Smart Grid Cyber Security: Challenges and Solutions

Salsabeel Shapsough, Fatma Qatan, Raafat Aburukba, Fadi Aloul, A. R. Al Ali
Department of Computer Science & Engineering
American University of Sharjah, UAE

***Abstract*— Cyber security in smart grid systems is becoming a major concern throughout the grid communication networks and software platforms that operate and manage the entire grid. The smart grid networks characteristics such as heterogeneity, delay constraints, bandwidth, scalability, and others make it challenging to deploy uniform security approaches all over the networks segments. Therefore, more research is required to develop standards and techniques that meet the smart grid network requirements at a low cost. In this paper, we discuss some of the existing cyber security issues in smart grid networks, highlight some of the latest solutions, and propose a new security conceptual model based on the Internet of Things paradigm.**

***Index Terms*—Smart Grid, Cyber Security, Networks, IOT**

I. Introduction

SMART grid research and development are gaining momentum as the grid role from conceptual model to deployment phase. The National Institute of Standards and Technology (NIST) described the smart grid as the integration of the last century power grid with the current century development in information and communication technologies (ICT)[1][2]. Such integration empowers utility, ICT developers and consumers to operate the grid efficiently by installing distributed and mixed renewable energy resources near the consumption premises [3][4][5]. In the smart grid, power flow is bidirectional, i.e. consumers and utility can exchange power by utilizing two-way communication networks [6][7]. Utility companies are not anymore the prime owner of the power grid. As projected in the NIST conceptual model, the smart grid has seven domains namely: bulk generations, transmission, distribution, consumption, service provider, operations and markets [1][8]. Technical shareholders of the grid utilize several layers of communication networks and software packages to manage the grid efficiently. For example IBM has introduced smart grid model that elaborates more on the communication networks, storage and computing platforms Infrastructure as a Service (IaaS) as well as software packages as services (SaaS) [9]. Such characterization provides better customization in terms of device communication needs, mainly: bandwidth, latency, resiliency, security, and protocol capacity.

S. Shapsough is with the Department of Computer Science & Engineering, American University of Sharjah, UAE. (e-mail: g00041619@aus.edu).
F. Qatan is with the Department of Computer Science & Engineering, American University of Sharjah, UAE. (e-mail: g00059135@aus.edu).
R. Aburukba is with the Department of Computer Science & Engineering, American University of Sharjah, UAE. (e-mail: raburukba@aus.edu).
F. Aloul is with the Department of Computer Science & Engineering, American University of Sharjah, UAE. (e-mail: faloul@aus.edu).
A. R. Al-Ali is with the Department of Computer Science & Engineering, American University of Sharjah, UAE. (e-mail: aali@aus.edu).

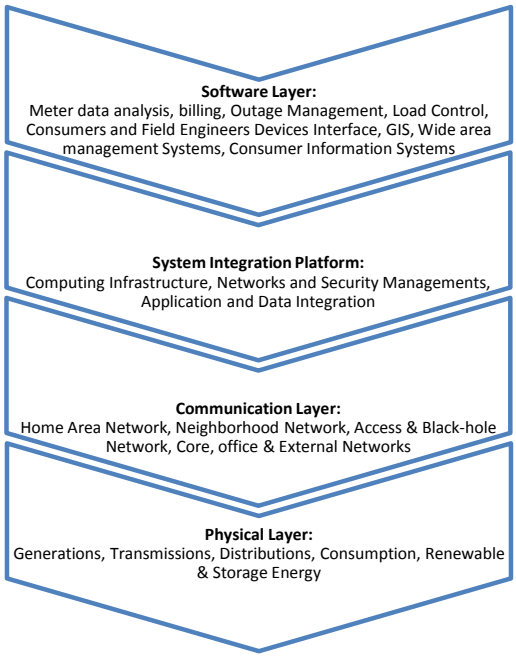

Figure 1: Smart Grid Conceptual Model

Figure 1 mimics the IBM model within the NIST conceptual model context [9]. With closer look to the IBM model one can find that the ICT layers constitute around 70% of the smart grid infrastructure [10].

As shown in the communications layer, there are different types of communication networks. Some maybe wired and others maybe wireless and can cover short or long areas. The software layer also consists of several different software packages to operate the grid.

Many operators, homeowners, workforce field engineers, service providers and marketing staff require access to the operating software packages and tools via many access points. Such access imposes serious cyber security threats that require authentication and authorization to protect the grid from any cyber-attacks.

This paper presents a survey on the cyber security challenges and existing solutions within the smart grid environment. The rest of this paper is organized as follows. Section II presents security requirements and objectives in the smart grid. Section III presents the security challenges in smart grids. Section IV surveys approaches related to the smart grid security challenges. Finally, Section V discusses open issues and recommendations and Section VI concludes the paper.

II. Security Requirements and Objectives

Smart grid is composed of a large number of interconnected devices. There are two types of data that are exchanged throughout the smart grid namely *information* data and *operational* data. Information maybe the power consumption bill, trending, logging, tagging, historical reporting geographical locations, consumers' information and emails [11]. Operational data could be real time current and voltage values, transformer tap changers, capacitors banks, transformer feeders' current loads, fault locations, relays status, circuit breakers status [11][12][13]. Operational data requires a high level of security to protect the smart grid systems from any vulnerability and attack that may cause power blackout.

The security requirements and objectives in the smart grid are:

- **Availability**: Accessing information in a timely in the smart grid. Loss of availability could affect the power delivery since access to authorized individuals might be denied. Attacks targeting the system availability are considered Denial of service attacks (DOS) which aim to disturb the data transfer in order to make the resources unavailable.
- **Integrity**: Preventing an unauthorized modification of information or system by illegitimate users. Loss of integrity in the smart grid might modify sensors values and products recipes which in turn can affect the power management.
- **Confidentiality:** Preventing unauthorized users from accessing information in order to protect personal privacy and safety. Smart grid networks carry information that varies in privacy and sensitivity levels; from consumption information all the way to consumer private information.
- **Authentication:** Validating the true identity of the communicating parties. Authentication of humans and machine is of high importance, and a weakness in it can lead to an attacker gaining access to private information, or an illegitimate devices making use of the smart grid resources.
- **Authorization:** Providing permission and granting access to a system (also known as access control). The variety of devices and humans that exist in a smart grid network requires an authorization system in order to provide proper management of information and resources.
- **Non-Repudiation**: Assuring that a certain action performed by a system or user can't be later denied. Non-repudiation becomes a major issue when valuable resources and information are involved.

III. Security Challenges in the Smart Grid

Smart grid is vulnerable to various threats and challenges. In this section, various cyber security challenges are addressed.

- **Connectivity:** The communication network in the smart grid is sophisticated as it combines a large number of devices that interoperate. Given the nature of the smart grid environment being decentralized, the systems require a high level of protection against attacks and vulnerabilities. Attacks can lead to physical damage, black-outs and lack of efficiency. This is because, attackers gain control of the system [14].
- **Trust:** Consumers are no longer assumed trustworthy due to the high connectivity of the smart grid systems which affected the design decisions. Some consumers will not adhere to the policies and agreements. For instance, users might intentionally damage the smart meter to report false data about the power consumption to save money.
- **Customer's Privacy:** Ensuring consumer's privacy is an important aspect in any system including the smart grid that should be well protected and preserved. The introduction of smart meter into the smart grid brought many challenges related to user's information privacy. Besides reporting back some essential information about user's power consumption, smart meter could compromise the user's privacy which is a critical. Since it could use the information received at the service provider to infer the behaviors of the users. The collected data about customers include information about the time they are available at home or travelling. It can even extract information about some daily activities such as sleeping, watching television or even what appliances they are using. Criminals who plan to commit a crime, business, marketers who want to advertise or even competitors are interested in the extracted data. So, data should be protected during the transmitting and the storage process to prevent unauthorized access to data in order to protect the user's privacy [15].
- **Software Vulnerabilities:** Software suffers from a wide variety of vulnerabilities that include malwares. Supervisory control and data acquisition (SCADA) systems composed of general purpose technology that introduces the risk of malwares and malicious updated. General purpose system suffers from a various well known vulnerabilities that should be patched to ensure that the system stay updated. On the other hand, patching is considered a difficult process especially in critical systems like the smart grid because it is very expensive and it could lead to downtime [14].

IV. Solutions to the Smart Grid Security

Cyber security in the smart grid is a crucial issue that attracted the attention of researchers and industry professionals. While some solutions were proposed to solve security issues in the smart grid, vulnerabilities still exist. This section surveys existing solutions and methods that address the cyber security issues in the smart grid.

A. Network Security

Denial of Service (DoS) is the most common attack in the smart grid network. When launched against any system, its main goal is to make the system unable to function as intended. Lots of attention is given to this type of attack. Handling DoS attacks in smart grid networks is usually done by: DoS Detection and DoS Mitigation [16].

1) DoS Detection

Smart grid systems must detect DoS attacks as they happen in order to apply appropriate counter measures. Detection is important with Distributed DoS (DDoS) attacks, where detection methods that target a source IP address is not an option. Several methods have been developed which attempt to

detect DoS attacks through the packet content, attack pattern, and other properties. Some recent methods are:

- **Using Flow Entropy:** Several recent studies in the field of DoS detection focus on using probabilistic approaches to analyze traffic in order to detect a DoS attack. The methods presented in [17][18][19] suggest sampling packets and measuring flow entropy to detect an attack. The router would sample one of every five packets to construct a flow, and then calculate measures of entropy such as the average entropy, and entropy of the source, as well as the number of packets per second. The router would then compare the measured values with known threshold values to decide if it was under attack.
- **Using Signal Strength:** Measuring signal strength to detect an attack is usually done by wireless devices. By measuring signal strength level or ambient energy, a device can decide if it is receiving legitimate data, or it is under a jamming attack. However, since every device comes with its own properties such as receiver sensitivity and noise threshold, it is not possible to assign a unified strength value for jamming attacks. Therefore, the decision has to be made at each device using empirical methods, which may sometimes come across as a flaw in the method. A jamming attack can take one of two forms; the attacker can either choose to send a continuous, amplified signal to jam the channel, or can send a noise-like signal. The detector must be able to develop two models to detect either. Another approach is to check the decoder output for signals that are strong enough to be detected. If the signal level is at one which should be decodable, but the decoder cannot make out a meaningful, there is a possibility of a jammer [20].
- **Using Sensing Time Measurement:** Carrier Sense Multiple Access (CSMA) is a popular multiple access techniques in wireless networks. In CSMA, a transmitter senses the channel to confirm that it is free before proceeding to send data. In case of a jamming attack, the sensing time will be long and the channel will never be free. Every time the transmitter attempts to send data, it will record the sensing time. Once the time hits a threshold, the transmitter will declare it as a DoS attack [21].
- **Using Transmission Failure Count:** This is a technique to detect jamming attack to keep track of transmission failure. This is done either at the transmitter or at the receiver. A jammer can cause transmission failure, or corrupt the transmitted packet. If the number of failures hits a certain threshold, the transmitter or the receiver can consider it a jamming attack [21].
- **Using Signatures:** DoS attack signatures are usually constructed using known attack patterns and characteristics. Any suspicious activity is compared to the signatures, and a match results in a DoS detection [20].

2) DoS Mitigation

Once a DoS attack has been detected, smart grid systems should be able to take appropriate actions within a short period in order to protect the nodes and minimize the outage time. Attack mitigation counter measures in smart grid networks are usually deployed at two layers: the Network layer, and the Physical layer. This is because DoS attacks can be in two forms: 1) DoS attacks exhausting the victim's resources, 2) DoS attacks trying to disrupt the communication over the network.

DoS attack mitigation on the network layer can be done through one or more of the following methods:

- **Pushback:** Once an attack has been detected at the victim side, characteristics of the attacker such as source IP address or pattern is pushed back to the upstream router. The router then blocks all traffic that matches the characteristics [20].
- **Rate Limiting:** Once an attack has been detected, the router limits the data rate allowed for a certain user. This method is used when the detector decides that the user is performing a DoS attack, but the false detection rate is high. In case the user is a legitimate user, then they can complain and the data rate can be raised again. Otherwise, limiting the rate can reduce the effectiveness of an attack.
- **Filtering:** The router filters the source IP of a suspicious packet against a detector's blacklist. If a match is found, the packets are immediately filtered out in order to make space for legitimate packets to go through.
- **Reconfiguration:** This is done by changing the topology of the network in order to dedicate more resources to a victim, or isolate an attacker. However, due to the current network implementation and hardware used in smart grid systems, this method is rarely used as it is very expensive.
- **Cleaning Center:** A hybrid of filtering and reconfiguration. Once an attack has been detected at one node, the traffic is directed to a "cleaning center", which is a particular node in the network that is capable of performing filtering, in addition to several other functionalities [20].
- **Physical Layer Mitigation:** DoS attacks on the physical layer level usually take the form of frequency jamming. In order to mitigate such attacks some of the employed algorithms are: Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS), and Chirp Spread Spectrum (CSS).

Those methods focus on similar a fundamental issue which is transmitting data on multiple frequencies depending on a certain sequence that has been agreed on by the transmitter and receiver. If the attacker is to acquire the sequence, the methods are no longer valid. For this reason, uncoordinated versions of the aforementioned methods are developed, where the sequence is further-randomized, and a new sequence is generated for every new transmission [22][23]. Frequency hopping technologies are already used in light-weight communication protocols such as Bluetooth and Zigbee.

B. Data Security

Another level of securing a smart grid network is by providing data protection and object authentication. Cryptography methods and algorithms are used to encrypt data in order to secure communication, protect user information, and to authenticate users in order to prevent attacks against data integrity.

In encryption, both Symmetric Key encryption and Public Key encryption are used in smart grid networks. While symmetric key requires lower computing capabilities, public key has been proven to be more secure and is easier to implement when it comes to key management. However, due to the variation of computational capability of devices across

smart grid networks, which range from simple sensors to smart phones and computers, both types of encryption are used. The choice of which type of encryption to use in a certain part of the network depends on factors such as computation capability, time contains, and data-criticality.

As for authentication, certain requirements have to be met. These requirements [14] include: High efficiency, Tolerance to faults and attacks, and the Support for multicast. The support for multicast relates to one of the most important component in the smart grid networks. Since a smart grid network handles energy monitoring, generation, and distribution, multicast provides the means for fast delivery of mass messages, such as those requiring routing of power to a certain target, or immediate breaking of a power circuit.

Authentication for multicast applications can be done through one of the following methods:

- **Secret-info asymmetry:** each transmitter uses a different key to authenticate itself at each receiver. The transmitter creates a message, appends all receivers' authentication keys, and then sends the message through multicast. The downside of this method is system overhead. The authentication information is considered redundant data, and as the size of the network grows, the throughput continues to decrease due to the number of keys required.
- **Time asymmetry:** the transmitter first sends the message, and then creates a temporary authentication key. The transmitter only sends the key after the message has been received by all nodes. This way, if an attacker sniffs the key, they will not be able to use it.
- **Hybrid asymmetry:** this method incorporates both secret-info asymmetry and time asymmetry by creating different temporary keys for every transmission.

C. Key Management

Key management plays a significant role in authentication and encryption to achieve a secure system. It is categorized into public key infrastructure (PKI) and symmetric key management. PKI technology ensures the security by verifying the true identity of the party through receiving a certificate from the certificate authority (CA) before establishing any communication. Symmetric key management is used in symmetric cryptography which is composed of key generation, key distribution, key storage and key update.

The advantage of symmetric key management over the PKI is the speed and efficiency. However, due to the criticality of smart grid information, and the differences in computing capability between smart grid objects, new approaches were proposed to the key management issue [6]. The first step was to identify smart grid key requirements which include:

- **Secure management:** In order to provide confidentiality and integrity.
- **Scalability:** Because of the large scale of the smart grid network, key management has to take into account the number of objects that share keys, and the distance they cover.
- **Efficiency:** In terms of computation, storage, and communication.
- **Evolve-ability:** The smart grid network consists of new cutting-edge technologies as well as legacy systems. Key management protocols are to accommodate existing devices, as well as to evolve to accommodate future technologies.

Despite the number of technologies, methods, and protocols available for smart grid network designers, the problem of achieving security in real-time and reduced cost remains unresolved. For this reason, research has extended into handling such problems at lower layers in the smart grid system; mainly at the physical layer.

Recent techniques such as physical layer authentication allow for fast authentication and add little to no overhead [6]. Physical layer authentication can be performed on the signal by altering either the modulation scheme of the physical signal, or by the characteristics of the signal and transmission channel. Although such technologies are still prone to errors, they introduce new means of authentication that can be further developed in order to meet the requirements of the smart grid.

D. Network Security Protocols

The design of secure network protocols and architecture plays an important role in smart grid security. Some of the existing smart grid systems use internet-based protocols for secure communication such as IPSec and TLS. However, since the smart grid requirements differ from classical data networks, many smart grid systems use protocols and standards that are more suitable. Such protocols include: Secure DNP3 and IEC61850 & IEC62351. Both protocols modify existing smart grid communication protocols by adding security layers to the architecture. Those protocols are used for end-to-end communication in the smart grid such as communication between different sensors.

Data-aggregation on the other hand, communicates data from sensors to the application layer. It has a different process that requires a set of protocols due to overhead and security requirements.

To have a secure architecture, smart grid networks are built using one of two architectures [6]:

- **Trust computing-based architecture:** Where the task of authenticating objects is distributed throughout the system, and all objects participate in authenticating each other by assigning trust levels.
- **Role-based network architecture:** Where a network is divided to sub-domains and each domain has a number of devices that take on certain roles and privileges.

E. Compliance Checks

Compliance checks is done via automated tools that run checks across all components in the system to ensure that configurations of each component are up to standards of secure mitigation and protection. The tool can also point out weaknesses that need attention. This is important because in a critical system such as the smart grid, a fault in one component can cause a huge security breach. Therefore, compliance check tools are highly recommended [24].

V. Open Issues and Recommendations

Despite the abundance of protocols, compatibility remains a challenge given the heterogeneous nature of smart grid environment. In such environment, high-level sophisticated computers are exchanging information with simple, low-computing, low-power devices. As explained in the IBM model [9], the data aggregation can cause security vulnerabilities because the features in one protocol cannot be perfectly translated into another.

The current movement towards IPv6 over Low power Wireless Personal Area Networks (6LoWPAN) can be the key to solving some of the current weaknesses in the smart grid model [25][26]. The proposed recommendation in this work suggests migrating to a purely-IPv6 system. By using IPv6 to address the various objects in the system, and using IP-based communication and security protocols. We suggest a system that is similar to the IBM model except for one difference; there is only one segment for the communication layer. All the devices would have a direct connection to the internet, and thus data coming from edge devices would not have to be aggregated through multiple devices in order to arrive at the application layer, but can be sent directly through WiFi or 4G network as shown in Figure 2. This recommendation requires thorough research in order to be applied in real-life systems, however, we believe similar contribution of the 6LoWPAN within the Internet of Things (IoT); can be applied to the smart grid.

Utilizing the IoT requires a large number of IP addresses. This is not an issue as the IPV4 is extending from 32-bits to 128-bits address size IP addresses. The IPV4 can address up to 2^{32} devices (4-billion unique addresses). Moreover, IPV6 can address up to 2^{128} (Trillions of unique addresses) [25][26].

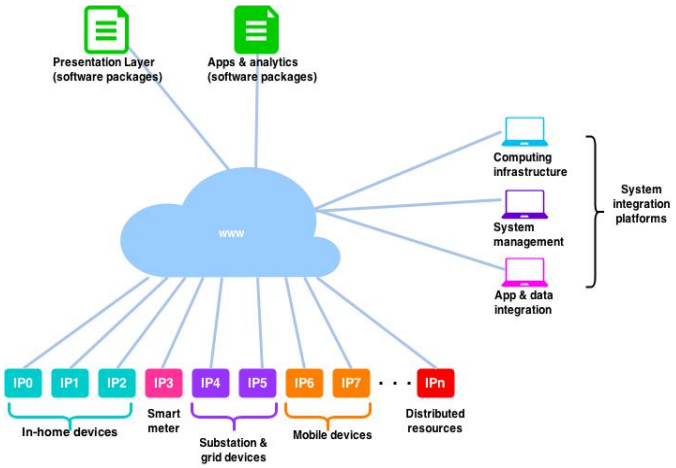

Figure 2: Proposed Smart Grid Model

VI. Conclusion

Cyber security in the smart grid is a critical issue that received attention of researchers and industry professionals. In this paper, we surveyed architecture models proposed for the smart grid. We also summarized the security requirements and challenges of the smart grid and we briefly addressed existing security solutions. Cyber security in the smart grid is still under research and needs more investigation to overcome the vulnerabilities and threats.

References

[1] NIST, Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security. *http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf*

[2] R. Apel, "Smart Grid Architecture Model: Methodology and Practical Application," in Workshop of Electrical Power Control Centers, 2013.

[3] H. Brown, S. Suryanarayanan, S. Natarajan, and S. Rajopadhye, "Improving Reliability of Islanded Distribution Systems With Distributed Renewable Energy Resources," IEEE Trans. on Smart Grid, 3(4), pp. 2028–2038, 2012.

[4] M. Miller, M. Johns, E. Sortomme, and S. Venkata, S. "Advanced integration of distributed energy resources" in Power and Energy Society General Meeting, pp. 1-2, July 2012.

[5] R. Morales Gonzalez, B. Asare-Bediako, J. Cobben, W. Kling, G. Scharrenberg, and D. Dijkstra, "Distributed energy resources for a zero-energy neighborhood," in 3rd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies, pp.1-8, 2012.

[6] W. Wang and Z. Lu, "Cyber security in the Smart Grid: Survey and challenges," Computer Networks, 57(7), pp. 1344-1371, 2013.

[7] W. Wang, "A survey on the communication architectures in smart grid," Computer Networks, vol. 55, no. 15, pp. 3604-3629, 2011.

[8] G. F. Reed, P. A. Philip, A. Barchowsky and C. J. Lippert, "Sample survey of smart grid approaches and technology gap analysis," in Innovative Smart Grid Technologies Conference Europe, 2010.

[9] G. Garner, "Designing Last Mile Communications Infrastructures for Intelligent Utility Networks (Smart Grid)," IBM Intelligent Utility Network (IUN) Communication Services, 2010.

[10] Claudio Lima, "An Architecture for the Smart Grid," in IEEE P2030 Smart Grid Comm. Architecture SG1 ETSI Workshop, pp. 1-27, 2011.

[11] H. Naidua and K. Thanushkodib, "Recent Trends in SCADA Power Distribution Automation Systems," in Bangladesh Journal of Scientific and Industrial Research, 45(3), pp. 205-218, 2010.

[12] A. Rezai, P. Keshavarzi, and Z. Moravej, "Secure SCADA communication by using a modified key management scheme," ISA Transactions, 52(4), pp. 517-524, July 2013.

[13] E. Knapp and R. Samani, "Security Models for SCADA, ICS, and Smart Grid," in Applied Cyber Security and the Smart Grid, ch. 5, 2013.

[14] M. B. Line, I. A. Tondel and M. G. Jaatun, "Cyber security challenges in Smart Grids," in 2nd IEEE PES International Conference and Exhibition , Innovative Smart Grid Technologies (ISGT Europe), Manchester, 2011.

[15] H. Khurana, M. Hadley, L. Ning and D. A. Frincke, "Smart grid security issues," IEEE Security & Privacy, 7(1), pp. 81-85, 2010.

[16] NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3, Nat'l Institute of Standards and Technology, 2014.

[17] J.-H. Jun, D. Lee, C.-W. Ahn and S.-H. Kim, "DDoS Attack Detection Using Flow Entropy and Packet Sampling on Huge Networks," in the 13th International Conference on Networks, Nice, 2014.

[18] G. Meng and N. Wang, "A Network Intrusion Detection Method Based on Improved K-Means Algorithm," Advanced Science and Technology Letters, 53(1), pp. 429-433, 2014.

[19] S. Shin, S. Lee, H. Kim and S. Kim, "Advanced probabilistic approach for network intrusion forecasting and detection," Expert Systems with Applications, 40(1), pp. 315-322, 2013.

[20] D. Lin, "Network Intrusion Detection and Mitigation against Denial of Service Attack," WPE-II Report, Univ. of Pennsylvania, Apr. 2013.

[21] W. Xu, W. Trappe, Y. Zhang and T. Wood, "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks," in 6th ACM Int'l Symposium on Mobile Ad Hoc Networking and Computing, 2005.

[22] C. Popper, M. Strasser and S. Capkun, "Anti-Jamming Broadcast Communication using Uncoordinated Spread Spectrum Techniques," IEEE J. on Selected Areas in Comm., 28(5), pp. 703-715, 2010.

[23] E. K. Lee, M. Gerla and S. Y. Oh, "Physical Layer Security in Wireless Smart grid," IEEE Comm. Magazine, 50(8), pp. 46-52, 2012.

[24] M. Kammerstetter, "Architecture-Driven SMART GRID Security Management," in ACM Workshop on Information Hiding and Multimedia Security, 2014.

[25] V. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. Hancke, "A Survey on Smart Grid Potential Applications and Communication Requirements," IEEE Trans. on Industrial Informatics, 9(1), pp. 28-42, 2013.

[26] Z. Huang and F. Yuan, "Implementation of 6LoWPAN and Its Application in Smart Lighting," Journal of Computer and Communications, vol. 3, pp. 80-85, 2015.