Smart Grid: Wireless Communication and Cyber Security

Rajiv Bhatia
Dept. Of Information Technology Terna Enggineering College Nerul, Navi-Mumbai 400-706
Email: raj.bhatia247@gmail.com

Varsha Bodade
Dept. Of Information Technology Terna Enggineering College Nerul, Navi-Mumbai 400-706
Email: varshasim@gmail.com

Abstract—Traditional or Unsmart grid is dead. Two way high- speed, secure and reliable wireless-communication is highly desir- able for smart grid. So communication networks play a key role in smart grid .Critical information like power-usage, billing-data, grid-status, control-messages etc are frequently communicated among smart grid elements. The cyber attacks against smart grid corrupts the security of smart grid. Thus this paper summarizes wireless communication technologies widely used in smart grid and possible smart grid Cyber security issues, Vulnerabilities, attacks and their detection in brief.

Index Terms—Smart grid, AMI(Advanced Metering Infrastructure), Cyber security, Attacks, Wireless networks, NAN(Neighbourhood Area Network).

I. INTRODUCTION

Smart grid is recognized by two-way communication of power in electrical network, and information in communication network. Interestingly, smart grid is designed in such a way to replace traditional electric infrastructure which is capable of making the electrical grid work more effectively, securely and reliably by virtue of bidirectional flows of power and communication. Thus such feature ensures numerous functionalities such as accurately and precisely utilizing power via monitoring, providing real-time price to the user by the vendors, inculcating demand response between customers, and power generators and so on.

Smart grid is highly essential for todays power grid because it reduces lot of energy losses and wastage by its efficient monitoring with the help of communication networking capability to distribute power in effiicient way, and thus thereby prevents the huge revenue losses especially with respect to transmission and distribution phases. Another thing is that, electricity on the grid cant be stored, and storage process of it causes lots of losses occured in the process. Therefore smart grid is needed to make generated electricity closely match to the demand. In addition to this, factors such as growing population and demand for energy, the global climate change, equipment failures, energy storage problems, the capacity limitations of electricity generation, one-way communication, decrease in fossil fuels, and resilience problems, lack of automated analysis, poor visibility, mechanical switches causings low response times, lack of situational awareness, etc. as a consequence of which occurs outages and blackout in traditional grid also forms the base for us to go for smart grid.

In smart grid, the Advanced Metering Infrastructure (AMI) is one of the most vital element to obtain efficient status monitoring, control and pricing, automatic meter reading, by deploying a large number of smart meters in homes, buildings and factories. Such smart meters would generates critical data in bulk that should be efficiently and securely collected, imposing a great challenge on communication networks.[9][1]

Interestingly, the vital involvement of the communication networks in smart grid puts a major issue of selection of wired or wireless technology to setup secure, reliable and high-speed communication for smart grid network. The smart grid communication network could be implemented using a variety of media ranging from fibre optic broadband to ZigBee/WLAN, etc. In reality wireless communication is usually more preferable as wireless systems offer the benefits of inexpensive products, quick deployment, zero cost installations, widespread access, and mobile communications which wired technologies often cannot provide. As against this, wireless technologies are widely vulnerable to cyber attacks than wired one's. Thus cyber security becomes a huge hurdle to deploy a secure and reliable smart grid communication network. Also which communication technology should be selected for a particular application of smart grid is wholly dependent on its requirement such as bandwidth, QOS, speed, reliability, no of nodes,future enhancement,cost etc. In case of wired communication, Powerline communication technology can also be used for implementing smart grid network which utilizes existing electric infrastructure for data communication, thus saving enough time and cost in setting it up. Also Power line technology is suitable for cities of skyscrappers where there are big buildings, thus imposing lots of barrier on usage of wireless technology. However an implementation in a region will be different from an implementation in other region; therefore, the communications requirements for the networks that are part of the system are repeated with some differences in each utility and region.Thus various parameters of each wireless technology must be known and its very challenging to decide which wireless technology should be used in smart grid. Interestingly, examining and implementing smart grid security is a challenging work, especially when considering the impact of the potential damages that could be caused by cyber attacks from external or internal entities which results into severe power cuts outages and blackouts.

The need for protecting smart grid data cyber security emerges from the need to interconnect smart grid components with a two-way communication network so as to energy suppliers and cus- tomers can exchange information in an coordination, real-time manner. This capability could leads to enabling features such as load shedding, load consumption management, distributed energy storage (e.g. in electric cars), and distributed energy generation (e.g. from renewable resources). In addition to this
,the need for fine-grained monitoring of smart metering data and grid, the security of an advanced metering infrastructure, transmission and distribution is of utmost importance.

Once an entry gate is found, it becomes less difficult for the attacker to attack down the smart grid. For example, agreement of the real-time pricing channel can result in energy robbing or malicious remote handling of equipments. Hence, there must be the rigorous mechanism through hardware/software security is required to ensure the validity of different communicating elements such as head-ends and smart meters. If an attacker captures the head-end, then probably he might be able to send smart meters a demand response command interrupting power supply. The interruption can be made permanent by also commanding all the meters to change their crypto keys to some new value only known to the attacker[1] .The impact can be deadly and expensive : millions of homes can be left powerless until they are locally replaced or rehashed with authentic keys, people suffer, health and safety could be jeopardized, and businesses could lose millions. Smart grid cyber-security needs to a) prevent such attacks from happening and b) have a recovery/survivability mechanism in case of (successful) attacks.Thus without proper security methods and technology makes smard grid useless.

More generally, using a top-down or a bottom-up approach risks and vulnerabilities in connection to smart grid security can be identified. The top-down approach encompases well-defined user scenarios such as automated meter reading (AMR) and collecting and maintaining billing information, while the bottom-up approach focuses on well-understood security attributes and features such as integrity, authentication, authorization, key management, and intrusion detection.[4]

The rest of the paper is organized as follows. In section II Literature survey inconnection to wireless networks, Cyber Security, PKI Selfhealing is accomplished. Further Section III summarizes with the wireless technologies widely used in smart grid applications and thereby sma Section IV and IV disscusses the Cyber security requirements, Issues,Vulnerabilities, Attacks for smart grid. Finally the paper is concluded in section V.

II. LITERATURE SURVEY

Now talking about the security of the smart grid, there is an attack widely known as false data injection which can lead to severe damage, in which the undesirable, deadly chunk of data is injected particularly when the data is in transit or from the origin, such injected data attack is performed intentionally to do a major damage to the system and is difficult to identify or traced. So inconnection to this a novel security architecture for detecting false data injection is proposed in [3] in which light weight secure watermark is used in meter reading information and that whole data is transmitted over the highspeed and unsecured network. At the receiver side the watrermarked data and original watermark are correlated and the involvement of any such false data can be detected algorithm in relation to this is also shown and from the implementation's view this method can prove effecive. However it can effectively detect the presence of false data but unable to detect the injector. In Power distribution side, the wireless communication technologies are mainly advantageous particularly wireless mesh networks(WMN) because it provides hop to hop communication to effectively sustain itself in case of error or failure. There are various Possible security attacks on WMNs such as Eavesdropping, Jamming, outside attacks and inside attacks with the measures needed to deal with them. In addition an intusion response system is also proposed in [4] which can reveal security attacks in a real time manner. There is strong indication of requirement of strong, lightweight authentication mechanism with easy and efficient key management schemes, secure routing protocols needs to be developed with cross layer design. The physical layer attacks with approprite security measures are also disscussed with respect to wireless technologies in smart grid in paper [5] in which lightweight distributed algorithm Frequency Quorum Rendezvous (FQR) in which there is not the overhead of the knowledge of preshared keys is proposed in connection to effective key managemet. Interestingly, in present situation PKI based technology is suitable for fulfilling authentication the devices of smart grid. PKI however puts less overhead of related calculations. [6] proposes the light weight authentication scheme in which there is mutual authentication of smart meters which are distributed at different hierarchical networks of the SG and establish the shared session key using Diffie-Hellman exchange protocol. Then, with these shared session key between various smart meters and hash-based authentication code technique, the subsequent smartmeter messages can be authenticated in a lightweight way.In[8] concept of Multiagent system based PKI authentication mechanism is proposed in which smart grid devices are authenticated through digital certificates, each smart grid element are designed as the agents which forms knowledge base and can effectively helps in achieving self-healing/self-recovery in smart grid in case of of fault. Various strong light weight Encryption mechanism are also needed to securely transmit the data from various nodes to the collector. The strong Homomorphic encryption mechanism used in [7] to achieve security of data in transit a spanning tree rooting at the collector device is constructed to cover all of the smart meters. Aggregation is performed in a distributed manner in direction to the aggregation tree.

Various wireless technologies for smart grid communication networks are compared on various grounds in [9] which mainly includes wimax, Cellular, Zigbee etc. in addition QOS, reliability, security aspect in connection with smart grid is

discussed. Smart grid implementation differs from region to region, thus these comaparison forms the base for selection of communication technology for smart grid. In [12] Zigbee 802.15.4 wireless technology for the smart grid is disscussed and analyzed,it also shows that it is useful in Home networks and AMI.In [13] wholly about wimax wireless technology for AMI is disscussed and challaenges and issues imposed by wimax.In [14] and [15] the wireless mesh network topology was discussed and compared with other topologies. It was found that the mesh network could supply a reliable, robust, and cost-effective topology for communication.Also wireless technologies for smart grid like zigbee, GPRS, 3G, Wimax etc with advantages/ disadvantages are disscused in detail in[2].

III. Wireless Comunication Technologies for Smart Grid

This section of the paper deals with some wireless technologies widely adopted in implementing the smart grid communication namely 1)Wireless Mesh 2)Zigbee 3)Wimax 4)3G Cellular 5)LTE 6)Wifi 802.11b/g/n.

A. Wireless Mesh Network(WMN)

A wireless mesh network (WMN) is a communications network made up of radio nodes organized in a mesh topology such that every node of the network can be able communicate with other nodes in the range and with router also. Wireless mesh networks often consist of mesh clients, mesh routers and gateways.IEEE 802.11, 802.16, operating on. WMN can be widely used in smart grid as Last-mile access connection upto residence and building nodes meter to meter communication; AMI distribution automation, backhaul , demand response, remote monitoring.WMN provides Non-line-of-sight communication, MIMO configurations, integrated antenna to handle wide range of deployment issues; Easily scalable; Mesh design allows improved coverage around obstacles, node failures and path degradation; also Rapid deployment using unlicensed; Security - SNMPv1/2/3 and data encryption; QoS available. In Addition WMN has disadvantages such as Increased delay/latency introduced by multiple hops; Increased complexity of protocols (MAC, routing, management, security); Increasing density ills the functionality of WMN. WMN provides frequency of 900 MHz, 2.3 GHz, 5.8 GHz andchannel bandwidth 20 to 40 MHz,coverags in WMN is for line of sight (0-15 miles) or non-line of site (0-3 miles) between links.

B. Zigbee (802.15.4)

Based on IEEE 802.15.4, ZigBee is specially designed for low-power and low-cost wireless mesh topology standard for wireless home area networks (WHANs) and or personal area network (PAN) to remortely monitor and control applications. ZigBee enables robust self organized wireless mesh networks with self-healing capability and allows end devices to work for years on battery power and can support large number of users.Zigbee is used in smart grid as Home area network for energy management, meter reading and monitoring: Smart meters; Smart lighting, appliances and electronic equipment.Zigbee supports frequency range such as 865 MHz , 910 MHz, 2.5 GHz (unlicensed); bandwith of 22 MHz with coverage of around 50 meters.Data rate of Zigbee is 20 to 250 kbps, depending on frequency band.

C. Wimax

WiMAX is a wireless communication for long range that can transport application data to and from terminal devices that use an intermediary wireless interface, such as ZigBee or WiFi. This is a likely situation for many smart metering applications, at least initially, with meters transmitting data to concentrators connected with WiMAX base stations.Wimax uses various standards such as IEEE 802.16d-2004, 802.16e-2005, etc frequency range of 2 to 2.5, 3.4 GHz licensed; 445 MHz, 700 MHz also used. Moreover in smart grid wimax is used as AMI Backhaul, SCADA Backhaul, Demand Response, Mobile Workforce, Video Surveillance applications etc. Wimax provides many advantages such as Efficient backhaul of data-aggregating 100s access points; QoS supports Service Assurance; Battery backup improves reliability and security; Simple, scalable network rollout.Wimax also issues several disadvantages like Limited access to spectrum license; higher bit rates overhead over longer distances; asymmetrical up- and downlink speeds; shared bandwidth; competing with 4G cellular standards for high-capacity and IP networks.Wimax gives wide coverage 3-5 miles; longer distances capability with lower bit rates and data rate of Typically 4-16 Mbps

D. 3G Cellular

3G is a cellular technology that includes wide-area wireless voice telephone, video calls, and wireless data, every thing in a mobile environment.This wireless technology can used as AMI Backhaul purpose, Communications Network, Mobile Workforce in smart grid.Nowadays 3G cellular technology is Widely deployed, stable and mature; standardized; equipment prices keep declining; Readily available expertise in deployments; the cellular chipset of it very inexpensive; Large selection of vendors and provides coverage of over 100 km.

E. LTE

LTE is a Low latency, high capacity, Low power consumption wireless technology Mainly for mobile carrier adaptation; Next-generation network for mobile telecommunication providing high spectral efficiency, very low latency, improved user experience, is fully integrated with 3GPP, and provides data rate of 2.0 Mb/s with coverage of approximately 120 km .LTE can be used in smart grid as AMI Backhaul, SCADA Backhaul, Demand Response, Mobile Workforce, Video Surveillance application so as to transmit the data for longer distances.

F. Wifi 802.11b/g/n

It is a Inhouse wireless local area networks, wireless mesh networks based communication technology. This wirelesss technology can be used in Home area network, home automation applications of smart grid. It is a low cost technology with

mature standards.Frequency range for is 2.3 and 5 GHz. It has disadvantages like Small coverge and short distances which limits widespread use of it; Security issues with multiple net- works operating in same locations. Thus these were the wire- less technologies maily adopted to accomplish the smart grid communication necessities. Thus which technology should be selected and used for any particular scenario depends wholly on its architecture. But WMN technology is widely used in distribution domain/AMI(Advanced Metering Infrastructure) of smart grid, because multihop wireless networking is definitely necessary, as electric equipments out of communication range of each other need to exchange information. To simplify net- work organization and maintenance, the entire network must in a way to be self-organized. Moreover, communication modules in an SDG may also includes heterogeneous properties in terms of communication range, computing power, and power efficiency. Thus these requirements occurs in the advantages of WMN's, hence WMN is suitable for communication at distribution domain/AMI of smart grid.

G. Wireless Sensor Networks(WSN)

Previously Monitoring and diagnostic operation in traditional grid were typically implemented in wired communications but these were pretty expensive as cables are required, installed, maintained which unnecessarily increases the burden. Efficient mon- itoring systems can be constructed by largescale deployment of smart sensor nodes which can provide complete information on the conditions of smart grid elemets comprising of generating units, transformers, transmission lines, motors, and each and every component in the grid etc in a remote and online means. By the online system monitoring and system- level coordinating controls and protections, a single system contingency in the power grid or facility can be detected and isolated before it causes hazardous consequences and results to more catastrophic system breakdowns.

In Smart Grid systems, wireless multifunctional sensor nodes should be installed on the critical equipment of the smart grid and monitor the parameters critical to each equipments condition. Such information enables the smart-grid system to respond to the changing conditions in a more proactively and timely manner. In this regard, WSNs play a vital role in creating a highly reliable and self-healing smart electric power grid which rapidly responds to events with appropriate actions and the system can be protected from the failure.[10] The existing and potential applications of WSNs on smart grid span a wide range, including Wireless Automatic Meter Reading (WAMR), remote system monitoring, equipment fault diagnostics, line monitoring etc. However, the realization of these currently designed and envisioned applications directly depends on effcient and reliable communication capabilities of the deployed sensor networks

IV. GENERAL SECURITY REQUIREMENTS AND THREATS

Generically, security requirements for managing data can be classified as follows:

- Confidentiality. data must be accessed only to authorized entities and none other, and that intentional or unintentional disclosures of the data do not occur.
- Integrity Requirement that data is authentic, correctly reflecting the source data, and complete, without unauthorized modifications, deletions, or additions. (This does not imply the data is valid, only that it is the same as the source.)
- Availability. Requirement that data is accessible by authorized entities whenever they need it.
- Non-Repudiation. Entities receiving the data do not subsequently deny receiving it. The reverse is also true: that if the entities did not receive the data, then they cannot subsequently state that they did receive it.

V. CYBER SECURITY ISSUES, VULNERABILITIES ,ATTACKS IN SMART GRID

Each line of the table I is an individual low-level attack technique that can be used alone or in combination with other techniques to build complex attack scenarios. AMI is taken as an application of smart grid in the table. The table also shows the information necessary to detect the attacks.[11]

The information required for detection can be organized into three categories:

- System Data. status reports from smart meter, and gateways (CPU,energy, battery usage) , firmware and software integrity of AMI devices, clock coordination.
- Network information NAN collision rate, packet loss, response time, traffic rate, status and integrity of routing table, connection between physical addresses and node identity.
- Policy information. Legitimate AMI protocols, devices, trafc patterns, authorized route updates, authorized firmware updates.

A. Effective Countermeasures for security attacks in Smart Grid

In smart grid communication network critical messages are communicated frequently in real time. Thus these should be protected from any of the security attackers whether inside attacker or outside. Therefore strong security mechanism and monitoring system need to be implemented in plural. In addition smart grid system should ensure self-healing/self- recovery and fault tolerance capability to tackle with any emergency, problem or damage.

1) Physical Layer Security. A physical layer attack is defined as malicious behavior disturbing legitimate communication on a wireless network. Attack is performed by injection of false data by the attacker to bring down the performance of the system or to accomplish a major damage. The attacks in this category are regarded as DOS(Denial of Service), eavesdropping, jamming, restricting access, and injecting. Eavesdropping can be mitigated by advanced cryptography. Encrypting packets hinders unauthorized nodes from reading data easily.

Category	Attack type	Target	Needed Information
DoS	Packet Transmission conflict	AMI Link Layer	AMI collision rate, node response time
DoS	Packet Flood	Node in AMI (Meter/DCU)	CPU and memory usage of target incoming network traffic to target, authorized network protocols, network health information, packet-per-second rate, node response time
DoS	Jamming	AMI Physical Layer	AMI signal level, node response time
DoS	Alter Routing Table	Routing Protocol	Routing table health, node response time
DoS	Drop Packets	AMI Traffic	Packet loss among nodes in mesh network
DoS	Time-Desynchronization	Node in AMI (DCU)	Time-synchronization traffic among nodes or time congured on nodes
DoS	Resource Exhaustion (Battery Bandwidth, or CPU)	Node in AMI (Meter/DCU)	Trafc among meters, valid trafc prole or node health (CPU, battery consumption), network health (bandwith usage)
Spoofing	Impersonate Regular Node	Node in AMI (Meter)	Associations between physical addresses and node identity
Spoofing	Impersonate Master Node	Node in AMI (DCU)	Associations between physical addresses and node identity, associations between regular and master node registrations
Spoofing	Man-in-the-Middle	AMI Traffic	Associations between physical addresses and node identity
Spoofing	Wormhole	AMI Traffic	Associations between physical addresses and node identity, routing table integrity/update
Spoofing	Slander	Distributed Detection System	Integrity of trust and reputation system
Eavesdropping	Passively Listen to Traffic	AMI Traffic	N/A (undetectable)
Eavesdropping	Active cryptoanalysis	AMI Traffic	Trafc among meters
Physical	Compromise Meter	Node in AMI(Meter)	integrity of meter firmware, memory contents of meter, meter firmware upgrade policy, meter status, information about bandwidth and wireless signal
Communication	Attack Coordination	Traffic in AMI	network protocols that are authorized for use, network traffic among the meters, network characteristics of legitimate traffic

TABLE I
CATALOGUE OF ATTACKS AND DATA REQUIRED TO DETECT THEM

Jamming can be mitigated through active and passive anti jamming techniques. E:g spread spectrum techniques can be applied to reduce the impact by intentional jamming signals. The passive schemes through monitoring electromagnetic emissions in the frequency band of wireless network for an smart grid. If abnormal jamming signals are detected, the next key step is to locate the jamming source. In this way, a security attacker can be captured. To get rid of injection attack only effective Authention at higher layers can alleviate it.

2) Strong Authentication Mechanism. Strong Authentication mechanisms need to be adopted very strictly in order to prevent the system from external attackers. PKI(Public Key Infrastructure) based authentication is regarded as the best for smart grid systems as it involves less processing overhead of keys. Hierarchical light weight authentication mechanism from macro to micro center needs to be adopted.
3) Effective Intrusion Detection System to wipe out insider attackers. Now to protect the system from legitimate or illegitimate nodes who have bypassed the authentication system, Strong IDS needs to be developed and adopted to eradicate inside security attacker nodes. Moreover IDS should detect quickly the attackers and respond in timely manner. In addition secure MAC and routing protocols needs to be implemented as per the system architecture and design. Strong key management schemes need to be implemented.

B. Self-healing

self healing refers to self recovery of the grid in case of tragic blackout/outages and restore its state automatically. Interestingly, to obtain such a feature, artificial intelligence based Multi Agent System scheme is employed in which ideas and programs can be injected. .Software agents comprising of ideas gives flexible and autonomous actions and are out to eye on energy consumption, status of the elements in grid, power quality for voltage irregularities, outages or power flow issues, security, etc. These agents forms knowledge base by getting the information from other agents, helps to form decision support system. Each agent in the network has the characteristics of collaboration, autonomy, and self-learning. Thus these agents smells the outages/blackout occurence in earlier stages, detects them and provide self healing. Agents work in companion and isolates the micro grid from main grid in case of security attack or fault. Thus it ensures the immunity of the system from blackout.[8]

C. Fault tolerance

Smart grid is highly interlinked network, on fault arrival, must be eradicated automatically without human intervention and thus such challenge must be addressed through fault tolerance means such as redundancy or monitoring and its effect must not be felt. Fault tolerance is a major challenge

in modernizing the electric power system. A fault in the transmission system is detected (by the relaying system) and cleared. The transmission system is highly interconnected: its architecture provides fault tolerance by redundancy. The fault can be hardware or software fault. As with the power system, the architecture of the overall system must be designed to cope with these faults. Fault containment is as possible in the communica tion and control system as it is in the power system.

D. Assured and Reliable Integration in AMI of Smart grid

The most widely discussed smart grid security challenges concern the protection of smart metering data against unautho- rized access, repudiation, tampering etc. This is an important requirement without which meter data will not be trusted by either the utility providers or the customers.So the hurdle the security of the meters and its data,thus, Solutions are required on different levels: high end to end secure communication and reliable protocols are need to be used, hardware components (e.g. smart meters) should be designed so that to withstand physical attacks, the grid should detect compromised or hacked components readily and nullify them quickly, and smart meter software should be bug-less. AMI communications security requirements can be addressed by combining existing crypto- graphic key protocols and tamper-proof hardware solutions, by exhaustively testing equipment and software against all sorts of major attacks, and by adopting an open reliable and secure architecture for further testing and secure updating. The AMI system must be designed that will balance the disturbance between security and performance, i.e. usage of adequate security measures while minimizing its power usage and cost overheads. In the future,

need of smart grid/metering communications may arise to integrate with heterogeneous network systems, Internet applications, extension etc. For example,a customer while in roaming wishes to use the power at any remote place way away from his meter but wants to impose its usage data from its own meter, such a service may put a further changes in the future of smart grid network. Such a type of scenario minimizes the meter deployment and reduces its density and less overhead in almost all aspects of AMI. In such an example, it will be necessary to establish secure communication protocols between different players of AMI such as a home smart meter, a mobile phone, a smart power appliances and the customer. Interestingly, customer may also additionally wish to allow third parties get access to its smart metering information in interchange for various services such as free entrance to facilities, or the customer may wish to remain anonymous. In addition one can also envisage further challenges arising as smart grid communication systems integrate with other communication systems: home entertainment systems, medical communication systems, and traffic monitoring communica- tion systems, just to name a few. Interestingly, these additional enchancements of Integration of services and interfaces further gives rise to a total new range of security and privacy vulnera- bilities and requirements and thus thereby increases the risks.

Thus its highly need to understand about the risks involved in such interconnected and complex computing, communications and energy management environment, how the compromise of one system leads to compromise of a downstream system. Risk cum vulnerability analysis should be made so as to able to detect both proactive and reactive system abnormality and take appropriate measures for the same [1]

VI. CONCLUSION

Thus in this paper we discussed about various wireless technologies for smart grid on various grounds such as fre- quency, coverage, advantage/disadvantage etc,this helps in deciding which wireless technology is eligible for any partic- ular application of smart grid. Further we disscussed about cyber security of smart grid containing various issues like selfhealing, fault tolerance, vulnerabilities, security attacks etc. Thus wireless communication and cyber security are integral part of this paper.

REFERENCES

[1] Z. Fan, P. Kulkarni, S. Gormus, C. Efthymiou, G. Kalogridis, M. Sooriya- bandara, Z. Zhu, S. Lambotharan, and W. H. Chin, ”Smart Grid Commu- nications: Overview of Research Challenges, Solutions, and Standardiza- tion Activities,” IEEE Communications Surveys & Tutorials, Vol. 15, No.1, First Quarter 2013 .

[2] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke, :Smart Grid Technologies: Communication Technologies and Standards,” IEEE Transactions On Industrial Informatics. vol. 7, no. 4, pp. 529-533, November 2011.

[3] S. Bhattarai, L. Ge and W. yu, ”A Novel architecture against False Data Injection Attacks in Smart Grid,” IEEE ICC 2012 Communication and Information Systems Security Symposium.

[4] Xudong Wang,and Ping Yi, ”Security Framework for Wireless Commu- nications in Smart Distribution Grid.” IEEE Transactions On Smart Grid., vol. 2, no. 4, December 2011

[5] E. K Lee ,M. Gerla and S Y Oh,”Physical Layer Security in Wireless Smart Grid,” Cyber Security For Smart Grid Commucication IEEE Communications Magazine,2012.

[6] MM. Fouda, ZM. Fadlullah, N. Kato, R. Lu and X. Shen, ”A Light weight Message Authentication Scheme for Smart Grid Communications,” IEEE Transactions On Smart Grid, Vol.2, No.4, December 2011

[7] F. Li, B. Luo, and P. Liu, ”Secure Information Aggregation for Smart Grids Using Homomorphic Encryption,”

[8] V. Dehalwar, R. K. Baghel and M. Kolhe, ”Multi-Agent based Public Key Infrastructure for Smart Grid ,” The 7th International Conference on Computer Science & Education (ICCSE 2012), July 14-17, 2012. Melbourne, Australia

[9] Q. D Ho, Y. Gao, and T. L. Ngoc., ”Challenges And Research Opportunities In Wireless Communication Networks For Smart Grid, ” IEEE Wireless Communications Open Call. pp.89-92, June 2013.

[10] V. C. Gungor, B. Lu, and G. P. Hancke, ”Opportunities and Challenges of Wireless Sensor Networks in Smart Grid,” IEEE Transactions On Industrial Electronics., vol. 57, no. 10, October 2010

[11] D. Grochocki, J. H. Huh, R. Berthier, R. Bobba, A. A. Cardenas and J. G. Jetcheva, ”AMI Threats, Intrusion Detection Requirements and De- ployment Recommendations,” IEEE SmartGridComm 2012 Symposium - Cyber Security and Privacy, 2012

[12] Q Zhang, Y. Sun, and Z. Cui, ”Application and Analysis of ZigBee Technology for Smart Grid ,” International Conference on Computer and Information Application(ICCIA 2010,2010

[13] R. Mao, and V. Julka, ”WiMAX for Advanced Metering Infrastructure,” 2012 International Conference in Green and Ubiquitous Technology,2012

[14] P. Yi, Y. Wu, F. Zou, and N. Liu, A Survey on Security in Wireless Mesh Networks, IETE Tech,

[15] Daintree Networks. (2007). ”Whats so good About mesh networks?” Available: http://www.daintree.net/downloads/whitepapers/ mesh-networking.pdf