Security Assessment of the Smart Grid: A Review focusing on the NAN Architecture

Oyeniyi Akeem Alimi, Khmaies Ouahada
Department of Electrical and Electronic Engineering Science
University of Johannesburg
Johannesburg, South Africa
alimioyeniyi@gmail.com, kouahada@uj.ac.za

***Abstract*—This paper presents a comprehensive review on the security aspect of the smart grid communication network. The paper focus on the Neighborhood Area Network (NAN) cybersecurity and it laid emphasis on how the NAN architecture is such an attractive target to intruders and attackers. The paper aims at summarizing recent research efforts on some of the attacks and the various techniques employed in tackling them as they were discussed in recent literatures and research works. Furthermore, the paper presents a detailed review on the smart grid communication layers, wireless technology standards, networks and the security challenges the grid is currently facing. The work concludes by explaining current and future directions NAN communication security could consider in terms of data privacy measures. The data privacy measures are discussed in terms of prevention and detection techniques.**

Keywords*— *Smart grid, Cyber-security, Neighbourhood Area Network, SCADA, AMI.

I. INTRODUCTION

Utility providers in the old electricity grid struggled in monitoring the performance of the grid. Infact, old grid operators usually await reports on blackouts, low voltage supplies, tripped distribution electric poles, faulty feeders, faulty transformers from energy consumers, after all the grid's sole expectation was to supply electricity. The modern electricity grid otherwise known as smart grid (SG) or intelligrid symbolizes the integration of advanced information communication technologies (ICT) and varieties of digital computing into the power-delivery infrastructure [1-3]. The characteristics of resilience, reliability, robustness, security, interoperability, and efficiency symbolizes the new grid [4]. Furthermore, the new grid incorporates beneficial goals such as efficient energy usage, distributed energy sources (DES) and robust cyber-safety etc. The National Institute of Standards and Technology (NIST) acknowledged a SG conceptual model [4-5] which gives the expected characteristics, requirements, operations and services for the SG. It is presented in figure 1. The model highlights seven key areas which are; bulk generation, transmission, distribution, customer, service provider, operations and markets.

The control and operation of the current and future SG network hinge on communication network complexity and its security. The advanced communication facilities make the electricity grid "smarter". The communication infrastructures utilize varieties of network nodes, control and monitoring devices that allows a two-way communication network between the various domains or sublevels of the electricity grid, thereby uniting every part of the grid into a single network [5].

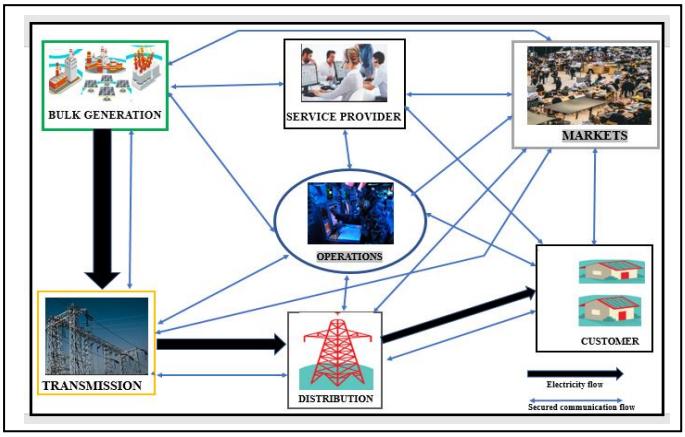

Fig. 1. Smart Grid Conceptual Model [4,5]

However, the fact that SG communication is the backbone of the electricity grid exposes the grid to all sorts of attacks. Numerous plethora of security concerns are uprising daily due to increased dependency on the interconnected network nodes that do the job of taking accurate state measurements, pricing information, control actions etc and transmitting the data to other nodes. Also, other reasons such as increased endpoints at SG domains as well as widespread SG devices and numerous commercial hardware and software have constituted to bigger security issues for successful SG implementation. A preliminary estimate at a utility presents a daily generation of 22 gigabytes of data from its 2 million customers [6], with this quantity of vital information from different residents, efficient security measures in terms of data privacy is imperative to maintain a successful grid network. [7] emphasized that, often security measures focus on outsider's attack, but attacks originating from grid insiders are equally destructive and damaging. From a report [8], insider attacks accounted for approximated 34% of reported cyber-crimes in the United States. A typical example of insider attacks was the Stuxnet attack whereby the grid network was infiltrated using USB devices [9]. Furthermore, attacks do not only lead to the shutting down of the grid, it also inflicts financial implications

on operators as experienced in the August 14, 2003 attack that caused blackout in some part of Canada and United States. The blackout yielded an estimated bill of $4 billion and $10 billion (U.S. dollars) and $2.3 billion for USA and Canada respectively [10, 11].

At the energy consumer level, the utility deploys Smart Meters (SM) as a component of the (Advanced Metering Infrastructure) AMI [1,3,5]. The smart metering facility integrates all appliances in the residential domain for effective home energy management systems (HEMS), thereby residents can manage their loads, energy billings and interact with the utility in real time. Various data being transmitted from various SMs create avenues for attackers to launch attacks. Retrieving and analyzing the real-time data being transmitted in the AMI architecture, various intimate information about residents' lifestyle and properties, such as types and number of household appliances and daily routine activities can be revealed to attackers. Also, a skilled cyber-expert who wishes to avoid enormous bills may tamper with his smart meter, hence making his SM vulnerable to bigger attack risks [12]

These security challenges and several others have consistently had inestimable socioeconomic effect not just on the grid and utility, but also on government, more especially with the fact that a country's electricity grid is the foundation for most other infrastructure as well as the country's economy. Hence, an attack on the electricity grid affects other sectors [11, 13] such as economy, defense, health, education etc.

To position current research work and gives direction for future research efforts, the paper presents a review on the smart grid communication layers, networks and the security challenges it is currently facing. The paper presents some of the recent research works on cyber-attacks and solutions for future grid. As the research and development of the SG is evolving, this review paper may not contain all relevant details comprehensively, however, the paper summarizes the status and future expectations of the communication security especially at the NAN architectural level of the SG communication.

The rest of the paper is organized as follows. Section II presents an overview on SG communication. An overview on NAN architecture in terms of communication infrastructure was presented in Section III. Section IV analyses an extensive overview of NAN cyber-security and prominent attacks. Section V presents solutions and future trends. Sections VI provides analysis on data privacy measures and Section VII concludes the paper.

II. SMART GRID COMMUNICATION

In several countries of the world, the transformation of the old electric grid to SG is highly imperative to achieve energy efficiency and sufficiency [4, 14]. The widespread monitoring and control by the communication substructures enables the SG in reacting to dynamic changes at all parts of energy generation, transmission and distribution (G, T&D), as well as energy usage [1].

In the communication pattern of the SG, several sensors and measurement devices are deployed for continuous monitoring of the energy generation, transmission, distribution and usage in real time [15-17]. The communication layer, being the heart of the SG is one of the most critical elements of the SG and it has consistently played a leading role in operation and automation of the power system through applications including Advanced Metering Infrastructure (AMI) and Wide-Area Monitoring, Protection and Control systems (WAMPAC) [16]. The AMI [17-18] is defined as the communication hardware, software as well as other various data management systems in the smart grid that plays important roles of creating effective operational network between all the elements involved in the generation and utilization of the electricity. AMI enables the collection and transmission of real time energy data from sensors, smart meters and phasor measuring units (PMUs) in various homes, substations and fields, for state estimation processing and effective operation of the SG [19]. As explained in [3,20,21], Advanced Metering Infrastructure (AMI) collects metering information of Home Area Network (HAN) devices via the smart meters, provides the information to Meter Data Management System (MDMS), detect spike electricity demand based on consumption detail records and provide billing information to customers. Typical messages such as consumption data, power loss/restoration notification, billing pricing, remote load control and load shedding constitutes AMI communication node messages [22]. The main components of the AMI include [23-24];

1) *Smart Meters (SM):* These are installed on energy consumers' domains. SM records energy consumption among other information, in regular time intervals ranging from 15 to 60 minutes and communicates that data to the utility server via the DAP. Typically, a reading utilizes about 4 bytes [24]. It is estimated that by the year 2020, an approximately 800 million Smart meters would have been installed worldwide [24].

2) Data Aggregation Point (DAP)/ Concentrators: DAPs act as the intermediary between SMs and a utility center, within a NAN domain covering a few kilometers [23-25] The DAP has a massive effect on the communication quality-of-service (QoS) factors such as packet delay, packet error probability and data rate [20].

3) Utility center: Located at control center, the server relays the electricity generators and controllers with real time consumption information for state estimation, thereby keeping track on demand expectations. The center houses the meter data management system (MDMS) database [24]. The MDMS comprehends analytical tools which includes Consumer Information System (CIS), Outage Management System (OMS), Enterprise Resource Planning (ERP), power quality management, Geographic Information System (GIS) Transformer Load Management (TLM) and Outage Management System (OMS) etc which are in charge of locating smart meters and defective meters, consumer information system (CIS) that is in control of customer billing and profiling as well as distribution management system (DMS), which controls energy quality [26].

In SG communication, characteristics such as coverage area and data rate are determining factors in deciding the category of information being communicated. Based on these factors,

the communication layer within the SG has a structural design similar to the one depicted in fig. 2 [27-30].

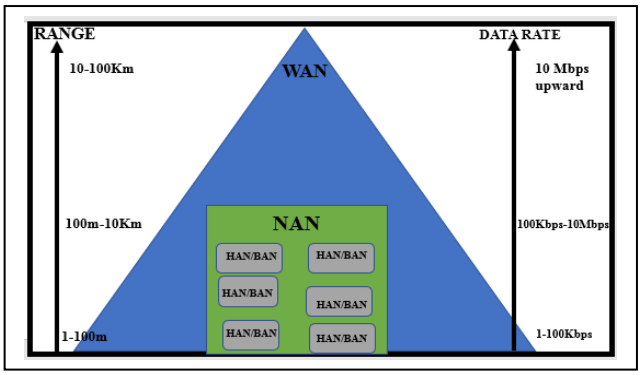

Fig. 2. Smart Grid Communication layers [27-30]

A. *Wide Area Network (WAN)*

The WAN provides a two-way real data transmission and monitoring communication between Generation domain and utility centers (Transmission domain) [27]. WAN connects the power grid control centers and several Data Aggregation Points (DAPs) (smart metering gateways), thereby transmitting massive energy data over high bandwidth links in a high-speed manner. These data transmission allows wide area situation awareness and it utilizes applications such as WAMS (Wide Area Monitoring Systems) [31]. WAN connects to several kilometers over numerous NANs in a big geographical space.

B. *Neighborhood Area Network (NAN)*

The NAN covers the distribution domain and it incorporates advanced bi-communication technologies between DAP and the smart meters located in various HANs/BANs in a smaller geographical location compared to WAN. The NAN can connect to a few hundred kilometers, housing several HANs/BANs smart meters [31-32]. In a NAN, the data transmission bandwidth rate is not as high compared to WAN.

C. *Home Area Network/ Building Area Network (HAN/BAN)*

The HAN/BAN is mainly categorized as the final energy consumers' domain. It describes a communication network within a building in which, different intelligent devices such as sensors, actuators, voltage controllers, circuit breakers etc installed in houses, exchange status information, energy usage data and instructions with the resident's smart meter to enable home energy management system [33]. Home area networks support low-bandwidth communications with bandwidth rate ranging between 10 and 100 Kbps per device [24].

Several communication technologies ranging from up to date wired and wireless communication standards have been employed in SG communication. The choice of either wired/wireless technologies depend on cost, maintenance and ease of connection to various geographical areas [34]. Also, there is the possibility of visible light communication (VLC)

TABLE I. SOME POPULAR WIRELESS STANDARDS EMPLOYED IN SMART GRID COMMUNICATION LAYER [34,74]

Layer	Standard	Spectrum	Data Rate	Coverage	Advantages	Disadvantages	Security
HAN	ZigBee (IEEE 802.15.4)	2.4GHz, 784MHz, 868-915mhz	250Kbps	30-50m	Low cost, low power and operates in ISM	Low data rate, short range	128-bit symmetric encryption key
	Bluetooth (IEEE 802.15.1)	2.4 - 2.485 GHz	721Kbps	10-100m	Low cost	Short range	secure and fast encryption routine + (SAFER+) with a 128-bit key
	Z-wave	868.42 MHz/ 908.42 MHz	40Kbps	30- 100m	Stronger security compared to ZigBee and Bluetooth, low cost	Low data rate	Z-Wave protocol supports AES-128
NAN	WLAN (IEEE 802.11X	900MHz, 2.4-60GHz	1Mbps-20Gbps (depending on standard)	20m-5Km (depending on the standard)	High data rate and it is widely used	Interference and costly (depending on the standard employed)	AES encryption, Extensible Authentication Protocol (EAP) Authentication
	WiMax (IEEE 802.16)	2.5GHz, 3.5GHz, 5.8GHz	75Mbps	10- 50Km (Line-of-sight, 1-5Km (Non-Line-of-Sight)	High data rate, QoS provisioning, low latency and scalability	Not widespread	DES, AES, Extensible Authentication Protocol (EAP) using Initial Network Entry Authentication (INEA)
WAN	Cellular (GSM, 3G, 4G, LTE	900-1800MHz, 1.92-1.98GHz, 2.11-2.17GHz (licensed), 700-2500GHz, 900MHz	up to 2Mbps, LTE allows up to 300Mbps	1-10Km, LTE allows up to 30Km	Ubiquitous coverage, High data rate	Costly spectrum,	Depending on cellular standards, there are various EAP and encryption at all nodes
	Satellite	1-40GHz	1-15Mbps	up to 6000Km	Ubiquitous coverage, low latency	Very costly	Authentication includes Timed Efficient Stream Loss-tolerant Authentication (TESLA) protocol etc
	Optical Fibre	up to 1625 to 1675 nm in wavelength	273 Gbps	up to 165Km	Ubiquitous coverage	Very costly	AES encryption & other nodal authentications

technologies as proposed in [20, 35]. However, current research innovations are tending towards wireless technology standards due to various advantages such as reliability, maintenance cost, self-healing and fast processing of data etc [36] which complements the expected features of the smart grid adoption. Table 1 presents some of the popular wireless standards utilized in SG communication layers and their various properties. Note that there are several other protocols (not included in table 1) that are currently being deployed in current and future grid. However, most of these wireless standards have technical vulnerabilities which intruders and attackers exploit in attacking the grid network. Irrespective of the type of communication technology (wired or wireless) employed, the SG network faces series of challenges, attacks and threats ranging from man-made or natural.

III. NAN Architecture

The Neighborhood Area Network (NAN) is an essential element of the AMI that connects smart meters to the DAP/concentrators [31]. In recent times, wireless communications tend to be more efficient and mostly employed for transmitting the data between the NAN domain and even beyond [37]. As explained in [19], the participation of energy users is paramount for the implementation of the SG vision. SM installations and the connection of DES (photovoltaic, and micro-CHP etc) are popular trends in today's residential and other energy consumers' domain. Also, the SM allows energy users in interacting with utility providers for optimized energy usage, less consumption patterns and other demand side management (DSM) advantages. The SM performs four distinct power management functions [38]; a) monitoring and recording usage, b) logging relevant events such as blackouts, c) transmitting catalogued messages to utility providers, and d) retrieving and activating control messages such as remote appliances disconnection.

Smart meters are continuously being deployed in several countries worldwide. SMs are expected to be in all household within the next 10 years, with Italy having the world's largest smart meter deployment so far [39]. The UK government plans on rolling out smart meters to every home by 2020 [40]. In 2012, United States electricity utility providers had approximately 43 million SM installed, out of which 89% were in the residential domain [43]. With the replacement of the previously used one-way communication meters with the advances SMs, functionalities such as billing, monitoring, scheduling, controlling and planning power consumption, production and detecting blackouts are easily accessible to all parties involved (operators, energy users and market) [32].

IV. NAN Cyber-Security

Electric Power Research Institute (EPRI) acknowledged cybersecurity as one of the biggest challenges disturbing the SG vision [42]. As explained in [30] the transformative effects of the grid domains have yielded numerous benefits on electricity users, however, it comes with severe cyber risks that are yet to be fully explored or known. The security in NAN layer of SG means security to communication network and the power grid. On the communication network side, typical considered characteristics includes energy efficiency, limited latency, guaranteed bandwidth, data manipulation avoidance etc. On the power grid side, the main security measures are reliability, stability and power quality, QoS availability & scalability. The authors in [4, 20] categorized SG attacks as;

A. Physical attacks

These are attacks that target the utility hardware components such as generator buses, transformers and transmission lines.

B. Cyber-attacks

Massive integration of wireless technologies and infrastructures has geometrically increased cyber threats and attacks. SG cyber-attacks can be classified based on topology as:

• Attack on the hardware: these include attacks on the human–machine interface (HMI) devices, automation devices, Terminal unit devices such as MTU and RTU.

• Attack on software: these attacks exploit vulnerabilities in protocols employed such as DNP3 and Modbus.

• Attack on network topology: these attacks exploit network topology vulnerabilities.

Furthermore, based on the mode of operation, [41] grouped cyber-attacks as passive and active attacks. Attacks such as eavesdropping, spoofing, traffic-analyzing and monitoring constitute passive attacks while DNS attack, flooding attack, DoS attack, IP hijacking, wormhole attacks etc constitute active attacks. Also, according to [44], security attacks in the NAN architecture can be via network protocol flaws or via component flaws. Security vulnerability which arises from flaws in network areas including protocol routing, network configuration, encryption, authentication protocol whereas component flaws include hardware/ software flaws which occurs in design/implementation e.g access to encryption key, read and write access to data storage.

The SCADA network utilizes cyber physical systems which provides relevant information on the state of the grid based on real time meter recordings and controlling gadgets such as Master Terminal Unit (MTU), Remote Terminal Unit (RTU), Programmable Logic Controllers (PLC), IEDs distributed at strategic locations, thereby creating a vast communication network [26, 45]. The meter measurements include the smart meter readings at HAN level and the readings from various substation domains such as bus voltages, bus power injections and reactive power flows. For substation automation standards, SCADA uses several standards including the Distributed Network Protocol 3 (DNP3), Generic Object-Oriented Substations Events (GOOSE), IEC 61850 etc [8, 42]. These measurements are conveyed to various SCADA facilities such as DAP, WAMS, control center etc whereby they are stored in telemetry files for state estimation, billing among other things. State estimation (SE) is a data processing technique that is used extensively for calculating power system state variables based on measurement collected from SCADA devices [46-47]. The various tasks performed by the SCADA networks makes the

network a profitable avenue for intruders to attack the SG network. Attacks targeting the SCADA system opens it up to varied level of risks and impacts. Some attacks increase the SCADA system's vulnerabilities to bigger risks.

In recent times, smart grid cybersecurity is an area that continuously receive attention in the industrial and academic world. Ideally, security should be considered more, in form of prevention, which involves detecting the attacks before they happen. NAN attacks occur in various ways and forms, including but not limited to:

- By accessing the messages sent from HAN's SM, various intimate information about residents' lifestyle and properties, such as types and number of household appliances and specific daily routine activities etc can be revealed to attackers.
- Attackers try to alter the content, sequence or/and timing of transmitted data to suit their motives.
- Attackers can create a signed and encrypted message to deceive legal receivers.
- Injecting false data and modifying/replaying the transmitted data that may destabilize the entire grid.

NIST identified integrity, availability and confidentiality as the major cyber-security requirements for SCADA systems as [48-49]

1) Integrity: Integrity is defined as the ability to verify that a transmitted message arrived at the destination node unaltered nor tampered with. It is a vital requirement whereby message/data received at either the NAN gateway or HAN gateway is a true copy of transmitted data. An antagonist having enough knowledge of the grid configuration can compromise meter measurements. Typical integrity attacks include the popular Man in the Middle (MiTM) attacks such as replay attacks. These form of attacks typically act in form of instructions changes i.e false data injection (FDI) which can result in fake state estimation thereby causing negative impact on electric power operation [43].

2) Availability: For any system to achieve its aim and objectives, the system's components must be available when needed. Availability requirements in SCADA network means that the cyber system's components for storing and processing data, the control devices and the communication channels must be available and functioning efficiently. Availability of power facilities ensures efficient service and protection against communication failures, manipulation and deceits due to failures and other various form of attacks [50].

3) Confidentiality: Confidentiality refers to the ability to avoid disclosing or interfering with the data flow by intruders or unauthorized personnel i.e ability to hide/protect data. Confidentiality requirement refers to a situation whereby only sender/receiver could access data being transmitted between nodes. Confidentiality attack focus on exploiting vulnerabilities. The SCADA systems and networks, just as any other systems have vulnerabilities that are exploitable by intruders. Typical confidentiality attacks include the popular DoS/DDoS. Distributed Denial of Service attack is a popular threat to servers, clouds and system nodes. DDoS attacks exhaust resources and hold up network bandwidth. The attacks have the capability of creating massive traffic and then spreading the attack to the whole network and causing a total shutdown [51]. In SG communication, DDoS attack can cause the flooding of the AMI network with volumetric traffic, thereby limiting resources even for legit users [52]. Estimation result showed that over 7000 DDoS attacks are succesfully launched daily, hence making DDoS a serious threat for data transmission [70]. Typical DDOS attacks that are peculiar to Smart grid AMI includes TCP SYN flooding, UDP flooding and ping flooding attacks [43,53]

Just as any other infrastructure, cyber-attacks have the capability to inflict massive damages on electricity grid. A report of the lengthy blackout in Yemen recently was attributed to rival political group who were accused of attacking transmission lines via cyber-attacks [54]. Russia was accused of bringing down Georgian critical infrastructure via cyber-attacks during Russian-Georgian war in 2008 [55]. A report from the wall street journal in 2009 stated that cyber-spies have penetrated the country's power grid [56]. In 2012, flame malware was discovered to be actively attacking many sites in Middle East and North Africa for at least two years [57]. In December 2015, cyber-attack on the Ukrainian power grid affected numerous circuit breakers thereby causing blackout to an estimated 230,000 energy users [8, 18]. Also, in January 2016, Israel's energy minister announced that the country grid was targeted successfully, hence the operators had to paralyze several grid computers [58].

V. SOLUTIONS TO CYBER-ATTACKS/FUTURE TRENDS

Addressing cyber security must not be restricted to deliberate attacks from resentful employees, industrial espionage, and terrorists. Failures attributed to human errors, equipment failures and natural causes are also feasible [42]. Utility companies in collaboration with federal agencies, such as the Department of Energy, North American Electrical Reliability Corporation-Critical Infrastructure Protection (NERC CIP) and the National Institute of Standards and Technology (NIST), via various programmes are consistently making efforts in addressing security and interoperability requirements for smart grid [39, 42]. All the mentioned organizations have various security procedures in place to cater for systems vulnerabilities. Examples of such is the USA Department of Energy (DoE) and the National Energy Technology Laboratory (NETL) project M635NL34 that involved designing cryptographic modules for SCADA data encryption [59]. Also, some of the current security solution are physical controls such as meter data authentication and encryption, tamper resistance seals on meters [38] and network control measures such as firewall/ deployed at access point [60].

However, cyber security research works in terms of attacks and their impacts are constrained due to non-availability of realistic practical and statistical data on cyber-physical

electricity infrastructure systems. Most research works on SCADA cybersecurity rely on models and testbeds developments on various simulation tools to achieve network security analysis. Numerous testbeds have been developed by various research centers, labs and varsities for monitoring, mitigating and analyzing the impacts of cyber-attacks. Examples of such testbeds include the Idaho National Laboratory SCADA testbed which was employed in investigating cyber-attack impacts using an aurora generator test [61]. Also, Sandia National Laboratory designed a virtual control system environment (VCSE) for studying impacts of cyber threats, defense training as well as exploring power system vulnerabilities [62]. A testbed was designed at the University of Arizona for simulating SCADA protection techniques against cyber-attacks [63]. Other various research works exploited commercial simulation tools, such as MATLAB, PSCAD/EMTDC, OpenDSS, PSSTMNETOMAC, NS2/3, OPNET, OMNET tools.

VI. DATA PRIVACY MEASURES

Security solutions to smart grid data privacy can be grouped into two main techniques namely; [64]:

A. Prevention techniques (Encryption & Authorization)

B. Detection techniques (Intruder Detection Scheme {IDS})

1. Prevention techniques

To prevent interception of wireless transmitted data over open channels such as the smart grid communication domains, the most effective and widely used security measure is encryption and authorization (E & A). Encryption and Authorization are popularly achieved via cryptography [30]. After the NIST announcement of AES in 2001 as the new standard encryption algorithm replacing DES and the adoption of Rijndael algorithm as the new AES for being strong security-wise, its ease of deployment on nearly all platforms, Rijndael has been favorably received and it has been continuously deployed [68]. Key management is the main issue in cryptography [22]. Conventional Symmetric and Public Key Infrastructure (PKI) [66-67] architectures are popular cryptography methods. In symmetric cryptosystems, both communicating nodes share the same key, hence making it extremely vulnerable to attackers. In PKI, each communicating node is assigned a public and private key for encryption and decryption [67]. Public key is issued by a trusted service provider [65] (TSP) otherwise known as Key Generation Center typically located at utility centers. Several E&A schemes have been proposed for SG data privacy [17, 67]. However, existing public key infrastructure schemes cannot be used efficiently for SG communications because of some drawbacks such as [69]: (1) PKI maintenance is costly, since the SG have numerous nodes (energy consumer meters), hence there is scalability issues, (2) Implementation of key recovery system is stressful. It requires a secured database of nodes key pairing, and (3) each entity is required to verify the public keys of receivers, which is arduous for SG operators.

NIST has endorsed against the deployment of PKI based cryptography for SG data privacy because PKI is costly [69].

To avoid key management issues, Identity based cryptosystem has been proposed in several literatures for SG data privacy [6, 65, 69]. Identity-based cryptography [65] concept was introduced in 1984. Just like PKI, IBC involves using a private key and a public key. The public key in IBC is taken from identities such as IP address, model number or license number, thereby eliminating certificate management issues associated with PKI schemes. The main advantage of IBC that makes it an ideal method for SG data privacy is that it simplifies key management and it does not require secured database to store key pairs. Furthermore, the cryptography type allows re-keying from message sender.

2. Detection techniques

A good security must be able to detect intruders. Intrusion detection models can be described as the second layer of security (after the prevention-based techniques might have failed). IDS can be described as the process of monitoring and analyzing the events in a network for any violation or abuse signs that is unusual [29, 70, 71]. IDS use various algorithms such as machine learning tools and prediction models to detect attacks and triggers an alarm when there is a sign of an intruder in the network. Detection techniques are categorized as [72, 73, 78]:

• Signature-based detection/ misuse detection: They detect attacks based on known template patterns i.e signature-based detection make use of the comparison between current observations of the network traffic and known attack signatures that have been previously stored.

• Anomaly-based detection employs statistical measures in performing a comparison check on the parameters of an observed traffic and a normal system behavioral traffic. Anomaly based detection simply declares the presence of an intruder once there is an observed change compared to a normal traffic.

The IDS is adjudged by many researchers as a secured way of securing the SG against attackers targeting the communication network, hence several IDS schemes [29, 75-78] have been proposed using prediction algorithms and machine learning tools etc.

VII. CONCLUSION

The fact that wireless communication technology is the future of the Smart Grid vision makes cybersecurity one of the most critical issues affecting the modernized grid. In this article, we focused on this cybersecurity issue and provided a comprehensive review on the current communication security in terms of attackers and intruders feasting and interfering with grid data. First, we review the smart grid communication layers and grid components. Then, we addressed the smart grid security challenges in terms of attacks and the solutions for the current and future grid. Finally, we identified the data privacy measures in terms of prevention techniques and detection techniques.

REFERENCES

[1] S. Aleksic, V. Mujan, "Exergy cost of information and communication equipment for smart metering and smart grids," in Sustainable Energy, Grids and Networks, vol. 14, pp. 1-11, 2018.

[2] R. Marah and A. El Hibaoui, "Algorithms for Smart Grid management," in Sustainable Cities and Society, vol. 38, pp. 627-635, 2018.

[3] S. Xu, Y. Qian and R.Q. Hu, "On reliability of smart grid neighborhood area networks" in IEEE Access, vol. 3, pp. 2352-2365, 2015.

[4] M.G. Seewald, "Benefits of end-to-end IP for cyber and physical security," in IEEE PES Transmission and Distribution (T&D) Conference and Exposition, pp. 1-6, May 2012.

[5] M. Yigit, V.C. Gungor and S. Baktir, "Cloud computing for smart grid applications," in Computer Networks, vol. 70, pp. 312-329, 2014.

[6] J. Baek, Q.H. Vu, J.K. Liu, X. Huang and Y. Xiang, "A secure cloud computing-based framework for big data information management of smart grid," in IEEE Transaction on Cloud Computing, vol. 3, no 2, pp. 233-244, 2015.

[7] K. El Defrawy and G. Tsudik," ALARM: Anonymous location-aided routing in suspicious MANETs," in IEEE Transactions on Mobile Computing, vol. 10(9), pp. 1345-1358, 2011

[8] C.C. Sun, A. Hahn and C.C. Liu, "Cyber security of a power grid: State-of-the-art," in Intl. Journal of Electrical Power & Energy Systems, vol. 99, pp. 45-56, 2018.

[9] D. Kushner, "The real story of stuxnet," in IEEE Spectrum, vol. 50, no. 3, pp. 48-53, 2013.

[10] G.I. Maldonado, "The performance of North American nuclear power plants during the electric power blackout of August 14, 2003," in IEEE Nuclear Science Symposium Conference Record, vol. 7, pp. 4603-4606, October 2004.

[11] J.W. Wang and L.L. Rong, "Robustness of the western United States power grid under edge attack strategies due to cascading failures," Safety Science, vol. 49, no 6, pp. 807-812, 2011.

[12] O. Kosut, L. Jia, R.J. Thomas and L. Tong, "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures," in IEEE Intl. Conference on Smart Grid Communications (SmartGridComm), pp. 220-225, October 2010.

[13] J. Wang, "Toward Resilience of the Electric Grid.," in Smart Cities: Foundations, Principles, and Applications, pp.535-574, 2017.

[14] M.M. Eissa, "New protection principle for smart grid with renewable energy sources integration using WiMAX centralized scheduling technology," in Intl Journal of Electrical Power & Energy Systems, vol. 97, pp. 372-384, 2018.

[15] Y.C. Chang and T.C. Huang, "An interactive smart grid communication approach for big data traffic," in Computers & Electrical Engineering, vol. 67, pp. 170-181, 2018

[16] M. Irfan, J. Iqbal, A. Iqbal, Z. Iqbal, R.A. Riaz and A. Mehmood," Opportunities and challenges in control of smart grids–Pakistani perspective," in Renewable and Sustainable Energy Reviews, vol. 71, pp. 652-674, 2017.

[17] M. Benmalek, Y. Challal, A. Derhab and A. Bouabdallah," VerSAMI: Versatile and Scalable key management for Smart Grid AMI systems," in Computer Networks, 2018.

[18] A. Hansen, J. Staggs and S. Shenoi. "Security analysis of an advanced metering infrastructure," in Intl Journal of Critical Infrastructure Protection, vol. 18, pp. 3-19, 2017.

[19] B. Asare-Bediako, W.L. Kling and P.F. Ribeiro, "Integrated agent-based home energy management system for smart grids applications", in 4th IEEE Innovative Smart Grid Technologies Europe (ISGT EUROPE), pp. 1-5, 2013.

[20] Y. Tsado, D. Lund and K.A. Gamage, "Resilient communication for smart grid ubiquitous sensor network: State of the art and prospects for next generation," in Computer Communications, vol. 71, pp. 34-49, 2017.

[21] H. Lim, J. Ko, S. Lee, J. Kim, M. Kim and T. Shon," Security architecture model for smart grid communication systems," in IEEE Intl. Conference on IT Convergence and Security (ICITCS), pp. 1-4, 2013.

[22] N. Liu, J. Chen, L. Zhu, J. Zhang and Y. He, "A key management scheme for secure communications of advanced metering infrastructure in smart grid," in IEEE Transactions on Industrial Electronics, vol. 60, no 10, pp. 4746-4756, 2013

[23] S.C. Yip, W.N. Tan, C. Tan, M.T. Gan and K. Wong, "An anomaly detection framework for identifying energy theft and defective meters in smart grids," in International Journal of Electrical Power & Energy Systems, vol. 101, pp. 189-203, 2018.

[24] M.F. Mohamed, M. El-Gayyar, A.E.R. Shabayek and H. Nassar, "Data reduction in a cloud-based AMI framework with service-replication," in Computers & Electrical Engineering, 2018.

[25] G. Wang, Y. Zhao, J. Huang and R.M. Winter, "On the Data Aggregation Point Placement in Smart Meter Networks," in 26th IEEE Intl Conference on Computer Communication and Networks (ICCCN), pp. 1-6, 2017.

[26] O.M. Longe, K. Ouahada, H.C. Ferreira and S. Rimer, "Wireless sensor networks and advanced metering infrastructure deployment in smart grid," in Intl. Conference on e-Infrastructure and e-Services for Developing Countries, Springer, Cham, pp. 167-171, 2013.

[27] M. Kuzlu, M. Pipattanasomporn and S. Rahman, "Communication network requirements for major smart grid applications in HAN, NAN and WAN," in Computer Networks, vol. 67, pp. 74-88, 2014.

[28] A. Naamane and N.K. Msirdi "Towards a smart grid communication," in Energy Procedia, vol. 83, pp. 428-433, 2015.

[29] H. Sedjelmaci and S.M. Senouci, "Smart grid Security: A new approach to detect intruders in a smart grid Neighborhood Area Network," in IEEE Intl. Conference on Wireless Networks and Mobile Communications (WINCOM), pp. 6-11, 2016.

[30] S. Alam, M.F. Sohail, S.A. Ghauri, I.M. Qureshi and N. Aqdas," Cognitive radio based smart grid communication network," in Renewable and Sustainable Energy Reviews, vol. 72, pp. 535-548, 2017.

[31] G. Wang, Y. Zhao, Y. Ying, J. Huang and R.M. Winter, "Data aggregation point placement problem in neighborhood area networks of smart grid," in Mobile Networks and Applications, pp.1-13, 2018.

[32] H.M. Nejad, N. Movahhedinia, M.R. Khayyambashi, "Improving the reliability of wireless data communication in Smart Grid NAN," in Peer-to-Peer Networking & Applications, vol. 10, no 4, pp.1021-1033, 2017.

[33] B. Subhash and V. Rajagopal, "Overview of smart metering system in Smart Grid scenario," in IEEE Power and Energy Systems Conference: Towards Sustainable Energy, pp. 1-6, March 2014

[34] V.C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati and G.P. Hancke, "Smart grid technologies: Communication technologies and standards," in IEEE transactions on Industrial informatics, vol. 7, no 4, pp. 529-539, 2011.

[35] S.V. Tiwari, A. Sewaiwar and Y.H. Chung, "Smart home multi-device bidirectional visible light communication," in Photonic Network Communications, vol. 33, no 1, pp. 52-59, 2017

[36] R. Makwana, J. Baviskar, N. Panchal and D. Karia, "Wireless based load control and power monitoring system," in IEEE Intl. Conference on Energy Efficient Technologies for Sustainability (ICEETS), pp. 1207-1211, April 2013

[37] F. Aalamifar, G.N. Shirazi, M. Noori and L. Lampe, "Cost-efficient data aggregation point placement for advanced metering infrastructure," in IEEE Intl conference on Smart Grid Communications (SmartGridComm), pp. 344-349, 2014.

[38] S. McLaughlin, D. Podkuiko and P. McDaniel, "Energy theft in the advanced metering infrastructure," in Intl. Workshop on Critical Information Infrastructures Security, Springer, Berlin, Heidelberg, pp. 176-187, September 2009.

[39] D. von Oheimb, "IT security architecture approaches for smart metering and smart grid," in Intl. Workshop on Smart Grid Security, Springer, Berlin, Heidelberg, pp. 1-25, December 2012.

[40] M. Mononen, J. Saarenpää, M. Kolehmainen, H. Niska and A. Rautiainen, "Monetary impact of dynamic pricing and demand response on households: The winners and losers," in Innovative Smart Grid Technologies Conference (ISGT), IEEE Power & Energy Society, pp. 1-5, February 2015.

[41] T. Roosta, D.K. Nilsson, U. Lindqvist and A. Valdes, "An intrusion detection system for wireless process control systems," in 5th IEEE Intl. Conference on Mobile Ad Hoc and Sensor Systems (MASS 2008), pp. 866-872, 2008

[42] A.R. Metke and R.L. Ekl, "Security technology for smart grid networks," in IEEE Transactions on Smart Grid, vol. 1, no 1, pp. 99-107, 2010.

[43] K. Shuaib, Z. Trabelsi, M. Abed-Hafez, A. Gaouda and M. Alahmad, "Resiliency of smart power meters to common security attacks," in Procedia Computer Science, vol. 52, pp. 145-152, 2015.
[44] Q. Hu and F. Li, "Hardware design of smart home energy management system with dynamic price response," IEEE Trans. Smart Grid, vol.4, no. 4, pp. 1878–1887, 2013
[45] G. Corbò, C. Foglietta, C. Palazzo and S. Panzieri, "Smart Behavioural Filter for SCADA Network," in Intl. Conference on Industrial Networks and Intelligent Systems, Springer, Cham., pp. 10-110, 2016.
[46] I. Kolosok and L. Gurina, "Calculation of cyber security index in the problem of power system state estimation based on SCADA and WAMS measurements," in Intl. Conference on Critical Information Infrastructures Security, Springer, Cham., pp. 172-177, October 2014.
[47] J. Yang, R. Yu, Y. Liu, S. Xie. and Y. Zhang, "A two-stage attacking scheme for low-sparsity unobservable attacks in smart grid," in IEEE Intl. Conference on Communications (ICC), pp. 7210-7215, 2015.
[48] L.A. Maglaras, J. Jiang and T.J. Cruz, "Combining ensemble methods and social network metrics for improving accuracy of OCSVM on intrusion detection in SCADA systems," in Journal of Information Security and Applications, vol. 30, pp. 15-26, 2016.
[49] S. Ahmed and F.M. Dow, "Electric vehicle technology as an exploit for cyber-attacks on the next generation of electric power systems," in IEEE Intl. Conference on Control Engineering & Information Technology (CEIT), pp. 1-5, 2016.
[50] T. Lu, J. Lin, L. Zhao, Y. Li and Y. Peng, "A Security Architecture in Cyber-Physical Systems: Security Theories, Analysis, Simulation and Application Fields," in International Journal of Security and its Applications, vol. 9, no 7, pp. 1-16, 2015.
[51] N. Hoque, H. Kashyap and D.K. Bhattacharyya, "Real-time DDoS attack detection using FPGA. Computer Communications," vol. 110, pp .48-58, 2017.
[52] S. Shitharth and D. P. Winston. "A Comparative Analysis between Two Countermeasure Techniques to Detect DDoS with Sniffers in a SCADA Network." Procedia Technology, vol. 21, pp. 179-186, 2015.
[53] R.C. Diovu and J.T. Agee, "Quantitative analysis of firewall security under DDoS attacks in smart grid AMI networks," in IEEE Intl Conference on Electro-Technology for National Development (NIGERCON), pp. 696-701, 2017
[54] C.Y. Ma, D.K. Yau and N.S. Rao, "Scalable solutions of Markov games for smart-grid infrastructure protection," in IEEE Transactions on Smart Grid, vol. 4, no 1, pp.47-55, 2013.
[55] M. Kenney, "Cyber-terrorism in a post-stuxnet world," Orbis, vol. 59, no 1, pp. 111-128, 2015.
[56] C. Ebinger and K. Massy, "Enhancing Smart Grid cyber security in the age of information warfare," Policy, 2011.
[57] B. Miller and D. Rowe, "A survey of SCADA and critical infrastructure incidents," in Proceedings of the 1st Annual conference on Research in information technology (ACM), pp. 51-56, 2012.
[58] Y. Ding and J. Liu, "Real-time false data injection attack detection in energy internet using online robust principal component analysis," in IEEE Intl. Conference on Energy Internet and Energy System Integration (EI2), pp. 1-6, November 2017.
[59] P.E. Weerathunga, "Security Aspects of Smart Grid Communication" 2012
[60] N. Beigi-Mohammadi, J. Mišić, H. Khazaei and V.B. Mišić, "An intrusion detection system for smart grid neighborhood area network," in IEEE Intl. Conference on Communications (ICC), pp. 4125-4130, 2014.
[61] J.L. Rrushi, "SCADA protocol vulnerabilities," in Critical Infrastructure Protection, Springer, Berlin, Heidelberg, pp. 150-176, 2012.
[62] M. McDonald, J. Mulder, B. Richardson, R. Cassidy, A. Chavez, N. Pattengale, G. Pollock, J. Urrea, M. Schwartz, W. Atkins and R. Halbgewachs, "Modeling and simulation for cyber-physical system security research, development and applications" Sandia National Laboratories, Tech. Rep. Sandia Report SAND2010-0568, 2010.
[63] M. Mallouhi, Y. Al-Nashif, D. Cox, T. Chadaga and S. Hariri, "A testbed for analyzing security of SCADA control systems (TASSCS)," in IEEE PES in Innovative Smart Grid Technologies (ISGT), pp. 1-7, 2011.
[64] V.V. Vineeth, N. Radhika and V. Vanitha, "Intruder Detection and Prevention in a Smart Grid Communication System," in Procedia Technology, vol. 21, pp. 393-399, 2015.
[65] E. U. Soykan, S.D. Ersoz and G. Soykan, "Identity based signcryption for advanced metering infrastructure," in Smart Grid Congress and Fair (ICSG), pp. 1-5, 2015.
[66] C. Adams and S. Lloyd, "Understanding PKI: concepts, standards, and deployment considerations," Addison-Wesley Professional, 2003.
[67] T. Baumeister, "Adapting PKI for the smart grid," in IEEE Intl. Conference on Smart Grid Communications (SmartGridComm), pp. 249-254, 2011.
[68] W. E. Burr, "Selecting the advanced encryption standard," in IEEE Security & Privacy, vol. 99, no 2, pp.43-52, 2003.
[69] Z. Wang, "An Identity-Based Data Aggregation Protocol for the Smart Grid," IEEE Transactions on Industrial Informatics, vol. 13, no 5, pp. 2428-2435, 2017.
[70] C.W. Ten, J. Hong and C.C. Liu, "Anomaly detection for cybersecurity of the substations," IEEE Transactions on Smart Grid, vol. 2, no 4, pp. 865-873, 2011.
[71] R. Berthier, W.H. Sanders and H. Khurana, "Intrusion detection for advanced metering infrastructures: Requirements and architectural directions," in IEEE Intl Conference on Smart Grid Communications (SmartGridComm), pp. 350-355, 2010.
[72] R.B. Blazek, H. Kim, B. Rozovskii and A. Tartakovsky, "A novel approach to detection of denial-of-service attacks via adaptive sequential and batch-sequential change-point detection methods," in Proceedings of IEEE Systems, Man and Cybernetics Information Assurance Workshop, pp. 220-226, June 2001.
[73] S. Otoum, B. Kantarci and H.T. Mouftah, "Mitigating False Negative intruder decisions in WSN-based Smart Grid monitoring," in 13th IEEE Wireless Communications and Mobile Computing Conference (IWCMC), pp. 153-158, 2017.
[74] A. Usman and S.H. Shami, "Evolution of communication technologies for smart grid applications," in Renewable and Sustainable Energy Reviews, vol. 19, pp. 191-199, 2013.
[75] A. Almalawi, X. Yu, Z. Tari, A. Fahad and I. Khalil, "An unsupervised anomaly-based detection approach for integrity attacks on SCADA systems," in Computers & Security, vol. 46, pp. 94-110, 2014.
[76] S. Parthasarathy and D. Kundur, "Bloom filter-based intrusion detection for smart grid SCADA," in 25th IEEE Canadian Conference on Electrical & Computer Engineering (CCECE), pp. 1-6, 2012.
[77] M. Attia, S.M. Senouci and E.H. Aglzim, "New optimization and security approaches to enhance the Smart Grid performance and reliability," in IEEE Intl. Conference on Network of the Future (NOF), pp. 1-3, 2016
[78] S. Otoum, B. Kantarci and H.T. Mouftah, "Detection of Known and Unknown Intrusive Sensor Behavior in Critical Applications," in IEEE Sensors Letters, vol. 1, no 5, pp.1-4, 2017