Asian Journal of Convergence in Technology **Volume V Issue I**
ISSN NO: 2350-1146 I.F-5.11

Architectural Integration for Wireless Communication Security in terms of integrity for Advanced Metering Infrastructure-Survey Paper

First A. Priyanka Halle, *Veltech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India,* Second B. Dr.S.Shiyamala, *Veltech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Chennai, India.*

***Abstract*— At present, cyber-security has become very significant problem. The universal security integration give number of cyber-security standards. These standards deliver different digital security methods which are established to escape cyber-security attacks. These standards suggest general outlines and accurate techniques for implementing cyber-security. For architectural integration the cyber-security standards play vital role. In this paper, authors are trying to improve wireless communication security for Advanced metering infrastructure by providing reliable architectural integration in terms of integrity.**

AMI is key part of the Smart Grid (SG). From the collected work it is clear that, AMI provides efficiency, reliability, scalability and privacy but due to security problem it lowers the performance. Wireless communication security of AMI to be determined by considering four parameters that is confidentiality (C), integrity (I), availability (A) and accountability (Ac) or non-repudiation. The number of researchers has done work on wireless communication security for AMI but stagnant there is enormous problem of security. Because of still no one researcher has considered four security parameters. By considering these four parameters we can see drastic change in wireless security for AMI. Improvement in these parameters, AMI will be more advanced. But in this paper we are going to focus on wireless security for AMI in terms of Integrity only.

AMI totally depends on wireless communication network. And now days AMI suffers from various cyber-attacks on wireless communication network. A security framework and architectural integration are the things necessary for confident communication of data and control messages. Existing security algorithms are not suitable for smart grid data communication because of their large execution time, more cost and the requirement of more memory. This paper tries to provide security algorithm in terms of integrity with less time and cost. After surveying the existing security solutions in this area, we propose for wireless communication security WiMAX technology (Worldwide Interoperability or Microwave Access Smart architectural integration is very essential for AMI. Infrastructure of AMI consists of basic steps like power generation, substation and distribution. Different attacker attacks on AMI infrastructure. By improving architecture we can make AMI more secure.

Keywords -Architectural integration, AMI, Security, Communication Standard, Integrity.

I. INTRODUCTION

For Architectural integration cyber-security standards piece an important role. To shield the cyber infrastructure, National Cyber-Security Division (NCSD) has accredited two important purposes: To paradigm and maintain a successful national cyberspace response system and to apply a cyber-risk management program for protection of critical infrastructure [1]. A security strategy should have two goals:

1. To avoid the hacker from getting access to critical data
2. To slow down the hacker enough to be caught

I. When planning a security policy, care is needed to be taken to identify precisely what you are trying to protect and while we think about the architecture for security above mentioned two security policies should be considered. Table 1 gives brief idea about standards for cyber security which is helpful for architectural integration [1]. These standards give policies for security purpose in architectural integration. AMI security has become a demanding problem nowadays because of its integration with the external networks, remote system and Internet world. Today's metering infrastructure employs computer based monitoring and control operations to enable application of one network to exchange data with other application of different network. Communication protocol, network topologies, and computerization plays vital role to make the metering infrastructure advanced. Metering infrastructure plays significant role in the smart grid and acts as a vital interface between utilities and its consumers. A metering network comprises a large number of different types of energy meters like advanced meters and legacy meters. To achieve the vision of smart grid, similar metering network can be integrated for exchanging the usage data and taking necessary control actions [2].Cyber-attacks are always linked with the computer networks and communication protocols. It can easily affect the communication of AMI applications [2].Thereby it can degrade the performance. Hence by providing smart architecture integration, cyber-attacks can be removed. This paper further describes different architecture integration techniques, various communication standards for security, parameters for controlled architecture and different algorithms and methodologies.

II. By initiation of malicious cyber-attacks, cascading failures may be triggered from the control system in the substation, thus components in the power system can be de-energized and operation can be irritated. Cyber-attacks may hamper the tripping of a breaker or even shut down the generator. There are different types of cyber-attacks done on AMI. Due to attack, it effects on performance of smart grid. Consequently now a day the developing electricity sector is increasingly dependent on information technology and communication infrastructure. The different architecture integration can help to improve the communication infrastructure. The security of the power system is dependent on it stability to resist the cyber-attacks targeting the general transmission lines [3].

AMI's key action is to accumulate and evaluate the data dynamically from smart-meter which is in the evidence of customer. It also delivers various services like on-demand applications, billing information, etc. It helps the customer to directly participate in the working of smart grid [4]. As a vital part of the smart grid, security of the AMI is of chief significance to ensure secure, reliable, and efficient power distribution to the end users of the grid system. Secure and reliable authentication of smart meters and data collectors connected in the network is the key step to ensure compliance of AMI system with the security requirements of smart grid. The existing preparation for secure authentication of smart meters includes storing cryptographic keys in non-volatile electrically-erasable programmable read only memory (EEPROM) or continually battery-powered static random access memory (SRAM). Hardware cryptographic operations are also used to protect the keys. However, nonvolatile memories are helpless to spoofing and invasive attacks. Also, additional battery-backed tamper detection circuitry is required to protect the smart meters against such attacks. The existing process of authenticating the smart meters is expensive in terms of design and power consumption [5]. Table 2 shows different wireless communication technologies used in AMI recently.

Figure 1 shows the requirement of AMI. From the figure 1 it is clear that security is very important parameter for AMI. Security required in each layer. But this paper tries to provide security only three layers.

1. Pole top to Network operating system
2. Meters to pole top
3. Home to meter

Integrity means that the sensitive data should be neither modified nor deleted in an unauthorized or undetected manner. Power Company can obtain the users' data about their consumption and sale electricity, and the customer can get the adapting electricity price information from Power Company through AMI. The consumption data can help the power company to use energy efficiently. The electricity price helps customers to arrange the use of their electrical appliances in

order to reduce the cost. If the hacker tempers the consumption data, the power company may make wrong decision on power generation. Subsequently electricity sector degrades the performance. In addition, if the customers get the wrong price, they will arrange their electrical appliances according to the false price. It can result in large-scale power outages. Therefore, the integrity of the data is important in AMI. Power Company can also send control command to smart meters. In the worst situation is that the attackers to launch disconnect commands to millions of meters through imagining meter management system. AMI in smart grid requires not only data integrity, but also the integrity of the control command. It is also very important to prevent unauthorized control commands transmitted from AMI system to a smart meter or gateway [6]. Figure2 shows AMI communication system Architecture [7].
In Smart Grid, the electric power is delivered to consumers through two components viz., the transmission substations(TS) and a number of distribution substations (DS). The AMI communication architecture is introduced in the lower distribution network, (i.e. from the distribution substation placed in different regions) connecting the entities of Smart Grid together through different network technologies. The Advanced Metering Infrastructure comprises following components [7]:

Smart Meter: The smart meter collects and sends the meter reading data periodically to the control center and thus monitors and optimize the power consumption. A smart meter itself consists of three main components viz. a meter to record the energy generated or consumed, a computer to process and log the data, and a modem to connect to the network.

• Gateway/Access Points: It acts as an interface between the smart meter and the control Centre. It forwards the control commands and meter reading data disseminated by the control Centre and smart meters respectively
• Control Centre: It receives the real time metering information from the network, performs the data storage and processing to generate the control commands to monitor and regulate the smart power generation, transmission and distribution throughout the grid.

• Communication Architecture: It facilitates the bidirectional communication path among the entities of AMI for disseminating the metering and management messages.

Due to its importance, AMI is gaining more and more attention towards the communication mechanisms to be deployed. The communication infrastructure of AMI is an amalgamation of different network technologies including both wire line as well as wireless mechanisms. Wired technologies for the AMI network include Ethernet, Power Line Communications (PLC) or Data over Cable Service Interface Specification (DOCSIS) as preferred choices. Whereas, Worldwide Interoperability or Microwave Access (WiMAX), Bluetooth, 802.11s and cellular standards, such as 3G, 4G, and LTE are the promising wireless technologies. We have considered each base station to be deployed for a specific service area, communicating with the smart meters in its realm. As shown in the Fig. 2 the AMI communication net-work is divided into a number of hierarchical networks classified according to the geographical domains and features:

• Wide Area Network (WAN): It provides the connectivity among WAN base station, its local management office, Central SCADA system and Access Point/feeder acting as a NAN Gateway. The WAN uses mostly wired communication such as fiber optical technologies or wireless broadband such as WiMax technologies as a backbone network to provide long range, high speed data and bulk delivery across domains [8].

• Neighborhood Area Network (NAN): NAN facilitates communication between Access Point/feeder and smart meters which play the role of HAN gateway. This net-work covers a few hundreds of nodes in its premises. This network is implemented using wireless communication technologies such as cellular systems, multi hop wireless networks due to its advantages of low cost, reduced complexity and providing access extension with-out requiring cables to accommodate data pipeline.

• Home Area Network (HAN): The network connects all the intelligent home appliances with the smart meter to monitor and optimize their power consumption. In Fig. 4, a HAN network is simply represented by a smart meter node associated with each terminal consumer. The HAN requires short range, typically low bandwidth network. The most prominent network technologies include Blue-tooth, IEEE 802.11(WiFi), ultra wideband (UWB), 802.15.4 ZigBee and 6LoWPAN [9].

The smart meters located at the customer's premises send the meter reading data to the Local management office associated with each DS via Access Points or Feeders serving as a gateway or forwarding station. The Access points/feeders also work the other way round i.e., it communicates the control commands or management messages from the base station to the smart meters to optimize the power consumption of all intelligent home appliances. The local management office serves as a computer Centre to its associated DS. The meter readings of each consumer is collected at the local management office and aggregated to further transmit them to the Central SCADA system for data processing, storage and demand analysis to optimize the power generation and distribution.

TABLE I. CYBER SECURITY STANDARDS AND POLICIES PROVIDED BY THE STANDARD

Cyber Security Standards	*Policies/Services provided By the standards*
ISO/IEC 27001:2013 International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC).)	It specifies a management system that is intended to bring information security under explicit management control.
Standard of Good Practice	The Information security Forum (ISF) published a Comprehensive list of best practices for information security.
North American Reliability Corporation (NERC)	These standards are used to Secure bulk electric systems although NERC has created Standards within other areas.
National Institute of Standard and Technology(NIST)	It provides computer security policy.
ISO 15408	It allows many different Software applications to be integrated and tested in a secure way.
Request for Comments(RFC)	The RFC 2196 provides a general and broad overview of information security including network security.
ISA/IEC-62443 (formerlyISA-99)	It defines procedures for implementing electronically secure Industrial Automation and Control System.

TABLE II. WIRELESS COMMUNICATION TECHNOLOGIES FOR AMI

Technology	*Application*	*Data Rates*	*Approximate Coverage*
ZigBee	Used for HAN ,home appliances and AMI	250Kbps	10 to 100m
HomePlug	It is power line uses for electricity wiring to communicate in HAN	14Mbps 200 Mbps	300m
WiMAX	Demand Response, AMI,WAMI	75 Mbps	50Km
Cellular G3-PLC	SCADA and controlling for RTUs AMI, Demand Response, monitoring for remote site	240 Kbps 33.4 Kbps	50Km 6Km
Satellite	AMI,WAN	450 Kbps	Depends on no of satellites and their beams

Fig. 1. AMI requirement

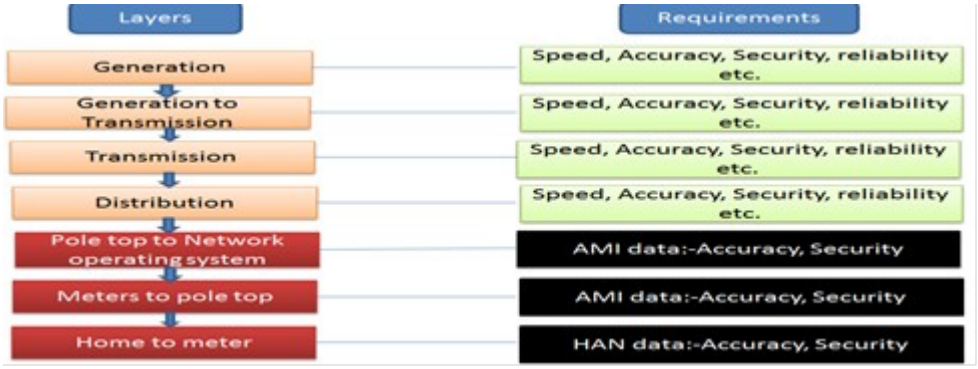
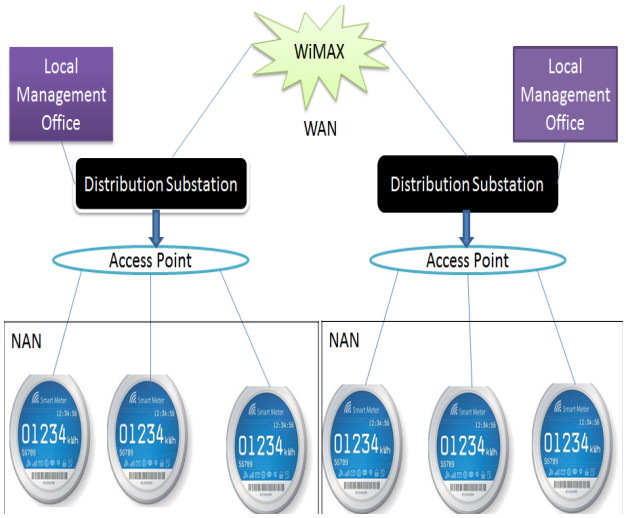


Fig. 2. AMI communication system architecture



II. STATE OF THE ART

This section provides circumstantial on security in terms of I. The overall idea of AMI communication network shows in figure 1[4].For this communication network security can be provided in terms of integrity which shown in table 4. Advanced Metering Infrastructure (AMI) becomes one of the most realistic and commercial systems in power grid since smart grid has been introduced, but its security issues are not cleared yet because of both economic and technical problems. However, the infringement of privacy becomes under controversy recently, security cannot be an option in deploying AMI system any more. In this paper, we propose the security architecture for AMI system after defining some security requirements, and then the AMI security protocol in more details. The emulation board is implemented in FPGA type to verify that our research is reasonable and realistic [10].

There are different algorithms and protocols are available for wireless security for AMI in terms of integrity. But there is lot of drawbacks having some protocols and algorithms. Table4 shows different algorithms and protocols for wireless communication.

First, confirm that you have the correct template for your paper size. This template has been tailored for output on the A4 paper size. If you are using US letter-sized paper, please close this file and download the file "MSW_USltr_format".

A. Maintaining the Integrity of the Specifications

The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

III. PREPARE YOUR PAPER BEFORE STYLING

Before you begin to format your paper, first write and save the content as a separate text file. Keep your text and graphic files separate until after the text has been formatted and styled. Do not use hard tabs, and limit use of hard returns to only one return at the end of a paragraph. Do not add any kind of pagination anywhere in the paper. Do not number text heads-the template will do that for you.

TABLE III. WIRELESS COMMUNICATION SECURITY TECHNIQUES AND DIFFERENT ALGORITHMS FOR AMI IN TERMS OF INTEGRITY

Sr. No.	*Name of the paper*	*Wireless security technique/Algorithm for AMI in terms of integrity*	*Simulation Platform*
1	Bit masking based Secure Data Aggregation Technique for Advanced Metering Infrastructure in Smart Grid System	Bit masking technique for collecting the smart meter data in AMI communication, AES algorithm.	Matlab Simulink
2	Hardware-based Novel Authentication Scheme for Advanced Metering Infrastructure	a novel authentication and key management scheme based on Configurable Ring Oscillator Physically Unclonable Functions (ROPUFs)	Xilinx Spartan 3E FPGA boards.
3	Wireless communication security in terms of Confidentiality, Integrity, Availability and Accountability for Advanced Metering Infrastructure	Algorithm is a combination of Rivest-Shamir-Adelman (RSA) and AODV2MAP is the Adhoc on-demand distance vector multiple alternative path (AODV-MAP)	
4	Energy-Theft Detection Issues for Advanced Metering Infrastructure in Smart Grid	SVM technique , state-based detection technique, SVM algorithms, P2P computing algorithms, cryptographic algorithm, Genetic Algorithm (GA), (HPC) algorithms	
5	PUF-based solutions for secure communication in Advanced Metering Infrastructure (AMI)	Physical Unclonable Function (PUF) technology in communication parties, authenticated key exchange protocol, Okamoto and Schnorr protocols	
6	A Response Cost Model for Advanced Metering Infrastructures	cost model using ArcGIS for topology generation, shortest path algorithm	Grid L AB-D for grid simulation
7	A Survey on Wireless Security: Technical Challenges, Recent Advances and Future Trends	(RSA) public-key algorithm, AES algorithm, AES algorithm ,PHY-CRAMR and PHY-AUR techniques	Ray tracingtool
8	Security Architecture for Advanced Metering Infrastructure	Block cipher ARIA-GCM-128Hash function SHA-1Random number generator CTR_DRBG(NIST)Public key encryption ECIESDigital signature EC-KCDSAKey agreement- ECDH	Xilinx ISE10.1 XST
9	Advanced Metering Infrastructure Security Issues and its Solution: A Review	intrusion detection system, encryption algorithm	KDD'99 dataset
10	Security Architecture Modelfor Smart Grid Communication Systems	AMI Group Security Architecture Model, public key algorithm, Hash function, symmetric key algorithm	
11	Wireless AMI Application and Security for Controlled Home Area Networks	Channel Switching Algorithm, Load profiling algorithm	

TABLE IV. DIFFERENT ALGORITHMS/PROTOCOLS FOR INTEGRITY

Sr. No.	*Different Algorithms/Protocols for Integrity*	*Advantages*
1	DLMS/ COSEM (IEC 62056), DLMS/COSEM supports AES GCM 128 cryptography	More flexible, cheaper
2	Distributed algorithm, ECC algorithm symmetric key cryptography with the use of Bloom's key pre distribution scheme.	Simple
3	AMI Sec Checker, auth-algorithm	Simple
4	Sophisticated cryptographic algorithms, (SQUARE) method.	Simple
5	Mining Algorithms (data stream mining) (IDS)Architecture.	Simple
6	Secure Hash Algorithm. IT security architecture.	Simple

III. CONCLUSIONS

Ultimately protected architectural integration for AMI is profitable to be a new revolution in smart grid. And as it includes all advanced secure technologies for integration, it will make more reliable and secure. To achieve security in terms of CIA model and accountability the different architectural integration are proposed. Enhancement in a CIA and accountability for AMI will make more secure and advanced. Eventually the good architectural integration and secure wireless communication makes AMI more tremendous. And due to this electric sector can save millions of dollars.

References

[1] "DHS National cyber security Division", DHS government 2010-10-03 Retrieved 2012-05- 12.

[2] Mini S. Thomas, Senior Member, IEEE, Ikbal Ali, Senior Member, IEEE, and Nitin Gupta, " A Secure Way of Exchanging the Secret Keys in Advanced Metering Infrastructure", 2012 IEEE Trans.

[3] Yichi Zhang, Lingfeng Wang, Weiqing Sun, "Reliability Evaluation of Power Grids Considering Worm Spreading Pattern in SCADA", 2013IEEE Trans

[4]R. Vijayanand, D. Devaraj, B. Kannapiran and K. Kartheeban, "Bit masking based Secure Data Aggregation Technique for Advanced Metering Infrastructure in Smart Grid System" ,978-1-4673-6680-9/16/$31.00 ©2016 IEEE, 2016 International Conference on Computer Communication and Informatics (ICCCI -2016), Jan. 07 – 09, 2016, Coimbatore, India

[5] Atul Prasad Deb Nath, Fathi Amsaad, Muhtadi Choudhury, and Mohammed Niamat, "Hardware-based Novel Authentication Scheme for Advanced Metering Infrastructure", 2016 IEEE

[6]SeonghoJu, Moonsuk Choi, Chunghyo Kim and Yonghun Lim, "Security Architecture for Advanced Metering Infrastructure", ACSIJ Advances in Computer Science: an International Journal, Vol. 2, Issue 3, No. , 2013 .4 July ISSN : 2322-5157

[7]VisvakumarAravinthan, VinodNamboodiri, SamshodhSunku and Ward Jewell, "Wireless AMI Application and Security for Controlled Home Area Networks", IEEE TRANSACTIONS

[8] S. Kaplantzis and Y. A. Sekercioglu" Security and smart metering", 18th European Wireless Conference, April 2012

[9] Z. Md. Fadlullah, A. Takeuchi, N. Iwasaki, Y. Nozaki "Toward Intelligent Machine-to Machine Communications in Smart Grid", IEEE Communications Magazine, vol. 49, issue 4, pp 60-65, April 2011, doi: 10.1109/MCOM.2011.5741147

[10]YulongZou, Senior Member, IEEE, Jia Zhu, Xianbin Wang, Senior Member, IEEE, and LajosHanzo, Fellow, IEEE, "A Survey on Wireless Security: TechnicalChallenges, Recent Advances and Future Trends", IEEE TRANSACTIONS

[11]Jing Xu Zhilei Yao, "Advanced Metering Infrastructure Security Issues and its Solution: A Review", Vol. 3, Issue 11, November 2015

[12] Hyunwoo Lim, Jongbin Ko, Seokjun Lee, Jongwan Kim, Mijoo Kim, TaeshikShon, "Security Architecture Model for Smart Grid Communication Systems", IEEE TRANSACTIONS

[13]Tanvi Mehra, R. K. Pateriya, "Cyber Security Considerations for Advanced Metering Infrastructure in Smart Grid", International Journal of Scientific & Engineering Research, Volume 4, Issue 8, August-2013 9

[14] ErasmiaEvangeliaTiniou, PeymanMohajerinEsfahani, and John Lygeros, "Fault detection with discrete-time measurements: An application for the cyber security of power networks", 52nd IEEE Conference on Decision and Control December 10-13, 2013. IEEE Trans

[15] Marco Crepaldi ,Michelangelo Grosso ,Alessandro Sassone, Stefano Gallinaro, Salvatore Rinaudo,MassimoPoncino, Enrico Macii, and DaniloDemarchi, " A Top-Down Constraint-Driven Methodology for Smart System Design", 2014IEEE I, first QUART ER 2014, IEEE circuits and systems magazine

[16] Henrik Sandberg, Saurabh Amin and Karl Henrik Johanss, " Cyber physical Security in Networked Control Systems", IEEE Control Systems Magazine ,Februwary 2015.

[17]Ahmed Fawaz, , Robin Berthier and William H. Sanders, "A Response Cost Model for Advanced Metering Infrastructures",IEEE Transactions on smart grid

[18] Ms. Priyanka D. Halle, "Wireless communication security in terms of Confidentiality, Integrity, Availability and Accountability for Advanced Metering Infrastructure", Volume 4, Issue 9, September 2015, ISSN: 2278 – 909X, IJARECE

[19] Rong Jiang_, Rongxing Lu, Ye Wang, Jun Luo, ChangxiangShen, and Xuemin (Sherman) Shen, "Energy-Theft Detection Issues for Advanced Metering Infrastructure in Smart Grid", ISSNll1007-0214ll01/12llpp105-120 ,Volume 19, Number 2, April 2014

[20]MahshidDelavar, SattarMirzakuchaki, Mohammad Hassan Ameri, JavadMohajeri, "PUF-based solutions for secure communication in Advanced Metering Infrastructure (AMI)".

[21]Ahmed Fawaz, Student Member, IEEE, Robin Berthier, Member, IEEE, and William H. Sanders, Fellow, IEEE, "A Response Cost Model for Advanced Metering Infrastructures" ,IEEE TRANSACTIONS ON SMART GRID

[22]YulongZou, Senior Member, IEEE, Jia Zhu, Xianbin Wang, Senior Member, IEEE, and LajosHanzo, Fellow, IEEE, "A Survey on Wireless Security: TechnicalChallenges, Recent Advances and Future Trends", IEEE TRANSACTIONS