 38–45, 2012.
[25] K. Sophia, Sekercioglu, Y. Ahmet, Security and smart metering, EW.18th European Wireless Conference,pp.1-8, 2012.
[26] L. Wallgren, S. Raza, and T. Voigt, Routing Attacks and Countermeasures in the RPL-Based Internet of Things, International Journal of Distributed Sensor Networks Vol.2013, 2013.
[27] William G. Temple, Binbin Chen, Nils Ole Tippenhauer, Delay Makes a Difference: Smart Grid Resilience Under Remote Meter Disconnect Attack, IEEE International Conference on Smart Grid Communications (SmartGridComm), pp.462-467, 2013.
[28] E. Bou-Harb, C. Fachkha, M. Pourzandi, M. Debbabi, and C. Assi, Communication Security for Smart Grid Distribution Networks, IEEE Communications Magazine, vol.51 No.1, pp. 42-49; 2013.
[29] Jing Liu and Yang Xiao, Shuhui Li, Wei Liang, C. L. Philip Chen, Cyber Security and Privacy Issues in Smart Grids, IEEE communications surveys and tutorials, vol. 14, no. 4, 981- 997, 2012.
[30] Zubair A. Baig and Abdul-Raoof Amoudi, An Analysis of Smart Grid Attacks and Countermeasures, Journal of Communications Vol. 8, No. 8, pp.473-479, 2013.
[31] Aditya Ashok, Adam Hahn, Manimaran Govindarasu, Cyber-physical security of Wide-Area Monitoring, Protection and Control in a Smart Grid environment, Journal of Advanced Research; Vol.15, No.4, pp. 481-489, 2014.
[32] Electric Power Research Institute (EPRI), Wide Area Monitoring, Protection, and Control Systems (WAMPAC), Standards for Cyber Security Requirements DRAFT, 2012.
[33] B. S ingh, N. K. Sharma, A. N. Tiwari, K. S. Verma, S. N. Singh "Applications of phasor measurement units (PMUs) in electric power system networks incorporated with FACTS controllers" International Journal of Engineering, Science and Technology Vol. 3, No. 3, pp. 64-82, 2011.
[34] Castellani, A. P, Ministeri, G.; Rotoloni, M.; Vangelista, L. Interoperable and globally interconnected Smart Grid using IPv6 and 6LoWPAN, IEEE International Conference on Communications (ICC), pp.6473-6478, 2012
[35] Cisco and its affiliates; Cisco Connected Grid Security for Field Area Network; (Online). Available: http://www.cisco.com/web/strategy/docs/energy/C11-696279-00_cgs_fan_white_paper.pdf, 2012.