ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 4, Issue 9, September 2015

Wireless communication security in terms of Confidentiality, Integrity, Availability and Accountability for Advanced Metering Infrastructure

Ms. Priyanka D. Halle

***Abstract*— In this paper, we are going to focus on security parameters of Advanced Metering Infrastructure (AMI). AMI is very important component of the SG. From the literature survey it is clear that, AMI provides efficiency, reliability, scalability and privacy but due to less security it degrades the performance. Also it degrades the performance of smart grid (SG).Wireless communication security of AMI depends on basically 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 security of AMI but still there is a big problem of security for the reason that no one considered four security parameters. By considering these four parameters we can see drastic change in security. Improvement in these parameters for AMI will make it more advanced. After surveying the existing security solutions in this area, we propose a new algorithm. The proposed security algorithm is a combination of Rivest-Shamir-Adelman (RSA) and AODV2MAP is the Adhoc on-demand distance vector multiple alternative path (AODV-MAP) and recently Internet Engineering Task Force (IETF) has offered simple reactive routing called Dynamic MANET on demand DYMO called AODVv2.This proposed algorithm helps to provide security in terms of CIA and alternative version of HTTPS and cryptographic algorithms can improve security in terms of accountability.**

***Index Terms*— AMI, Security, confidentiality, integrity, availability and accountability or non repudiation.**

I. INTRODUCTION

The AMI accumulate, evaluate and analyze energy usage from networks that are connected to smart meters. AMI is a combination of software, hardware, communication networks, customer-associated systems and a meter data management system (MDMS). As the smart grid becomes a reality, security threats are also estimated to grow enormously, from equally inside and outside the system [1]. Figure 1 shows AMI wireless communication security requirement. Followings terms performs vital role in security.

Confidentiality – It refers to the capability of preventing access to sensitive data (e.g., smart meter data) from unauthorized users. It is related to maintaining privacy or keeping data secret from being disclosed to criminal parties.

Integrity - It is the capacity of smart grid components to guarantee that the information is not modified in transit by any unauthorized person or system. It relates to maintaining the accuracy and consistency of messages being transmitted.

Availability - It refers to the ability of authorized participants to obtain access to certain resources (e.g., electricity service) whenever required.

Accountability - Identifying & tracing back misbehavior entities are required to secure a system. This idea is called accountability or non repudiation [2].

Figure1- Security requirement for wireless communication in AMI

By improving these four parameters we can improve wireless communication security in AMI. Specifically, security necessities in AMI for managing data can be classified as confidentiality, integrity and availability. The cryptograph keys play a core role on encryption and authentication and signature protocols for Securing data confidentiality, integrity and non-reputation. To guarantee the key security, the key management scheme (KMS) plays indispensable roles for AMI systems [3].AMI offers new opportunities for deception to control the consumption information. The communication channels used by AMI to communicate the data between smart meter and utility systems are also susceptible to cyber-attacks. The data transit through these channels can be intercepted and tampered by intruders. Additionally, the attacker is now able to access the smart meter data and firmware remotely. In order to guarantee security of AMI, it is required to expansively analyze, how the AMI can be attacked and what methods can be applied to protect the AMI. In this paper we make a start of the art analyze of security issues which can be applied for AMI systems, since this has not been done intensively before. Based on this the paper proposes a secure system based on a CIA triad model and considering non repudiation security parameter [4].

II. RELATED WORK

This section provides background on security in terms of C,I,A and Ac. Wireless security properties and approaches in AMI are as mentioned in table 1 below. Commonly used

cryptographic mechanisms to prevent the attack in AMI are encryption and decryption technique for confidentiality, Hash function for integrity, for availability generally provides whatever resources required and for accountability generally used communication protocols using proposed architecture. Highly reliable communication network is required for transferring the high volume of data in AMI. For this reason by using appropriate wireless communication technology we can make more reliable AMI. This paper considers for communication Worldwide Interoperability for Microwave Access (WiMAX).

Table 1 -Security properties and approaches in AMI

Security property	Considered features of AMI	Commonly used cryptographic mechanism to prevent the attack
Confidentiality and Integrity.	Hybrid transmission mode of messages, storage and computation constraints of SMs.	KMS, Key management framework constructed based on key graph (Simple cryptographic algorithms) **[14].**
Confidentiality, Integrity and availability.	NAN, multi-hopping is considered ,wireless mesh AMI network.	Secure on-demand routing protocols, multipath routing protocols for wireless mesh AMI networks, AODV2MP based on combination of AODV-MAP and AODVv2 **[15].**
Integrity	Highly complex heterogeneous network.	Tool AMI Sec Checker (auth-algorithm) Security control ,Reachability , Misconfiguration and Data delivery analysis **[16].**
Integrity	In home energy management.	Wireless Sensor Networks (WSNs) **[17].**
Confidentiality, Integrity & availability.	Cloud -based solutions for smart grids, Energy at Home scenario.	a framework based on ABAC model, open-source Spring Security framework, energy-optimization algorithms, ABAC mechanism in the Spring Security framework. ,authorization protocols such as OAuth **[18].**
confidentiality, integrity, availability, non-repudiation	Data stream mining	IDS architecture for AMI,, sliding window and sequence mining algorithms, two clonal selection algorithms named CLONALG and AIRS2Parallel **[19].**

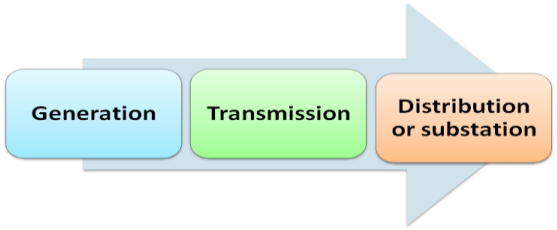

Figure2-Data flow in AMI.

Figure 2 illustrates the data flow in AMI [5]. Smart grid physical layer consists of physical infrastructure required for power generation. Network layers comprises of transmission lines that provides transmission path for electric power. Data Link Layer provides protocols to be used for transfer of data between control centre and consumer or service provider. Application layer specifies the methods of interfacing application with the host communication system. .

Meter Data Management System is one of the important part of AMI .It manages all data. Therefore the attacker can attack on MDMS and they can hack the data. This paper mainly focuses on wireless communication security primarily in MDMS.

Table 2 elaborates different algorithms and methodologies for wireless security of AMI in terms of C, I, A and Ac. From the table it is clear that security is a big problem in AMI. The no of researchers has done work on it but still there is a big problem because no one considered four parameters.

Table2- Different algorithms and methodologies for wireless security of AMI in terms of C, I, A and Ac.

Paper. No.	Paper Title and Publication Year	Security methodology /protocol/algorithm for Data confidentiality	Security methodology /protocol/algorithm for Data Integrity	Security methodology /protocol/algorithm for Data availability	Security methodology/ protocol/algorithm for Data non repudiation or accountability
1	An Efficient Security Protocol for Advanced Metering Infrastructure in Smart Grid (Year-2013)	Integrated Authentication and Confidentiality (IAC), backbone node selection (BNS) algorithm, NS2 for simulation.		?	?
2	Security Analysis of Selected AMI Failure Scenarios Using Agent Based Game Theoretic Simulation(Year 2014)	Agent Based Game Theoretic (ABGT) simulations, National Electric Sector Cyber security Organization Resource (NESCOR), verified with the results from game theory analysis.			?
3	A Key Management Scheme for Secure Communications of Information Centric Advanced Metering Infrastructure in Smart Grid(Year2014)	Information Centric AMI (ICN-AMI) structure, novel key management scheme (KMS), NDN sim simulation, data authentication considered.		?	?
4	Attacks and their Defenses for Advanced Metering Infrastructure (Year-2014)	Strong encryption, secure key distribution, dynamic routing and proper mechanism for Intrusion detection and prevention.			?
5	Towards Secure End-to-End Data Aggregation in AMI through Delayed-Integrity-Verification (Year-2014)	?	Chameleon Signatures, Trapdoor Chameleon Hash Function, authenticity and data originality also provides, digital signatures used.	?	?
6	Reconciling Security Protection and Monitoring Requirements in Advanced Metering Infrastructures(Year2013)	IDS-friendly protected AMI stack.	?	?	?
7	A Game Theoretical Analysis of Data Confidentiality Attacks on Smart-Grid AMI(Year-2014)	non-cooperative game theory, Nash equilibrium, encry-ption algorithms	?	?	?
8	Secure communication for advance metering infrastructure in smart grid(Year-2014)	bootstrapping protocol, public key cryptography for authentication and secret key exchange, pycrypto library for cryptographic operation			?
9	An Efficient Message Authentication for Non-repudiation of the Smart Metering Service(Year-2011)	?	efficient message authentication scheme, cryptographic algorithms	?	efficient message authentication scheme, cryptographic algorithms
10	Key Distribution and Management for Power Aggregation and Accountability in Advance Metering Infrastructure(Year2012)	?	distribution and management, key distribution table	?	framework for key distribution and management, key distribution table
11	A Practical Model For Rating Software Security(Year2013)	Based on ISO 25010.			Based on ISO 25010.
12	Non repudiation for internet access by using browser based user authentication Mechanism (Year2013)	?	?	?	Browser security, browser based validation;
13	An alternative version of HTTPS to provide non repudiation security property(Year-2014)	?	?	?	Architecture LECCSAM can provide an Alternative version of HTTPS.

.

III. PROPOSED WORK

Enhancement in wireless security for AMI will make it more sophisticated, capable and trustworthy. Ultimately AMI is a tool going to be an important part of SG. And as it include all types of advanced features will make it most dominant technology in future. By developing AMI we can save millions of dollars and electricity.

The proposed system consists of basic elements of AMI. The MDMS is the heart of the AMI, it manages all important data. Therefore this paper mainly focuses on wireless security in terms of C, I.A, Ac in MDMS

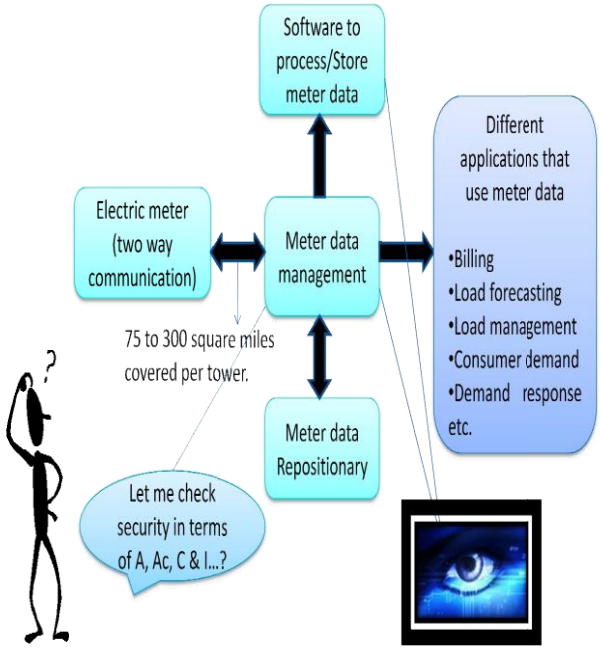

Figure 3– Proposed System For Advanced Metering Infrastructure (AMI).

IV. CONCLUSION

The proposed system to recover security in terms of A, C, I, Ac can save millions of dollars in spoil avoidance and preservation cost for energy providers and consumers. Also it helps to save power. Improved security for transmitted information and delivered power is another advantage of AMI. Additionally, AMI allows the users to better control their consumption pattern. It also offers higher power quality and stability. To achieve security for AMI, cryptographic algorithm that is RSA and combination of AODV-MAP and AODVv2, alternative version of HTTPS will be very valuable so security can be improve.

V. REFERENCES

[1] Ye Yan, Rose Qingyang Hu, Sajal K. Das, Hamid Sharif and Yi Qian, "An Efficient Security Protocol for Advanced Metering Infrastructure in Smart Grid", 2013 IEEE Trans.

[2] Robert K. Abercrombie, Bob G. Schlicher, and Frederick T. Sheldon, "Security Analysis of Selected AMI Failure Scenarios Using Agent Based Game Theoretic Simulation", 2014 IEEE Trans.

[3] Keping Yu, Di Zhang, Arifuzzaman Mohammad, Nam Hoai Nguyen, Takuro Sato, "A Key Management Scheme for Secure Communications of Information Centric Advanced Metering Infrastructure in Smart Grid", POWERCON 2014, 2014 International Conference on Power System Technology (POWERCON 2014), 2014 IEEE Trans.

[4] Sheeraz Niaz Lighari, Dil Muhammad Akbar Hussain, Birgitte, Bak Jensen, Asad Ali Shaikh, "Attacks and their Defenses forAdvanced Metering Infrastructure", 2014 6th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2014 IEEE Trans.

[5] Sye Loong Keoh, Zhaohui Tang," Towards Secure End-to-End Data Aggregation in AMI through Delayed-Integrity-Verification", 2014 IEEE Trans

[6] Robin Berthier, Jorjeta G. Jetchevay, Daisuke Mashimay, Jun Ho Huh, David Grochocki, Rakesh B. Bobba, Alvaro A. C´ardenasz, and William H. Sanders, "Reconciling Security Protection and Monitoring Requirements in Advanced Metering Infrastructures", 2013 IEEE Trans.

[7] Ziad Ismail, Jean Leneutre, David Bateman, and Lin Chen, "A Game Theoretical Analysis of Data Confidentiality Attacks on Smart-Grid AMI", IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 32, NO. 7, JULY 2014

[8] Vijay Kumar and Muzzammil Hussain, "Secure communication for advance metering infrastructure in smart grid", 2014 Annual IEEE India Conference (INDICON)

[9] Jaeduck Choi, Incheol Shin, Jungtaek Seo, and Cheolwon Lee, "An Efficient Message Authentication for Non-repudiation of the Smart Metering Service", 2011 IEEE Trans.

[10] Joseph Kamto, Lijun Qian, John Fuller, John Attia, Yi Qian, "Key Distribution and Management for PowerAggregation and Accountability in Advance Metering Infrastructure", 2012 IEEE Trans.

[11] Haiyun Xu, Jeroen Heijmans, Joost Visser, "A Practical Model For Rating Software Security", 2013 IEEE Trans.

[12] Nithesh K.Nandhakumar, Binu A., Viji Paul, "Non repudiation for internet access by using browser based user authentication mechanism", 2013 IEEE Trans.

[13] Stassia Resondry, Karima Boudaoud, Michel Kamel, Yoann Bertrand and Michel Riveill, "An alternative version of HTTPS to provide nonrepudiation security property", 2014 IEEE Trans.

[14] Nian Liu, Jinshan Chen, Lin Zhu, Jianhua Zhang, Yanling He "A Key Management Schemefor Secure Communications of Advanced Metering Infrastructure in Smart Grid", IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 60, NO. 10, OCTOBER 2013.

[15] Binod Vaidya , Dimitrios Makrakis Hussein Mouftah "Secure and robust multipath routings for advanced metering infrastructure", 14 September 2013 Springer Science+Business Media New York 2013

[16] Mohammad Ashiqur Rahman and Ehab Al-Shaer "A Declarative Logic-Based Approach for Threat Analysis of Advanced Metering Infrastructure" Springer International Publishing Switzerland 2013.

[17] Omowunmi M. Longe(&), Khmaies Ouahada, Hendrick C. Ferreira, and Suvendi Rimer "Wireless Sensor Networks and Advanced Metering Infrastructure Deployment in Smart Grid", Springer 167–171, 2014.

[18] Alessandro Armando, Roberto Carbone, Eyasu Getahun Chekole, Claudio Petrazzuolo, Andrea Ranalli, and Silvio Ranise, "Selective Release of Smart Metering Data in Multi-domain Smart Grids", Springer International Publishing Switzerland 2014 J. pp. 48–62, 2014

[19] Mustafa Amir Faisal, Zeyar Aung, John R. Williams, and Abel Sanchez " Securing Advanced Metering Infrastructure Using Intrusion Detection System with Data Stream Mining", Springer-Verlag Berlin Heidelberg 2012.

First Author

I, Mrs. Priyanka D. Halle have done my Bachelor of Engineering in Electronics and Telecommunication in Dr. Babasaheb Ambedkar Marathawada University in 2007, located in Aurangabad, Maharashtra. I was excellent both at academic courses and extracurricular activities. I have done my Master of Technology in Digital System and computer Electronics in Jawaharlal Nehru Technical University in 2013, located in Hyderabad, Andhra Pradesh. I have published one international paper based on my project. Recently, I am working as Assistant Professor in E&TC department at SKN Sinhgad Institute of Technology & Science, Lonavala and District - Pune Maharastra..My research interests include Wireless Communications and Cyber security.