TELKOMNIKA Indonesian Journal of Electrical Engineering
Vol. 15, No. 3, September 2015, pp. 436 ~ 444
DOI: 10.11591/telkomnika.v15i3.8461

Cyber Security Threats in Synchrophasor System in Wide Area Monitoring System

Surender Kumar[1], M K Soni[2], D K Jain[3]
[1,3]DCRUST, Murthal, Sonepat, India
[2]MRIU, Faridabad, India
*Corresponding author, e-mail: grewalsk@gmail.com[1], dr_mksoni@hotmail.com[2], jaindk66@gmail.com[3]

Abstract

Cyber security has become a critical priority for electric utilities. With the increase in the use of intelligent measuring devices like PMUs and more advanced communications and information technology in smart grid, the overall attack surface has increased. Cyber attacks against synchrophasor system critical infrastructure are detrimental to the functioning of the society as a whole. This paper presents the latest on cyber security of synchrophasor system in smart grid, specifically; it focuses on the deep understanding of the risk in terms of threats, vulnerabilities and consequences that arise from cyber attacks. Since the research on cyber security for the smart grid is still in its early stage, our objective is to provide an overview, analyze potential cyber security threats, and review existing security solutions in the Wide Area Monitoring System.

Keywords: *phasor measurement units (PMUs), PDC, synchrophasor system, cyber security, cyber attacks, cryptography, IPSec*

1. Introduction

Modern power grid infrastructure is comprised of hardware and software owned and operated by many interconnected entities, relies on the secure real-time data collection and transmission service provided by an intelligent monitoring system. Better communication infrastructure is required to providing improvements in security, efficiency, and reliability of smart grid. This infrastructure largely revolves around communication between control centers and individual substations. With the increased use of information and computation tools in the smart grid, its vulnerability to cyber attacks are becoming more and more frequent and sophisticated [1].

In recent years, there is a dramatic increase in cyber attacks targeted against critical infrastructures. One of the recent examples is cyber security attack on Telvent in Sept., 2012, the smart grid giant owned by Schneider Electric, where hackers were able to access the critical Supervisory Control and Data Acquisition System (SCADA), which is used to control power grid, oil, and gas pipeline systems. Hackers were able to install malicious software and access project files of SCADA systems [2]. Similar attacks are becoming more prevalent on critical Wide Area Monitoring System (WAMS) infrastructure due to the integration of intelligent measurement devices such as phasor measurement units (PMUs). Cyber attacks against synchrophasor system critical infrastructure are detrimental to the functioning of the society as a whole.

The move from legacy propriety systems to open system standards has accelerated the cyber attacks associated with the electric grid. The term cyber security refers to all the approaches which ensure the confidentiality, integrity, and availability of data, systems, and networks from intentional attack as well as accidental compromise, ranging from preparedness to recovery. The weaknesses in personnel, processes, technology, and the physical environment can attract cyber security vulnerabilities. Issues related to cyber security occur due to actions taken by attackers, and also by disgruntled employees. Cyber security needs a holistic approach to deal with vulnerabilities and threats linked with synchrophasor system.

North American Electric Reliability Corporation-Critical Infrastructure Protection (NERC-CIP) was developed to address the risks and vulnerabilities associated with PMUs based WAMS by designing and enforcing various standards and regulations [3]. The brief introduction

Received May 13, 2015; Revised August 1, 2015; Accepted August 15, 2015

of cyber security concepts and issues related to emerging modern electric grid is provided in [4-11]. G. N. Ericsson addresses the cyber security and power system communication as smart grid solution. It also highlights access points in a substation. Three levels; system, scenarios, and access point vulnerabilities of SCADA systems is evaluated in [5].

The remaining paper is organized as follow. The overview of WAMS is presented in section II, cyber security issues in WAMS are presented in section III, types of cyber attacks and cyber security measures for PMUs based WAMS is given in section IV, followed by conclusion in section V.

2. Wide Area Monitoring System

A measurement system that incorporates PMUs deployed over large portions of the power system is known as Wide Area Monitoring System (WAMS). The basic components of WAMS are PMUs, PDC, Super PDC, PMU application systems and Communication networks, as shown in Figure 1.

PMUs, the main part of WAMS, are deployed at substations, connected to a Local Area Network. PMUs are responsible for generating more than 50% of WAMS' network data [6]. The LAN is in turn connected via a substation router to a Wide Area Network (WAN). The application that utilizes the PMU data resides at a central location connected to a Local Area Network of control center. Data from PMUs is concentrated in PDC via WAN which adopts UDP/TCP/IP, after then sort them according to the GPS time stamp, after which they are sent to super PDC. Thereafter, the actions generated by application in super PDC, are transferred via the WAN to the substation [7].

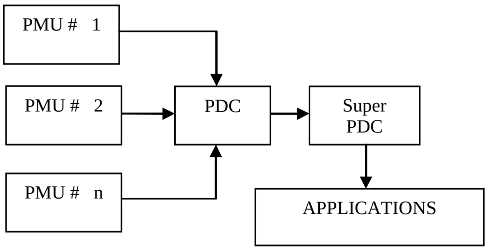

Figure 1. General Block Diagram of WAMS Architecture

The WAMS network uses several communication infrastructures ranging from serial communication to VPN. As WAMS evolve more fibre optics and licensed digital microwave technologies will be incorporated into WAMS communication infrastructure, to provide enhanced data delivery services [8].

The majority of protocols used by a WAMS, however, do not include security mechanisms in their specifications. A few standards are in development to incorporate message authenticity and confidentiality features to IEEE C.37.118 network traffic. IEC 61850.90-5 packets will encapsulate IEEE C.37.118 packets to provide the additional security features [9].

3. Cyber Security Issues in WAMS

In [10], smart grid is defined as a cyber-physical system (CPS) and identifies unique security challenges and issues encountered in such systems that are not prevalent in traditional IT security. They also discuss security solutions to address these unique challenges.

It is almost impossible to ensure every part or node to be invulnerable to network attacks in PMUs based WAMS in smart grid. The synchrophasor system must be resilient to the cyber/ physical attacks by using some of the smart grid security protocol, and the WAMS network must have the self-healing ability to continue network operations in the presence of attacks. PMUs based WAMS, being an integral part of smart grid, it is crucial to ensure the availability and integrity of the PMUs data it carries and the communication and computation infrastructure involved. The PMUs based WAMS is expected to operate over large scattered geographical areas, which make the security aspect more complex. The security risk grows as the deployment of PMUs becomes more widespread [11].

To ensure secure and reliable WAMS operation, it is essential to understand what are the security objectives and requirements before providing a comprehensive treatment of cyber security in the context of data delivery and time bound actions [12]. The cyber security objectives and requirements for the PMUs communication in WAMS are discussed as follow.

3.1. Security Objectives of Synchrophasor System

Considering the crucial role of synchronized measurements in PMUs based WAMS, various groups/organizations are working on developing security standards and recommendations for WAMS in smart grid. The NISTIR 7628 [13], “Guidelines for Cyber Security in the Smart Grid” standard provides a comprehensive set of guidelines for designing cyber-security mechanisms or systems for the smart grid. The standard proposes methods for assessing risks in the smart grid, and then identifies and applies appropriate security requirements to mitigate these risks. National Institute of Standards and Technology (NIST) has also released a draft on Cyber Security Framework for critical infrastructure.

The IEC 62351 standard series [14], developed by working group WG15 of IEC TC57, defines security mechanisms to protect communication protocols for substation systems, in particular, IEC 60870 and IEC 61850. The primary focus of this standardization is to provide end-to-end security. The Critical Infrastructure Protection (CIP) set of standards developed by the North American Electric Reliability Corporation (NERC) aims at introducing compliance requirements to enforce baseline cyber-security efforts throughout the bulk power system (transmission).

IEC 61850 90-5 is a communication standard currently in preparation which allows transmission of synchrophasor data and includes a digital signature to provide authentication and tamper detection and optionally provides encryption to provide confidentiality [15]. Table 1 provides a summary of these initiatives.

Table 1. Research Initiatives on Security Challenges to WAMS

Initiative	Research Direction
IEC 62351	Describes recommended security profiles for various communications media and protocols
NERC CIP 002-009	Deals with cyber-security standards
IEEE C37.118	The communications protocol for PMU communications
NISTIR	Guidelines for smart grid security
IEC 61850-90-5	Security issues

There are three high-level security objectives of synchrophasor system, i.e., availability, integrity, and confidentiality [12].

Availability ensures uninterrupted, reliable, timely access of data, and resources to authorized users. It implies to network, communication infrastructure, systems, applications, database, and supporting infrastructure. Services must be available to authorized users. Ensuring timely and reliable access to and use of information is of the most importance in the synchrophasor system. This is because a loss of availability is the disruption of access to or use of information, which may further undermine the power delivery.

Integrity of the data communication in WAMS network should be guaranteed so that any alteration of the PMUs data can be detected. Data integrity protects unauthorized modification and destruction of information either within the system or while transmitting across the LAN/WAN. Integrity ensures non repudiation and authenticity of information. Integrity can be classified as; system and data integrity. System integrity deals with the protection of systems like PMUs, IEDs, relays, and PDCs. Integrity can be achieved through hash verifications, input/output checksums, stringent access and authentication systems and well designed security policies. A loss of integrity is the unauthorized modification or destruction of information and can further induce incorrect decision regarding power management.

Data confidentiality in PMUs communication should be protected, otherwise, utility consumption values will be known by attackers, which will leak much information on consumers' behaviors. Confidentiality ensures prevention of illicit revelation or disclosure of data [16]. Confidentiality prevents exposure of stored data, processed data within system, and data though LAN/ WAN. Confidentiality can be breached either through well coordinated attacks or, through unauthorized disclosure of. Confidentiality can be achieved through data encryption, access control, training & awareness, and data classification.

The availability and integrity are crucial for such systems, whereas data confidentiality is less important because there is no customers' private information involved. Availability also works in parallel with confidentially and integrity. In general, the primary security objective for control systems is availability, with integrity second, and confidentiality third.

3.2. Security Requirements in Synchrophasor System

Prior to deployment of synchrophasor system in WAMS, a set of cyber security requirements must be developed, new equipments must be undergo vulnerability testing, and proper security controls must be designed to protect the synchrophasor system from unauthorized access. The cyber security requirements must be based on availability, integrity, and confidentiality of system, data, and process. Based on the recommendations of various studies, the requirements of cyber security measures for synchrophasor system are [17-19]:

1) The security measures adopted should not in any way hamper the primary objective of the synchrophasor system.
2) The availability cyber security requirements assure the PMUs and PDC network servers must remain available to perform its primary functions in timely manner.
3) The access to every PMU or PDC of a utility should be through an authentication procedure.
4) The system should accept only authenticated and authorized changes in the configuration of the network.
5) The transfer of information between different components in the synchrophasor system in WAMS such as PMU, PDU, GPS, control center and applications must be confidential.
6) Accountability must be achieved through implementation of authorization, authentication, auditing, and non repudiation.
7) There should be proper mechanism to validate the integrity of data exchanged.
8) The system should continue to perform essential functions in case of loss of synchronized measurements.
9) The security mechanism should be able to minimize the impact of abnormalities on the performance of WAMS.

3.3. Types of Cyber Attacks at Synchrophasor System

Several modes of attack can take place to tamper the synchrophasor system which can range from physical attacks to remote access attacks. Cyber attackers reconnoiter a system before attacking. It is highly crucial to prevent these attacks for the proper functioning of the WAMS system.

There are main two vulnerable points in WAMS where data can be hacked and manipulated at substation level (PMUs) and control center level. However, cyber attacker can attacks at any level i.e., component-wise, protocol-wise, topology-wise [20].

The current attacks that threaten PMU networks are Denials of Service (DoS), physical, Man-in-the-Middle, packet analysis, malicious code injection, and data spoofing attacks.

3.3.1. Denial of Service (DoS) Attack

It is one of the most common threats on the synchrophasor systems. DoS attack occurs when an attacker compromises the availability of an information system of WAMS. During DoS attack in WAMS infrastructure, the attacker attempts to deny access to legitimate user to a particular resource, or, at the very least, reduce the quality of service of a resource. DoS attack on communication network rendering computational resources ineffective [21].

An attacker, who manages to gain access to the communication infrastructure, can launch a DoS attack by flooding a critical link with bogus traffic or by saturating the computing resources of a critical network device such as a router or metering field device. Such an attack causes real-time measurement data from field devices to be delayed or at worst dropped. DoS attack can also delay or drop critical control signals from a controller.

When wireless technologies are adopted in a WAMS substation, jamming attacks may become a primary security threat. At substation, a DoS attacker does not need to completely shut down network access by using some extreme means (e.g., all-time jamming) but instead it may launch weaker versions of attacks to intentionally delay the transmission of a time-critical message to violate its timing requirement. A recent work [22] has showed that jamming attacks can lead to a wide range of damages to the network performance of power substation systems, from delayed delivery of time-critical messages to complete denial-of-service.

3.3.2. Man-in-the-Middle Attacks

In a PMU network the Man-in-the-Middle attack occurs between the PMU and the PDC. The attacker disguises themselves as the PDC to the PMU and as the PMU to the PDC. An attacker can manages to gain access to the communication infrastructure, either remotely or locally. The false certificates can be sent to conduct a Man-in-the-Middle attack [23].The man-in-the-middle attacks on measurement data are effective mainly if the attack is persistent but a single attack on control signals can be catastrophic.

3.3.3. Packet Analysis Attack

Contents of the PMU TCP/IP packets are susceptible to packet analysis (sniffing) [24]. Attackers abuse packet sniffers to steal unencrypted information, spy on network traffic, and gather information to leverage in future attacks against the network. This attack uses Address Resolution Protocol (ARP) spoofing to sniff traffic between hosts.

3.3.4. Packet Injection Attack

Packet injection can be classified into two subgroups; sensor measurement injection and command injection. Sensor measurement injection attacks inject false sensor measurement data into a control system. Sensor measurement injection can be used by attackers to cause control algorithms to make misinformed decisions. Command injection attacks inject false control commands into a control system [19]. Packet injection is commonly used in Man in the Middle attacks and DoS attacks.

3.3.5. Data Spoofing Attack

In spoofing attack, attacker can make the system to act in malicious way by sending illegal message to the different components and devices in the synchrophasor system. Spoofing of GPS signals resulting into bad time synchronization could be offset with redundant time synchronization schemes, on synchronization error detection. Data spoofing gives the forged data instead of actual data. This can be fetal to grid stability and reliability. This can lead to the instability or malfunction of the system depending on the wrong information sent by the attacker [25-26].

4. Cyber Security Measures of Synchrophasor System

There are main two vulnerable points in WAMS where data can be hacked and manipulated at substation level (PMUs) and control center level. Further, the Synchrophasor system security measures are divided into two groups

a) Substation Security Measures
b) Information Security Measures

4.1. Substation Security Measures

One of the main security concerns in synchrophasor system is the attack on the substation network and cyber assets within it. The attacks to substation will most likely come from access points, as they are connected to substation and other entities the systems. PMUs and PDCs need to be shielded from the larger network.

One of the ways to protect the substation from external cyber attack is to secure the access points and limit their exposure to the outside world. As shown in the Figure 2, PMUs, which send the data outside the substations, are in security gateway device. These security gateways devices have the same properties which can fulfill the roles of Firewall and Virtual Private Network (VPN) tunneling.

The security gateway provides an interface between the critical network components and the internet. Security gateways provide the network with a firewall [27]. In [28] the authors suggest firewalls should have three main properties, i.e., all PMUs traffic must enter; only trusted traffic may pass, and the firewall is immune to penetration. All traffic from the PMU to the PDC, or from PDC to PMU, needs to pass through the security gateway to improve security. If the component trying to connect to the PMU or PDC is not on the trusted list for the security gateway, then it is not permitted to pass [24]. So, if the security gateway is configured and setup correctly, only traffic from the trusted list may pass. Although, this provides some security, data spoofing still remains a threat to the system. Figure 2. shows the PMU and PDC being shielded from the wider network by the security gateway. It can be a local area network behind the security gateway. The other job of the security gateway within the network is to establish a VPN. Establishing a VPN between substations allows measurement and configuration data to be sent securely between substations.

The security gateway uses the IPSec protocol to establish VPN connections. IPSec uses Encapsulated Security Payload (ESP) and Authentication Header (AH) protocols to secure data. Once the payload is encrypted, it is transmitted across the network. When it reaches the designated security gateway, the gateway will check to see if the packets were delayed or replayed and decipher the packet. The measurements are then recorded in the PDCs' database [24].

4.2. Information Security Measures

A cyber attack is not only limited to the attack on the substation, but also on the data that is coming out of the substation. All security requirements should be maintained all the way from PMUs, substations, Wide-area network (WAN) to the end user application. As synchrophasor data are used in power system monitoring and control, a potential attack on these data can be dangerous. The best practices for information security in the synchrophasor system are discussed as follows [27].

4.2.1. Data Transmission

To ensure integrity of the message, mutual authentication should be used between substations and the clients. The information in the synchrophasor system needs to be encrypted in order to provide data confidentiality. Synchrophasor systems uses VPN to encrypt the data and send the information to the client in decrypted form and at the end point of VPN, the data are decrypted and delivered to the client.

4.2.2. Data Handling Practices

In synchrophasor system, data is not only exchanged between the substation and utilities but also between the substation and third party contractors. So data transmission must be done in secured condition so that only authorized entities can access the data and only necessary information is exchanged with outside entities.

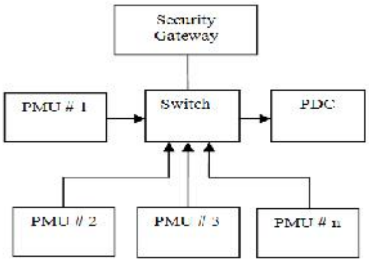

Figure 2. Security Gateway as a Firewall

Data in synchrophasor system is mainly transmitted through the IP networks or direct serial links Communication link connects various substations to one another and to control centers. However, these links cannot be trusted as they may be passing through the untrusted networks. This can lead to many threats and attacks on the synchrophasor data, if the data confidentiality and integrity is not maintained. One of the solutions to maintain data confidentiality and integrity across these untrusted networks is encryption during the link layer or IP layer. This is done by converting the data into cipher text.

Encryption schemes can be based on symmetric key cryptography (e.g., AES, DES) or asymmetric key cryptography (e.g., RSA). Symmetric key cryptography uses the same key for encryption and decryption. Asymmetric or public key cryptography uses private and public keys to encrypt and decrypt, respectively [29].

Advanced Encryption Standard (AES) is an encryption algorithm which generates the ciphertext through a number of iterative recalculations. Data Encryption Standard (SES) is a cipher that operates on 64-bit blocks of data, using a 56-bit key. It is a private key system. In Rivest-Shamir-Adleman (RSA) the encryption key is public and differs from the decryption key which is kept secret. RSA can be used for key exchange, digital signatures, or encryption of small blocks of data. RSA uses a variable size encryption block and a variable size key. Hash functions are used as building blocks in various cryptographic applications. There are a lot of works in the literature [30] that have provided comprehensive comparisons between symmetric and asymmetric schemes for network protocol design.

After the RSA algorithm was published, Diffie and Hellman have developed their own algorithm. Diffie Hellman is a well known cryptographic algorithm used for secure key exchange [31-32]. The algorithm allows two users to exchange a symmetric secrete key through an insured wired or wireless channel and without any prior secrets. The algorithm itself does not encrypt data, but instead it generates a secret key common to both users i.e., the sender and the recipient. The major challenge being faced by Diffie Hellman algorithm is the intelligence and computational capability of the hacker. Diffie Hellman public key cryptography is used by all major VPN gateway's today. This algorithm is a bit slow [33].

Authentication is a crucial identification process to eliminate attacks targeting data integrity. For a message authentication code (MAC) based authentication protocol, a MAC is generated using a keyed hash function, and appended to a message [34-35]. Computation involved in authentication (e.g., digital signature and verification) must be fast enough to meet timing requirements of messages in the synchrophasor system. In public key based multicast authentication, all receivers share the public key of the sender. The sender signs a message with its own private key, and then each receiver uses the sender. The sender signs a message with its own private key, and then each receiver uses the sender's public key to verify the message.

4 Conclusion

The reliable, secure, and effective information of measurements from PMUs and PDCs, is a key to the success of the future WAMS. Cyber-security is one of the main obstacles to widespread deployment of PMUs. All traffic from the PMU to the PDC, or from PDC to PMU, needs to pass through the security gateway to improve security. Synchrophasor systems uses VPN to encrypt the data and send the information to the client in decrypted form and at the end point of VPN, the data are decrypted and delivered to the client. It is almost impossible to ensure every part or node to be invulnerable to network attacks in PMUs based WAMS in smart grid. Security should be a continuous process and requires intelligent monitoring, reviewing and adjusting to be effective.

References

[1] Carl H Hauser, David E Bakken, Anjan Bose. A failure to Communicate: Next Generation Communication Requirements, Technologies, and Architecture for the Electric Power Grid. *IEEE Power and Energy Magazine.* 2015; 3(2): 47-55.

[2] Kiran Gajrani, Annapurna Bhargava, Ramesh Bansal. Cyber Security Solution for Wide Area Measurement Systems in Wind Connected Electric Grid. *IEEE Innovative Smart Grid Technology-Asia, ISGT Asia 2013.* 2013: 1-5.

[3] North American Electric Reliability Corporation. Critical Infrastructure Protection (CIP) Reliability Standards. 2009.

[4] J Hull, H Khurana, T Markham, K Staggs. Staying in Control Cyber Security and the Modern Electric Grid. *IEEE Power & Energy Magazine.* 2012; 10(1): 41-48.

[5] GN Ericsson. Cyber Security and Power System Communication - Essential Parts of a Smart Grid Infrastructure. *IEEE Transactions on Power Delivery.* 2010; 25(3): 1501-1507.

[6] MD Hadley, et al. *Securing Wide Area Measurement Systems*. Pacific Northwest National Laboratory. Report number: PNNL-17116. 2007.

[7] C Martinez, M Parashar, J Dyer, J Coroas. Phasor Data Requirements for Real Time Wide-Area Monitoring, Control and Protection Application. *CERTS/EPG, EIPP Real Time Task Team.* 2005: 1-27.

[8] Ekram Hossam, Zhu Han, H Vincent Poor. Smart Communications and Networking. Cambridge University Press. 2012.

[9] KE Martin, D Hamai, MG Adamiak, S Anderson, M Begovic, G Benmouyal, G Brunello, J Burger, JY Cai, B Dickerson, et al. Exploring the IEEE Standard C.37. 118–2005 Synchrophasors for Power Systems. *IEEE Transactions on Power Delivery.* 2008; 23(4): 1805-1811.

[10] Siddharth Sridhar, Adam Hahn, Manimaran Govindarasu. *Cyber–physical System Security for the Electric Power Grid*. Proceedings of the IEEE. 2012; 1(100): 210-224.

[11] The Synchrophasor Report, SEL. 2010; 2(5).

[12] Y Yan, Y Qian, H Sharif, D Tipper. A survey on Cyber Security for Smart Grid Communications. *IEEE Communications Surveys and Tutorials.* 2012; 14(4): 998-1010.

[13] Lee, T Brewer. Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements. *NISTIR 7628*. 2010.

[14] IEC 62351. *Security Standards for the Power System Information Infrastructure*. 2012.

[15] IEC Standard. IEC 61850. *Communication Networks and Systems in Substations*.

[16] RB Bobba, J Dagle, H Khurana, WH Sanders, P Sauer, T Yardlet. Enhancing Grid Measurement: Wide Area Measurement Systems, NASPInet, and Security. *IEEE Power & Energy Magazine.* 2012; 10(1): 67-73.

[17] D Wei, Y Lu, M Jafari, P Skare, K Rohde. Protecting Smart Grid Automation Systems Against Cyber Attacks. *IEEE Transactions on Smart Grid.* 2011; 2(4): 782. 795.

[18] The Smart Grid Interoperability Panel – Cyber Security Working Group, Guidelines for Smart Grid Cyber Security. *NISTIR 7628*. 2010: 1-597.

[19] Thomas H. Morris, Shengyi Pan, Uttam Adhikari. Cyber Security Recommendations for Wide Area Monitoring, Protection, and Control Systems. *IEEE Power and Energy Society Meeting.* 2012.

[20] Dong Wei, Yan Lu, Mohsen Jafari, Paul Skare, Kenneth Rohde. *An Integrated Security System of Protecting Smart Grid against Cyber Attacks.* Proceedings of Innovative Smart Grid Technologies (ISGT). 2010: 1-7.

[21] S Zargar, James Joshi, David Tipper. A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. *IEEE Communications Surveys & Tutorials.* 2013; 15(4).

[22] Zhou Lu, W Wang, C Wang. Modeling, Evaluation and Detection of Jamming Attacks in Time-Critical Wireless Applications. *IEEE Transactions on Mobile Computing.* 2014; 13(8): 1746-1759.

[23] Franco Callegati, Walter Cerroni, Marco Ramilli. Man-in-the-Middle Attack to the HTTPS Protocol. *IEEE Security and Privacy.* 2009; 7(1): 78-81.

[24] Christopher Beasley, G Kumar Venayagamoorthy, Richard Brooks. *Cyber Security Evaluation of Synchrophasors in a Power System*. Clemson University Power Systems Conference (PSC). 2014: 1-5.

[25] Hua Lin, Santhosh Sambamoorthy, Sandeep Shukla, James Thorp, Lamine Mili. A study of Communication and Power System Infrastructure Interdependence on PMU-based Wide Area Monitoring and Protection. *IEEE Power and Energy Society General Meeting.* 2012: 1-7.

[26] Daniel P Shepard, Todd E Humphreys, Aaron A Fansler. Evaluation of the Vulnerability of Phasor Measurement Units to GPS Spoofing Attacks. *International Journal of Critical Infrastructure Protection.* 2012; 5(3): 146-153.

[27] John Stewart, Thomas Maufer, Rhett Smith, Chris Anderson, Eren Ersonmez. Synchrophasor Security Practices. *Schweitzer Engineering Laboratories*. Pullman, Washington. 2010.

[28] Steven M Bellovin, William R Cheswick. Network Firewalls. *IEEE Communications Magazine.* 1994; 32(9): 50-57.

[29] O Kosut, Jia Liyan, RJ Thomas, Lang Tong. Malicious Data Attacks on Smart Grid. *IEEE Transactions on Smart Grid.* 2011; 2(4): 645-658.

[30] Whitfield Diffie, Martin E Hellman. New Directions in Cryptography. *IEEE Transactions on Information Theory.* 1976; 22(6): 644-654.

[31] Gary C Kessler. An Overview of Cryptography. http://www.garykessler.net/liberary/crypto.html.

[32] Henk CA van Tilborg. Fundamentals of Cryptography: A Professional Reference and Interactive Tutorial. Springer. 1999.

[33] William Stalling. Cryptography and Network Security Principles and Practice. 5th Edition. Pearson. 2010.

[34] Fadi Aloul, AR Al-Ali, Rami Al-Dalky, Mamoun Al-Mardinia, Wassim El-Hajjb. Smart Grid Security: Threats, Vulnerabilities and Solutions. *International Journal of Smart Grid and Clean Energy*. 2012; 1(1): 1-6.
[35] A Metke, R Ekl. Security Technology for Smart Grid Networks. *IEEE Transactions on Smart Grid.* 2010; 1: 99-107.