https://doi.org/10.36785/BUITEMS.JAES.326

Exploring the Privacy Issues of Smart-Grid Infrastructure – A Network Security Perspective

Irshad Hussain[1], Ishtiaq Ahmad[2], Faizullah Khan[2], *M. Riaz*[1], Surat Khan[2], Muhammad Ashraf[2], and Akbar Khan[2]

[1]Faculty of Electrical and Computer Engineering, UET Peshawar Pakistan.
[2]Faculty of Information and Communication Technology, Balochistan University of Information Technology, Engineering and Management Sciences (BUITEMS), Quetta, Pakistan

***Abstract*— The proposed smart grid infrastructure aims to make use of the existing public networks such as internet for data communication between consumer premises to the public power utility network. The smart-grid adopts smart-meters which basically collect vast amount of data to provide a holistic view of the connected load behavior and preferences pattern related to power and water consumption. The smart-grids provide benefits to the utilities and consumers alike. For utilities the benefits are real time data collection, ease of power management, and reduced personnel requirement. The benefits for the users on the other hand include availability of real time usage data, providing information on ways to minimize power consumption, monetary savings and so on.**

Since, the smart-grid uses existing public networks the utilities do not have the burden of installing any new infrastructure (except for installing the smart-meters), thus an added advantage. But, the downside of using the public network is susceptibility to a variety of network attacks, if not guarded well against. This paper talks about the various network security vulnerabilities that exist and the measures to patch the same before employing in the smart grid networks.

***Keywords*: IP networks, Privacy, Public Keys, Smart-Grid, VPN**

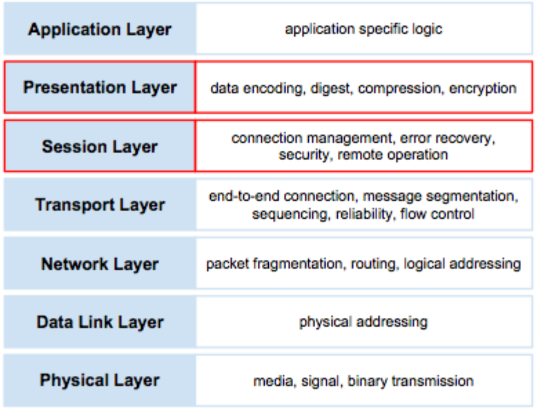
Date Received 29-10-2019
Date Accepted 25-12-2019
Date Published 31-12-2019

I. Introduction

THE smart grid network uses IP technology for a two-way communication between the customer premises and the power utility. The data being communicated through the network is of sensitive nature and includes information of power usage of the customers, health and behavior of the assets, along with control class information to control the smart grid equipment remotely. This calls for the approach which has to secure the infrastructure on several layers from various sorts of vulnerabilities. The IP layer infrastructure needs to be guarded the most. It is because the network layer is responsible for packet forwarding including routing through intermediate routers, whereas the data link layer is responsible for media access control, flow control and error checking.

The Open System Interconnection (OSI) model (**Figure-1**) is based on the layered approach. It divides each functionality into separate layers. It is due to this layered approach that there is no inherent mechanism to communicate the occurrence of an undue event such as attack to another layer [1]-[2]. To overcome this limitation it becomes necessary to defend or secure each of the layers in the OSI model separately.

The IP (Internet Protocol) is a routed protocol meaning, IP is designed to be routed over and through different networks.



Application Layer	application specific logic
Presentation Layer	data encoding, digest, compression, encryption
Session Layer	connection management, error recovery, security, remote operation
Transport Layer	end-to-end connection, message segmentation, sequencing, reliability, flow control
Network Layer	packet fragmentation, routing, logical addressing
Data Link Layer	physical addressing
Physical Layer	media, signal, binary transmission

Figure1: OSI Layer with its applications (general) [3]

The network layer provides the functional and procedural means of transferring variable-length data sequences from a source to a destination host via one or more networks, while maintaining the quality of service functions. The protection of this layer becomes the most essential part of any network architecture making use of the IP technology.

Each of the OSI layers has several key functions and for communication between the OSI layers they usually employ different protocols. Each layer employs several different protocol/s and is often subject to attacks by the malicious users. In the evolution of these technologies several mechanisms have been developed to defend against such attacks [4].

There are several methods to provide security at application (Layer 7), transport (Layer 4) and data link (Layer 2) layers of the network but network layer (Layer 3) security has not been addressed adequately. Even though switches and routers have built in security features they are not enough to fully secure the network layer. Security at each layer is discussed in detail under section II. The presentation (Layer 6), session (Layer 5) and the physical (Layer 1) layers themselves are mostly passive and no attacks are devised to subvert their functionality

The IPSec is often looked as the one stop solution to solve all of the layer-3 vulnerabilities. It will no doubt address major problems like providing confidentiality to the data using cryptographic protocols [5]-[6]. But, the information needs to be protected not only from the confidentiality aspects but we also have the responsibility of guarding the network resources to provide the integrity [7] and accountability [8] which form the complete security triad [9]-[10],[11] and [12].

The OSI layers with the primary security features are depicted in **Figure -2**.

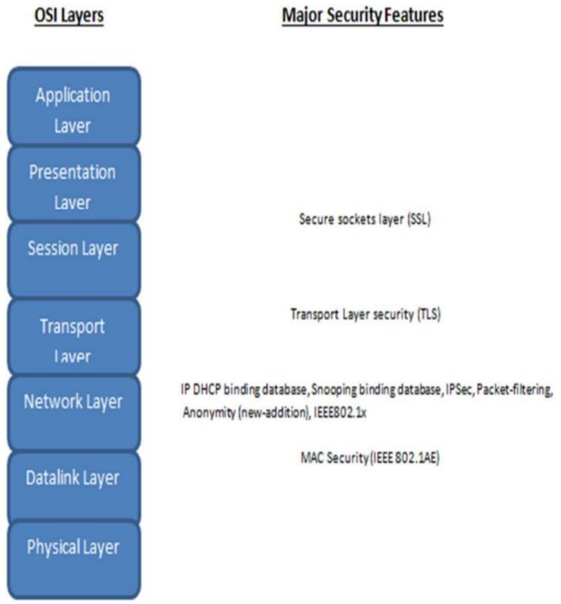

OSI Layers
Major Security Features
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Datalink Layer
Physical Layer
Secure sockets layer (SSL)
Transport Layer security (TLS)
IP DHCP binding database, Snooping binding database, IPSec, Packet-filtering, Anonymity (new-addition), IEEE802.1x
MAC Security (IEEE 802.1AE)

Figure 2: Major Security features of OSI Layers [10]

II. General Security Threats to Smart Grid Infrastructure

The future smart grid is expected to enhance the security and reliability of the existing power system. Without strong security measures in place, however, not only the smart grid will inherit the vulnerabilities of the legacy power grid but also new vulnerabilities will be exposed because of the new technologies introduced in the smart grid.

Many security threats have been reported for the legacy power system until now. In March 2007, the US Department of Energy’s Idaho National Laboratory conducted an experiment named “Aurora Generator Test.” In this experiment the exploitation of a security vulnerability in the SCADA system caused physical damage to a diesel generator [10].Later, in 2008, the Idaho National Laboratory published are port in which several vulnerabilities of the SCADA system were categorized and described [11]. Still, many flaws in the legacy power system might not have been publicly announced. By considering that the smart grid will be built on top of the existing power grid, it is crucial to improve the security of the legacy system.

The supporting technology for the smart grid includes several devices located in physically insecure environments, such as smart meters, intelligent appliances, distributed generation, and storage equipment. These devices have two-way communications with the electric system and therefore add numerous entry points to the grid. Because of their unprotected locations, it is easier for attackers to exploit the vulnerabilities of these devices to either cause local damages or gain access to the more critical parts of the network by taking advantage of the two-way communications. In [12], the authors explained how important data such as authentication keys can be extracted from the memory of a smart meter and malicious codes can be inserted into such a device to launch attacks against other parts of the grid. By considering the large scale of the smart grid deployments, a single software vulnerability in a device, such as a smart meter, can be used to compromise millions of devices.

Wireless technologies are widely used in the smart grid deployments because of their low-cost, low-power consumption, ease of installation, and so on. On the other hand, wireless networks are inherently more vulnerable to several types of passive and active attacks, such as eaves-dropping and denial of service, compared with wired networks because they usually communicate through shared frequency spectrum. The Zig-Bee standard, which is the dominant technology for HANs in North America, is in early stages of deployment, and its security has not been evaluated broadly. Serious vulnerabilities in the Zig-Bee protocol have been reported [13–16].

The smart grid is an attractive target for different attackers with various motivations. Unethical customers, publicity seekers, curious or motivated eaves droppers, and so on [17] might take aims at the grid for a variety of malicious reasons. The smart grid is a critical infra-structure that many other utilities depend on; therefore, not only will it attract normal hackers with less harmful intentions but also terrorists who might want to disrupt the grid as well. When many individuals with high motivations and rich resources aim at attacking the system, the risk of finding and exploiting the vulnerabilities and penetrating to the system increases.

III. LAYER 3 SECURITY THREATS ON THE SMART-GRID NETWORKS

There are broadly three types of attacks; one aiming at disrupting the smart-grid network, he second type of attack eavesdrop on the smart-grid network to collect confidential user information traveling over the smart-grid, and the third attack targets the confidentiality and integrity of the data by false data injection or changing the data in transit. The first attack that threatens the availability of services on the smart-grid is an active attack and is felt immediately. The other two types of attacks threaten the privacy of the user information falls under the category of passive attack, hence are harder to detect [18] and [19].

A. IP Spoofing Attack

In computer networking, IP address spoofing or IP spoofing is the creation of Internet Protocol (IP) packets with a forged source IP address, with the purpose of concealing the identity of the sender or impersonating another computing system. This attack is usually combined with the DoS attack or to repudiate the integrity of the source. IP Source address validation can prevent the IP address spoofing attack. There are primarily two methods available to block these attacks they are Ingress filtering as mentioned under the RFC 2827. This technique lacks the ability to distinguish the spoofed source IP packets if they are originating from the same network. A better approach to this is the Source Address Validation Improvements (SAVI) [2]. The SAVI technique actually binds the IP address to its data link layer address and enforces the IP source addresses match the binding to which they are bound.

The attacker might sometimes try to spoof the IP address of the Dynamic Host Configuration Protocol (DHCP) servers. If security features are not enabled on the layer-2 (like DHCP trusted port) then the attacker might be able to fake the DHCP server and improperly route all the traffic the way he wishes.

The SAVI technique can be added when DHCP snooping is enabled on an untrusted interface. After IP Source Guard (IPSG) is enabled on an interface, the switch blocks all IP traffic received on the interface except for DHCP packets allowed by DHCP snooping. A port access control list (ACL) is applied to the interface. The port ACL allows only IP traffic with a source IP address in the IP source binding table and denies all other traffic. This way we have finer granularity in identifying the spoofed IP addresses in a DHCP environment

B. IP Routing Attack

These are the control plane attacks on the network devices with an intention to spoil the routing table of the layer-3 devices such as router, firewalls and gateways. Most of the routing protocols today have the ability to authenticate the peers prior to sharing the routing information and this feature has to be enabled on all the layer-3 devices for forming the neighborship. The Routing Information Protocol (RIPv2) supports the plain-text password feature [3] to authenticate peers and also a much advanced security feature like keyed MD5 hashing security [4] feature to authenticate peers before forming neighborship. OSPFv2 in its initial RFC supported the MD5 hashing to authenticate the peers. New security features have been proposed to include the HMACSHA authentications in the later RFCs. BGP which is an exterior routing protocol has the same problems as the interior routing protocol. It also has the security features that is to be enabled to provide the authentication to form neighborship [21].

C. Denial of Service (DoS) Attack:

This attack mainly targets the availability of the service. The server providing the service is overwhelmed with the service requests up-to a point beyond its handling capacity. DoS attacks can be leveraged against poor software quality. It can cause application resource exhaustion, operating system resource exhaustion and triggered lockouts and quota exhaustion [8]. Under the DoS mitigation strategies at the network level we must take care to provide Redundancy and Distributed Service, authenticate routing adjacencies and isolate router to router traffic [8]-[22].

D. Man in the middle (MITM) Attack:

This is the attack which typically occurs between the source and destination. Not necessarily all the time do we have the source and the destination connected directly or with no hops. Often times the packet has to travel multiple hops (different routers) to connect to the destination. The attacker will leverage this fact to fabricate himself as the destination by displaying fake routing tables or in the LAN does the ARP spoofing(a layer-2 attack) to cheat the sender to send his traffic to the attacker. Then the attacker will either reply back as the original destination or drop without responding causing a type of DoS to the user. This type of attack can be prevented if we have a mechanism to authenticate the server from the client so that the client will send the packets only after the server is verified to be legitimate. Hence using the TLS or SSL to verify the server from the client before the packets are exchanged is a good idea to protect the integrity of the source and destination at the same time.

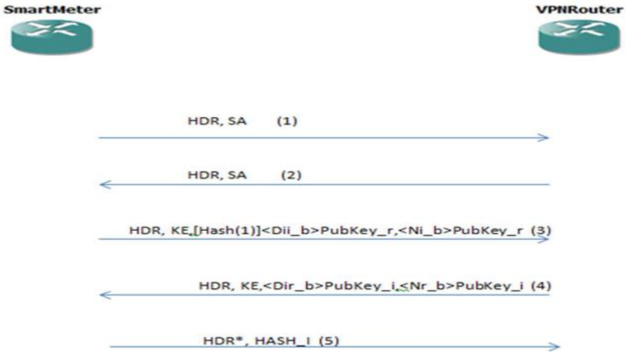

SmartMeter
VPNRouter
HDR, SA (1)
HDR, SA (2)
HDR, KE,[Hash(1)]<Dii_b>PubKey_r,<Ni_b>PubKey_r (3)
HDR, KE,<Dir_b>PubKey_i,<Nr_b>PubKey_i (4)
HDR*, HASH_I (5)

Figure 3: IPSec VPN Setup using Public-Key (Salah et al., 2014)

E. Network Monitoring Attack:

Since the packets flow across multiple hops before reaching the destination the packets flow across multiple networks and the attacker leverages this fact to sniff the network packets for the packets of his interest. If the attacker is motivated to take down the network he will be interested in taking down the access to management plane and will look at the usernames and passwords. If he is interested in making financial gains he will be targeting the information such as credit card numbers etc. Some of the attackers might make a heist by selling the consumer’s personally identifiable information such as SSN, address, power usage, address of residence etc. These attacks can go undetected for long. Hence all the information flowing through the smart-grid network must flow in an encrypted manner. This provides confidentiality to the data. To provide the confidentiality to the data normally IPSec VPNs are used. Initially the keys are exchanged in the VPN establishment phase by Internet Key Exchange (IKE) protocol.

IV. IPSEC SECURITY

Applying IPSec security directly between the consumer networks and the billing sites will decrease the bandwidth on the server side. The service is also affected by the overhead the server's CPU experience to encrypt the packets flowing to and from the clients. Apart from these issues it also causes the dilemma as to who will be exchanging the keys between the smart-meters and the servers. The other problem is the key revocation. Identifying a trusted third party would be even harder. So the IPSec VPNs using asymmetric key cryptography is the only viable option (as mentioned in **Figure-3**). The Trusted Platform Modules can be used in the generation of keys (public and private keys) in the smart meters because of the advantage it provides. Although TPM itself might be vulnerable to side channel attacks the communication occurring using the TPMs are resilient to such attacks. The IPSec VPN setup uses the public-key as mentioned in the **Figure-3**.

The messages 1 and 2 form the IKE security association negotiation phase, the messages 3 and 4 establish the Diffie-Hellman Key exchange, and the messages 5 and 6 authenticate the peer. In **Figure-3** the PubKey_r means the public key of the router and the PubKey_i means the public key of the smart meters. HDR means the ISAKMP header and KE is the key exchange. HDR*: denotes that ISAKMP payload is encrypted, this mean that identities (IDii and IDir) are protected during authentication exchanges (the last 2 messages) [9]-[10] and [11].

Generally, TPM is a specialized chip on an endpoint device that stores RSA encryption keys specific to the host system for hardware authentication. Each TPM chip contains an RSA key pair called the Endorsement Key (EK). The pair is maintained inside the chip and cannot be accessed by software.

V. PRIVACY IN THE SMART-GRID

Since the businesses are mandated by several state laws and federal laws there arises the need to protect the privacy of the consumer data. The attackers might perform known text attack on the VPN traffic and in a long term might be able to decrypt the traffic. Hence, it is essential that a separate privacy protection mechanism be provided by design of the smart-grid. The solution proposed here is that of the Chaum's mixer network [18]. Chaum's mixer network has been in use for protecting the privacy of the users, for web browsing using the onion router (TOR). It has also been used in the anonymous mailing system. Below is the proposed solution which is similar to TOR architecture (the difference here is that it is layer 3 encrypted traffic flowing unlike layer 7 traffic).

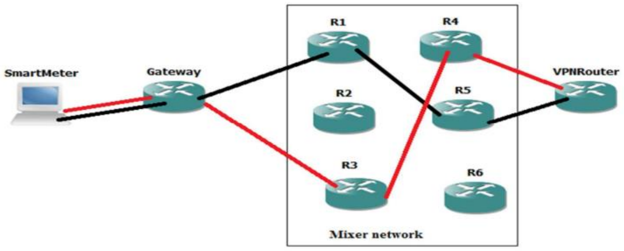


Figure 4: Architecture of Smart Grid Network with a VPN Router

Many of the smart-meters are connected to a gateway (only one is shown for simplicity). The traffic flowing from the source to gateway is encrypted by the public key of the last hop router by the gateway and then by the public key of the previous hops successively. Each of the routers successively decrypts in the reverse way and finally the IPSec packet moves to the destination. The black and red routes depicted are two of the different methods by which the traffic can flow through the mixer network.

Advantages of this method are that the attacker on the internet cannot perform analysis just based on the source IP and destination IPs as these are transformed by the mixer networks. Another advantage is that we have removed the need for another dedicated directory server (as in TOR [20]. Limitation is that the analysis is possible if the attacker is present on the same LAN and we do not have layer-2 security features like MAC binding.

The second approach involves making changes to the DHCP protocol. The idea is to allow the DHCP server to provide a set of IP addresses that it possess in its pool to the pool of clients. Ask the clients to make use of the IP addresses based on some random manner, such that the IP address used by the same client varies each time while communicating. However for making two way communication possible using such method, there must be some device in between which has a track of the MAC to IP binding and the NAT sessions.

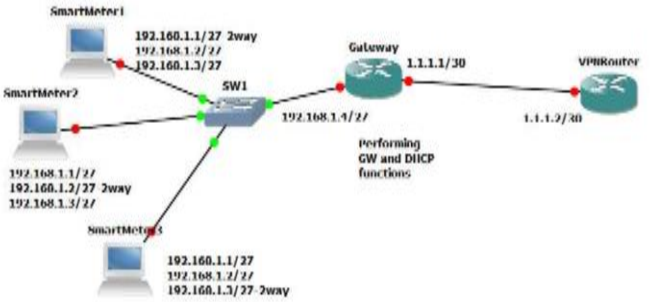


Figure 5: SM network with their allocated IP Addresses

Consider the scenario of the three smart meters for the sake of example. The Gateway provides the allowed DHCP IP address list or pool IP to all the three smart meters and assigns one of the IP as its permanent IP address (purpose being two way communications). Now suppose the smart-meter has three different packets to be sent then it starts out by using IP address randomly allowed from the pool it received from the Gateway. For the first packet it use IP of 192.168.1.2 and for second packet IP address 192.168.1.1 and for the third packet IP address of 192.168.1.3. The person monitoring the network will assume the first and the third packets came from SmartMeter-2 and SmartMeter-3 thus getting deceived in attributing it to a particular consumer.

Now what happens if the two smart-meters happen to get the same IP addresses at an instant? Still, it should not be problematic if the protocol is defined properly. Ideas on how to develop this protocol are as under:

1. The DHCP (GATEWAY) server will maintain the IP to MAC table for each request sent just to maintain the logs.

2. Maintain a permanent IP to MAC address binding on the DHCP server and communicate the two ways IP address a particular host must reserve one particular IP which the DHCP server has provided as the two-way IP address. In simple sense the client has to listen to the replies sent on that particular IP only.
3. No LAN host can communicate on the IP address of the two way IP address if the permanent host is receiving the packets from external IP.
4. The simpler approach would be to create a pool of IP address that is unused and share it with the hosts to use it randomly.

So how should server attribute the packet to the correct host or resolve the host properly? The solution is to send the MAC address of the Smart Meter in the data packet which will be encrypted. For the server to communicate to a particular host it has to get the two way-IP address from the gateway and then communicate back on that particular IP. To further obfuscate the IP address we can clear the permanent IP to MAC mapping in the DHCP [14] used for two way frequently. Thus by randomizing the source IP address using the DHCP we will be able to communicate the data over the internet with assurance of privacy.

VI. Conclusion

The focus of this research paper is securing the network layer or OSI layer 3 in the smart grid network. Different aspects of network security at each OSI layer and the security threats at network layer have been elaborated. An overview of the privacy preserving mechanism has been provided. Apart from the Chaum's Mix networks solution a new solution based on the new DHCP model has been developed. Based on the study of various security threats faced by network at each layer and the possible remedies, the paper concludes that privacy of the customer can best be protected at the network layer using the techniques mentioned.

VII. References

[1] P Ferguson and D Senie, “Network ingress filtering” RFC 2827, 2000.

[2] J. Wu, J. Bi et al., “Source Address Validation Improvement (SAVI) Framework in RFC” 7039, 2017.

[3] G Malkin, “RIP version 2 authentication feature RFC 2453” 2010.

[4] M. Bhatia, M. Fanto , R. White , M. Barnes , Cisco Systems , T. Li and R. Atkinson, OSPFv2 HMAC-SHA Cryptographic Authentication", RFC 5709, 2009.

[5] Atul Aggarwal, Shelej Khera, “Combat Resources Shortages by making Stub Areas and Route Summarization in OSPF”, International Journal of Scientific and Research Publications, 2012

[6] R Rivest (1998), “BGP authentication RFC 1325”, 1998

[7] J. Touch A. Mankin and R. Bonica, “TCP authentication option RFC 5925”, 2013.

[8] Jelena Mirkovi, “Internet Denial-of-Service Considerations” M. Handley, Ed. UCLA E. Rescorla, Ed. Network Resonance, 2002.

[9] Deploying Cisco IOS Security with a Public-Key Infrastructure – Cisco Deployment guide, 2016

[10] C. Bonati, S. Turner et.al, “Requirements for an IPsec Certificate Management Profile RFC 4809”, 2012

[11] Salah, “HENDEL, IPsec VPN, Main mode Vs Aggressive mode”, 2014.

[12] Department of energy office of electricity delivery andenergy reliability. Common cyber security vulnerabil-ities observed in control system assessments by theINL NSTB program, November 2008.

[13] McLaughlin S, Podkuiko D, McDaniel P. Energy theft in the advanced metering infrastructure. Critical Information Infrastructure Security 2010; 6027:176–187.

[14] O’Flynn CP. Message denial and alteration on IEEE 802.15.4 low power radio networks. 4th IFIP International Conference on New Technologies, Mobility and Security, Feb. 2011.

[15] Sokullu R, Dagdeviren O, Korkmaz I. On the IEEE 802.15.4 MAC layer attacks: GTS attack. Second International Conference on Sensor Technologies and Applications, Aug. 2008.

[16] Law YW, Hartel P, den Hartog J, Havinga P. Linklayer jamming attacks on S-MAC. Proceedings of IEEE WSN’05, 2005.

[17] Xiao Y, Sethi S, Chen H, Sun B. Security services and enhancements in the IEEE 802.15.4 wireless sensor networks. In Global Telecommunications Conference, IEEE GLOBECOM’05, 28 Nov - 2 Dec. 2005

[12] David Chaum, “Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms”, Communications of the ACM, 1981.

[13] Shashank Singh, “Layer 2 security for Smart Grid networks by Indukuri N R”, Advanced Networks and Telecommunications Systems (ANTS), IEEE International Conference on Smart Grids, 2012

[14] R Droms RFC 2131, Dynamic Host Configuration Protocol (DHCP), 2012.

[15] TOR and HTTPS, Electronic Frontier Foundation, 2017

[16] CISCO guide to harden CISCO IoS devices 2013.

[17] Irshad, Aamir, Ullah, Ibrar, Khan, N. & Riaz, M., “Reliable and Secure Advanced Metering Infrastructure for Smart Grid Network”. 1-6. 10.1109/ICECUBE.2018.8610995, 2018.

[18] P. Venkitasubramaniam and V. Anantharam, "On the anonymity of Chaum mixes," IEEE International Symposium on Information Theory, Toronto, ON, 2008, pp. 534-538.

[19] G.N. Ericsson, “Cyber security and power system communication - essential parts of a smart grid infrastructure,” IEEE Trans. Power Delivery, vol. 25, no. 3, Jul. 2010, pp. 1501-1507.

[20] G. Kalogridis, S. Z. Denic, T. Lewis, and R. Cepeda, “Privacy protection system and metrics for hiding electrical events,” International Journal of Security and Networks (IJSN), special issue on security and privacy in smart grids, Vo. 6, No. 1, 2011, pp. 14-27.