# Smart Grid Security Concepts and Issues

Mustafa Saed, Kevin Daimi, Nizar Al-Holou

***Abstract*— The smart grid is a new technology using innovative and sophisticated methods of electrical transmission and distribution in order to provide excellent electrical services to customers. It is a two-way communication system that allows users to manage their energy service, as well as access smart grid convenience features, such as using energy when it is at low cost, reading current consumption electricity bills online, scheduling turning on/off home appliances, and managing alternative energy sources. These conveniences, however, introduce risks to the smart grid system, increase the possibility of cyberattacks, and cascade failures propagating from one system to another. The security of the smart grid is very critical. The intend of this paper is to survey the attempts that have been made to tackle smart grid security, and to present the security approaches necessary to enforce tough security measures that fully protect the smart grid infrastructure.**

***Index Terms*— Smart Grid, Electrical Service, Security, Vulnerabilities**

## I. Introduction

THIS smart grid is a new technology that uses new and sophisticated techniques for electrical transmission and distribution in order to provide excellent electrical service to customers, and allow them to manage their electricity consumption in a two-way communication [1]. This communication network will be constructed to enable new energy services, such as real-time pricing, load shedding, and consumption management. It also enables cost saving resulting from peak load reduction and energy efficiency, integration of plug-in hybrid electric vehicles for grid energy storage, and the integration of distributed generation including photovoltaic systems and wind turbines. The new network will be created using various communication paths including fiber optic cable, hybrid fiber coax, twisted pair, wireless technology, and broadband over power line. These types of communication networks are all currently operating in the electric grid but are not yet implemented to the extent required for enabling the smart grid.

The smart grid incorporates many resources, applications, and enabled technologies. Resources are the devices that may affect supply, load, or grid conditions, including delivery infrastructure, information network, end-user systems, and related distributed energy resources. Applications are operational strategies that use resources to create benefits or values. Enabled technologies are essential crosscutting elements of the smart grid that facilitate many resources and applications. They include smart meters, standards, and protocols [2].

Figure 1 shows the dual infrastructures (the power system and the information system of smart grid). It demonstrates network connections that can be traced from the customer's premises to collector nodes. These connections are traced to the utility control center and to transmission and distribution substations where the electronic controllers are located.

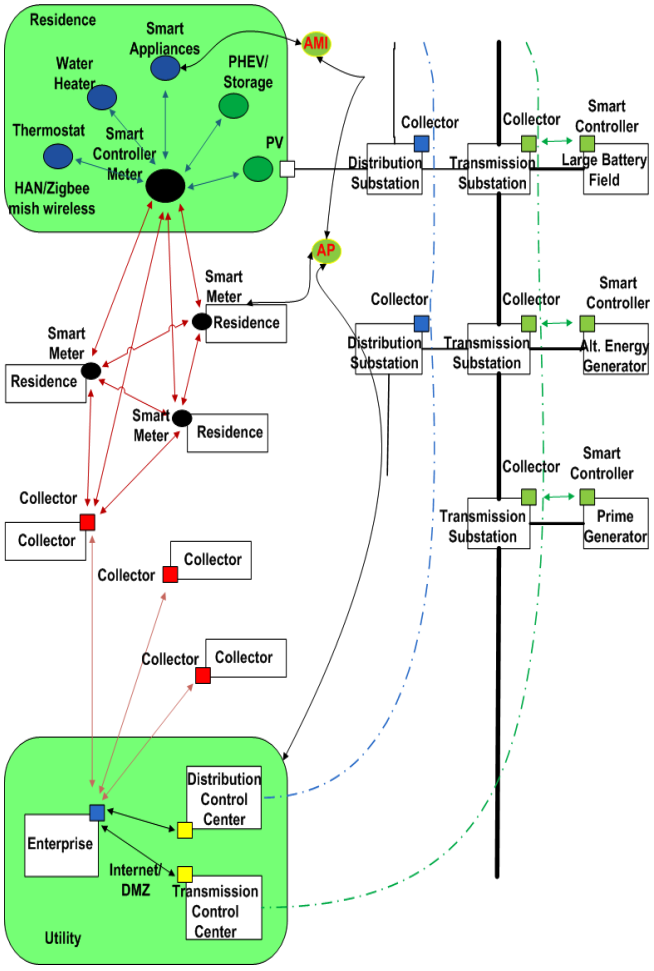


Fig. 1. A block diagram for typical smart grid

The electronic controllers manage the generation and flow of electrical power. The residence block in the figure represents the home area network that may include communicating smart grid components, such as a smart thermostat, smart water heater, smart appliances, plug-in hybrid electric

Manuscript received February 13, 2013; revised March 11, 2013.

M. Saed is with the Department of Electrical and Computer Engineering, University of Detroit Mercy, Detroit, MI 48221 USA (phone: 313-993-1060; fax: 313-993-1187; e-mail: saedma@udmercy.edu).

K. Daimi is with the Department of Mathematics, Computer Science, and Software Engineering, University of Detroit Mercy, Detroit, MI 48221 USA (e-mail: daimikj@udmercy.edu).

N. Al Holou is with the Department of Electrical and Computer Engineering, University of Detroit Mercy, Detroit, MI 48221 USA (e-mail: alholun@udmercy.edu).

ISBN: 978-988-19252-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

vehicle/storage, and photovoltaic. Note that the home area network devices are connected to a smart controller/meter through a network, such as Zigbee or mesh wireless.
It may also communicate with the home area network located nearby. Collector nodes communicate with the utility through common communication mechanisms, including the Internet. In addition, they communicate with intranet communication paths within the utility premises, including a Demilitarized Zone (DMZ) which is designed to prevent the flow of unauthorized messages. The distribution and transmission control centers have legacy communication paths and additional smart grid communication paths [3].
Some signals travel with various vulnerabilities to many end-user devices through media networks, such as controlling and monitoring. In addition, concerns have been raised regarding the resistance of the smart grid and how it repairs itself without resulting in equipment or infrastructure damage, or blackout.
Through information technology, the smart grid allows customers to manage their energy services and access smart grid convenience features. However, this can cause damage to the smart grid system and increase the possibility of cyberattacks and cascade failures propagating from one system to another [4]

The rest of the paper is organized as follows: Section 2 focuses on the possible vulnerabilities in smart grid. Section 3 discusses smart grid security issues. Smart grid security requirements and smart grid security approaches are presented in sections 4 and 5 respectively. The future of smart grid security is introduced in section 6. Finally section 7 concludes the paper.

## II. Vulnerabilities in Smart Grid

In this section, the four major classes of the vulnerabilities and their specific description are addressed. These classes create significant risks and open the door to various cyberattacks [5].

### A. Class 1: People, policy and procedure

Lacking the needed training and not abiding by policy and procedures lead the system to various risks and security issues. As a result, stakeholders should be trained on how to avoid the risks by following the security requirements. In addition, they should have a specific level of access to the system, depending on their technical responsibilities.
i. Training: Every person should be trained on security awareness based on their technical responsibilities to avoid cyberattacks. Inadequate security training and awareness programs are critically related to security problems.
ii. Policy & Procedure: Insufficient identity validation and background check will result in various security breaches. Background checks and using known references to identify the person who works on a specific program with high level of security must be enforced.
iii. Risk Management: Inadequate periodic security audits gives rise to missing critical security holes, risks, and future attacks. The system should have a periodic check on the policy and level of security access to avoid future internal and external attacks.

### B. Class 2: Platform Software/Firmware Vulnerabilities

The software and firmware in the system are responsible for protecting the system from unauthorized access by people, who are trying to intrude the system and tamper with databases and other information. For any application that needs to be applied in the smart grid, the secure software development life cycle should be taken into consideration. This will help to avoid the lack of oversight in this area and mitigate possible vulnerabilities to achieve the security as described below.
i. Authentication Vulnerability: All users, applications, and devices need to be authenticated for any kind of communication to avoid the authentication bypass vulnerability, which keeps the smart grid system in under attack situations.
ii. Authorization Vulnerability: The system should give users a level of access to the needed specific data depending on their technical responsibilities. This will allow the authenticated entities the ability to perform actions that the policy allows.
iii. Cryptographic Vulnerability: The system shall support cryptography to prevent unauthorized people from reading the encrypted data. The use of cryptography will also lead to achieving the confidentiality, integrity, and availability of the system.
iv. Input and Output Validation: The input validation allows the user to evaluate the content of the data, and provide the expected information. However, any failure in validating the external input will cause faulty system behavior. The output validation allows the system to encode the data during the communication between the components. Failure in the output validation allows the hacker to read the data and to send the wrong commands to the system resulting in unexpected behavior.
v. Password Management Vulnerability: The password is a way to achieve authentication in the system. The system should have a way to secure the password from others, except the authorized personnel, in order to achieve integrity and privacy [6].
vi. Link Vulnerability: The system shall protect and prevent users from using insecure links to avoid tracking path attack.
vii. Protocol Errors: The system should be based on strong security functions in order to protect the communication protocols. Otherwise, the system will definitely be opened to cyberattacks.
viii. Buffer Overflow: Buffer overflow occurs when a program attempts to input more data in the buffer than its capacity or when trying to input data in memory. This will cause the software using Industrial Control Systems (ICS) to face this vulnerability [5].
ix. Use of Insecure Protocols: This vulnerability deals with the insecure communication protocols, such as Distribution Network Protocols version 3 (DNP3), Modbus, Inter-Control Center Communications Protocol/Telecontrol Application Service Element 2 (ICCP/TASE.2) and International Electro Technical Commission's (IEC 61850). The ICS should have secure communication protocols with

ISBN: 978-988-19252-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

some level of authentication, like the Secure Sockets Layer/Transport Layer Security SSL/TSL used in Information Technology (IT) [6].

### C. Class 3: Platform Vulnerabilities

The software, operation system, and hardware have a common security concern in the smart grid network because of the complexity of the architecture and configuration.

i. Design: Use of inadequate security architectures and designs, which could result from lack of training and awareness regarding the security requirements, will lead to vulnerabilities in the system security architecture.

ii. Implementation: The smart grid system must have strong protection software, such as anti-various or intrusion detection system, to prevent malware from affecting the system.

iii. Operational: Lack of prompt security patches from software vendors is very risky. The system should have a fast response for recovering from the vulnerabilities and sending mature patches to cover the known and expected vulnerabilities.

iv. Poorly Configured Security Equipment: Inadequate anomaly tracking is very harmful with regards to security. Alerts and logging are very important for informing the system in case of any attack or threat. However, this will bring the issue of vulnerability in false alarm notification. In order to solve this problem, the system shall have the ability to set up an alert before taking an action [7].

### D. Class 4: Network

The network is the method of communication between different devices using a standard communication protocol to send and receive data. The communication via network must be secured in order to prevent any attack and threat. The network shall have the security requirements designed to achieve integrity, confidentiality, availability, protocol encryption, and authentication.

i. Adequate Integrity Checking: The system should support message integrity and verify the sender and the receiver before taking any further action [7].

ii. Appropriate Protocol Selection: The system should use a secure communication protocol for the communication between different devices, especially the external communication, in order to prevent attackers from accessing and understanding the data, and then manipulating the system.

iii. Weaknesses in Authentication Process or Authentication Keys: To avoid suck weaknesses, the system should use a secure protocol, which will support authentication of the communications through the network. This will prevent unauthorized people from accessing the system and attacking the network.

iv. Insufficient Redundancy: Insufficient redundancy refers to the lack of enough redundancy in critical networks. This lack of redundancy exposes the system to some vulnerability, such as Denial of Service (DoS).

v. Physical Access to the Device: The physical access to the smart grid's electronic devices is a critical concern. The system must be protected from physical attack. This protection can be enforced through keeping these devices in a secure place and installing security alarms and cameras to notify the person in charge of any threat or serious attack.

## III. Smart Grid Security Issues

### A. Current Security Issues

The current electronic devices of the power grid do not support cryptography and data security [8]. When the power grid was built, engineers and designers did not consider the security implementation in the electronic design. This was because there was no external communication to these electronic devices. Also, the communication between the customers and the power grid is a one-way communication, from the power grid to the customers. Therefore, the electrical power system does not have extra capacity to perform any security function.

Power grid uses a serial data link to communicate with the different devices in the grid at a slow speed of 1200 baud. Moreover, the communication between any two devices in the network is a device-to-device communication. Consequently, any problem occurring in one device causes a problem in the behavior of the other device [9].

It is also important to mention the lifespan of power grid electronic devices. The replacement cycle of these devices is about 15 to 20 years. This cycle will cause a technology implementation gap between the legacy devices and the new ones. These devices were built 15 years ago and do not support the current security requirements. Security concerns and issues are constantly increasing.

The communication protocols of the power grid have been constructed with no security consideration. Therefore, any device can send any command to the other device in the network, with no authentication or any level of trust. All the communication protocols that are used in the power grid are built to support the internal communication only. Hence, there is no external communication to the power grid from the outside. Examples of communication protocols used in the power grid are: DNP3, Modbus, ICCP/TASE.2, and IEC 61850.

### B. New Security Issues

New security concerns arise when switching to the smart grid as a result of merging ICSs and IT [8]. As explained in the previous section, industrial control systems have been built without any consideration to security concerns. However, Information Technology considers security as a high priority. This requires changes to the ICS to upgrade the hardware and software of the power grid. There are many benefits for these changes. One possibility is to use Commercial of the Self (COTS) components. However, extra care must be taken to ensure these components will not increase vulnerabilities. Both ICS and IT personnel need to communicate with each other. There are considerable differences between the two technologies. The IT is using the patching server to update the system or add another level of access to the system and then forward the required update to all the hosts. This will cause the system to restart. Consequently, this will force the power grid to eventually shut down and cause blackout.

ISBN: 978-988-19252-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Another issue has to do with the power grid using a dedicated serial line that has low speed and very limited access. IT uses the TCP/IP protocol for communication in the Ethernet and Wi-Fi connection. This is characterized by high-speed communication and multiple accesses at the ftp server, telnet client, and web server. Consequently, many benefits to remote access and troubleshooting will be provided. Unfortunately, this will also create a new vulnerability for cyberattacks.

The smart grid technology uses many new devices, such as Advance Meter Infrastructure (AMI), Smart Meter, and Demand Response. AMI device will be installed in residences to provide two-way communication between the customer and the power grid control center. This implementation requires an AMI security profile to define and address all security concerns and find the solutions for these concerns. Setting up an AMI in each house and having it acting as an access point will demand monitoring, managing, and maintaining such devices. This approach is very difficult if not impossible [10].

There are other devices that the smart grid is using, such as Smart Meter and Demand Response, which allows customers to access their bills anytime in order to monitor the power consumption of home appliances and decide which one to shut down, turn on, or even schedule the appliances operation time. This will create security and privacy concerns. For example, if nobody is at home, a sophisticated cyberattacks may result in tampering with electrical appliances.

Thus, the interconnected networks and increased complexity of the grid could give rise to new vulnerabilities because of the merging of two different technologies in one system, and also lead to increasing the possibility of cyberattacks, such as Denial of Service (DoS), increase the amount of private information disclosed when data is collected, or any other malicious attack. Furthermore, increasing the number of entry points and paths provides an opportunity for potential adversaries to exploit [9].

## IV. Smart Grid Security Requirements

The most important intervention needed to ensure security is to build the security requirements in the Smart Grid and to have the information technology and power system experts communicate and understand each other [10]. Information technology experts will bring up the security concerns and address the possible cyberattacks in the network. The concerns of the IT group will help create the roadmap to build smart grid security requirements [9]. The power system experts will contribute to better understand the traditional power grid and help in deciding if the proposed security solution of the IT group affects the operational efficiency of the power grid and creates new issues. Hence, the two groups should work together to develop a robust security implementation in the smart grid.

According to the Department of Energy, and the Department of Homeland Security [10], each smart grid's security requirement has a unique identifier associated with it. This security requirements identifier is divided into three parts. The first part denotes the smart grid (SG). The second part specifies the family name, such as Access Control (AC), Awareness and Training (AT), and Continuity of Operations (CP). The third part is a unique numeric identifier. Examples of the main requirements include SG.AC-1 Access Control Policy and Procedures, SG.AC-2 Remote Access Policy and Procedures, SG.AC-3 Account Management, SG.AC-4 Access Enforcement, SG.AC-5 Information Flow Enforcement, SG.AC-6 Separation of Duties, SG.AC-7 Least Privilege, SG.AC-8 Unsuccessful Login Attempts, SG.AC-9 smart grid Information System Use Notification, SG.AC-10 Previous Logon Notification, and SG.AT-1 Awareness and Training Policy and Procedures.

## V. Smart Grid Security Enhancement

### A. Framework

Delivering the electricity generated by the power grid to the substations at a high voltage of at least 100KV is accomplished by power transmission. Then the power distribution delivers this electricity from the substations to the customers at a low to medium voltage below 100KV. Figure (2) demonstrates that.

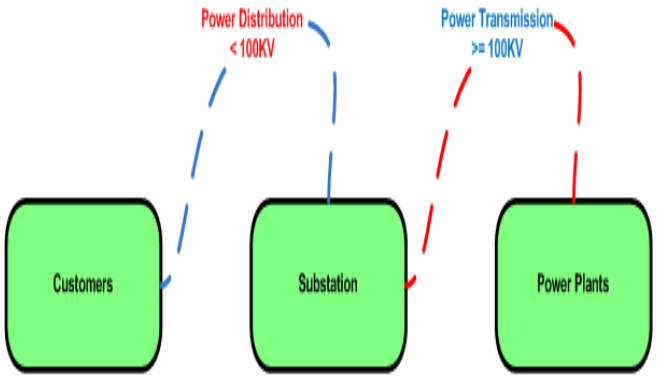


Fig. 2. Power Grid System

The current (traditional) power grid automation system is divided into three parts: Control Center, Substations, and Intelligent Electronic Devices (IEDs).

The Control Center normally contains an Energy Management System (EMS) and a Supervisory Control and Data Acquisition (SCADA) master. Substations are made up of Remote Terminal Unit (RTUs), Programmable Logical Controller (PLCs), Global Positioning System (GPS) Sync, Timers, Human Machine Interface (HMIs), communication devices (switches, hubs, and routers), log servers, data concentrators, and a protocol gateway. The RTU is also referred to as SCADA slave. Finally, Intelligent Electronic Devices are devices involving a matrix of transducers, meters, tap changers, circuit re-closers, phase measuring units, and protection relays [11]. Figure (3) demonstrates that [11].

The traditional power grid automation system has been physically isolated from the corporate network. However, smart grid networks shall allow power grid automation to connect to public networks. This kind of connection will

ISBN: 978-988-19252-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

increase the vulnerability of hacking the power grid automation [9].

The current architecture of the power grid automation does not support the security needed to deter cyberattacks. Wei et al. [11] proposed a new framework by introducing an additional layer of security to protect the power grid automation system from hackers and unauthorized people. They presented the needed security and safety when the power grid automation system is connected to public networks or the cloud, and divided the security layer into three major parts:

i. Security agents: The agents provide protection to the edge of the system to secure the network from the cyberattacks. The security agents in the Control Center are more intelligent and complex than the security agents in the IEDs.

ii. Managed Security Switch: This connects the Substations in the Control Center.

iii. Security Manager: The manager is located in the automation network and connected to switches using current IT security implementation.

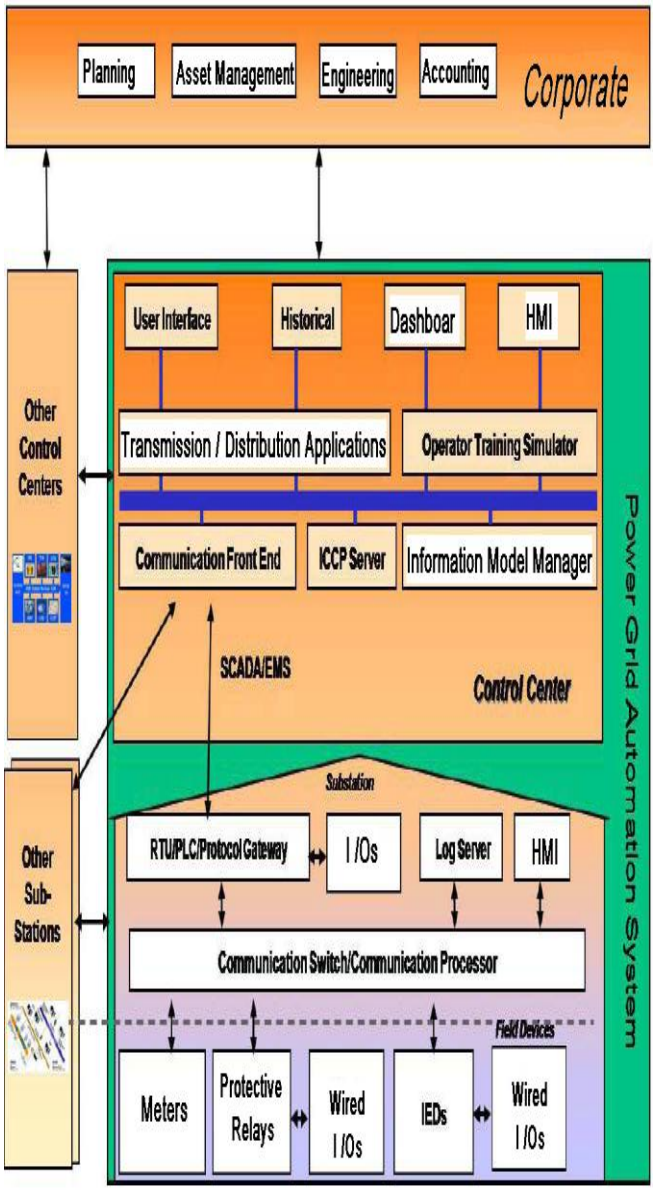


Fig. 3. Power Grid Automation

### B. *Framework End - to – End*

Zhang et al. [12] proposed a framework, which depends on the design method of information security protection architecture for the U.S. smart grid, the new information security protection requirements of China smart gird, and new information security risks including endpoint, access layer, transportation layer, border, and application system.

The proposed framework consists of four parts: security governance, security management, security maintenance, and security technology. This proposed framework sets up the smart grid model of information security and strategy, and designs the supporting information security architecture of smart grid. It ultimately establishes the information security protection system for the smart grid including the close coupling of the following six areas: generation, transmission, substation, distribution, electricity scheduling and achieving strong smart grid information security control, and controllability [9].

The technical phases of this model include *advanced threat notification* for the early notification warning of a possible network attack, *protection* to ensure confidentiality, integrity and availability of information system, *detection* to find the kind of the network attack and illegal information flow, *response* to allow the system to take the next step to prevent any further manipulation of information system, *recovery* to take the serious actions to back up the data and turn on the auxiliary system to support the power grid, and *counter-attack* to perform the reverse action and protect the system from the serious threat [12].

### C. *Cryptography and Key Management Solution*

The smart grid shall have accurate cryptography and key management to build a robust security implementation. Some of the smart grid devices permit physical access to the customer, such as smart meter, and advanced meter infrastructure. This possibly reveals the key generation algorithm and leads to potential cryptanalysis. Furthermore, cryptography implementation requires complex hardware and software design support. All customer information and the power system must be encrypted to protect privacy and maintain integrity, confidentiality, and availability [9]. Cryptography and key management shall be an appropriate solution to protect the smart grid from cyberattacks, and tackle the physical access concerns of the smart grid security [10].

## VI. The Future of Smart Grid Security

The future of smart grid security seems promising. The following security enhancements should be taken care of:

1) Enhancing the smart grid security approach by adopting the Internet protocol version 6 (IPV6) in the smart grid communication protocol, synchrophasor security/NASPInet, anonymization, behavioral economics/privacy, cross-domain security involving IT, power, transportation systems, and remote disablement/switch of energy sources [13].

ISBN: 978-988-19252-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

2) Using the public key infrastructure (PKI) in the smart grid, and addressing all the related requirements of the operation and devices of the smart grid [14].
3) Securing the trusted device profile and implementing and developing the smart grid certificate lifetime [5].
4) Resolving the privacy concerns regarding customer information and the power system data transfer via the smart grid [15].
5) Preventing the transfer of some critical data, such as the business location or cross border data transmission [10].
6) Implementing a robust security approach for the smart grid as a future priority to achieve proper authentication in any device communication via the smart grid [16].
7) Addressing all the newly created vulnerabilities of the smart grid by monitoring and tracking the communication and the data flow through the smart grid [10].

## VII. Conclusions

This paper presented the work that has been done so far with regards to the security of the smart grid. It also presented the future approaches, techniques, and methods needed to improve and enhance this security. All of the security features that the smart grid needs to cover were addressed. The paper provided a broad view of how we can make the smart grid a very secure system to take full advantage of all its features. Our future work will focus on extending security requirements to all the smart grid subsystems, including transmission, distribution, customer interface, distributed energy resources, and third party access. The main focus will be on how to implement powerful cryptographic protocols to achieve outstanding security.

## References

[1] *Study of Security Attributes of Smart Grid Systems - Current Cyber Security Issues*, INL/EXT -09-15500 – 2009.
[2] *Communication Networks and Systems in Substations*, IEC Standards 61850 – 2005.
[3] F. Cleveland, "Enhancing the Reliability and Security of the Information Infrastructure Used to Manage the Power System," presented at the IEEE PES General Meeting, Tampa, FL, Jun. 24-28, 2007.
[4] L. Wang, C. Li, H. Cheung, C. Yang, and R. Cheung, "PRAC: A Novel Security Access Model for Power Distribution System Computer Networks," presented at the IEEE PES General Meeting, Tampa, FL, Jun. 24-28, 2007.
[5] *Guidelines for Smart Grid Cyber Security*, NISTIR 7624. 3-2010.
[6] B. A. Forouzan, *Cryptography and Network Security*. New York, NY: Mc Graw Hill, 2008, pp. 1-358.
[7] W. Stallings, *Cryptography and Network Security: Principles and Practices*. Upper Saddle River, NJ: Prentice Hall, 2006, pp. 527-645.
[8] S. Clements, and H. Kirkham, "Cyber-Security Considerations for the Smart Grid," presented at the IEEE PES General Meeting, Minneapolis, MN Jul. 25-29, 2010.
[9] G. N. Sorebo, and M. C. Echols, *Smart Grid Security:An End-to-End View of Security in the New Electrical Grid*. Boca Raton, FL: CRC PRESS, 2012, pp. 1-79.
[10] *Guidelines for Smart Grid Cyber Security*, NISTIR 7624. 1-2010.
[11] D. Wei, Y. Lu, M. Jafari, P. Skare, and K. Rohde, "An Integrated Security System of Protecting Smart Grid against Cyber Attacks," presented at the 2010 Conf. Innovative Smart Grid Technologies (ISGT), Gaithersburg, MD.
[12] T. Zhang, W. Lin, Y. Wang, S. Deng, C. Shi, and L. Chen, "The Design of Information Security Protection Framework to Support Smart Grid," presented at the 2010 Int. Conf. Power System Technology (POWERCON), Hangzhou.
[13] X. Miao and X. Chen, "Research on IPv6 Transition Evolvement and Security Architecture of Smart Distribution Grid Data Communication System," presented at the 2010 Int. Con. Electricity Distribution, China.
[14] M. Zhao, S. Smith, and D. Nicol, "Evaluating the Performance Impact of PKI on BGP Security," presented at the 2005 4th Annual PKI Research and Development Workshop, Gaithersburg, MD.
[15] A. Barenghi and G. Pelosi, "Security and Privacy in Smart Grid Infrastructures," presented at the 2011 22nd Int. Workshop Database and Expert Systems Applications, Toulouse.
[16] Q. Li and G. Cao, "Multicast Authentication in Smart Grid with One-Time Signature," in *Proc.2011 IEEE INFOCOM*.

ISBN: 978-988-19252-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)