ISSN 2320 2629
Volume 3, No.6, November - December 2014
International Journal of Information Technology Infrastructure
Available Online at http://warse.org/pdfs/2014/ijiti01362014.pdf

Performance Analysis of Security Protocol for Advanced Metering Infrastructure in Smart Grid

Divya Menon[1], Soniya Joseph[2]
[1]Professor, Department of Computer Science and Engineering
Jyothi Engineering College, Cheruthuruthy, Thrissur, India
divya@jecc.ac.in
[2]Department of Computer Science and Engineering
Jyothi Engineering College, Cheruthuruthy, Thrissur, India
soniyajoseph111@gmail.com

ABSTRACT

The smart grid is a network of computers and power infrastructures that monitor and manage energy usage**.** This paper aims to provide a deep understanding of security vulnerabilities and solutions in the Smart Grid and shed light on future research directions for Smart Grid security. A security protocol, Integrated Authentication and Confidentiality (IAC), for advanced metering infrastructure in smart grid is proposed for avoiding the main issues in confidentiality as well as message authentication. With the help of Integrated Authentication and Confidentiality (IAC), an AMI system can provide trust services, data privacy, and integrity by mutual authentications whenever a new smart meter initiates and joins the smart grid AMI network. Simulation and analytical results show that the proposed IAC protocol has better performance in terms of end-to-end delay and packet loss than a basic security scheme.

Key words: Smart Grid, AMI Network, Confidentiality, IAC Protocol.

1. INTRODUCTION

The current electrical grid is perhaps the greatest engineering achievement of the 20th century. However, it is increasingly outdated and overburdened, leading to costly blackouts and burnouts. For this and various other reasons, transformation efforts are underway to make the current electrical grid smarter. The smart grid could be referred to as the modernization of the current electric grid for the purpose of enabling bidirectional flows of information and electricity in order to achieve numerous goals**.** The Smart Grid power transmission and distribution system delivers power from the power plant to end users through a transmission substation and a number of distribution substations **.**

The electrical power industry is in the process of integrating its distribution system with communication networks and control networks and control techniques to form a bidirectional power and information flow infrastructure, commonly called a smart grid. Such integration not only moves power automation systems from outdated technology to today's new communication technologies and systems, but also brings the proprietary network of power control systems to public data networks.

Cyber security is an extremely critical issue in smart grid due to increased potential of cyber attacks and incidents against this critical sector of the power grid as it becomes more and more interconnected. Cyber security must address deliberate attacks, such as those from disgruntled employees, industrial espionage, and terrorists, as well as inadvertent compromises of the information infrastructure due to user errors, equipment, failures and natural disasters. So it is very important in smart grid Applications. Vulnerabilities imply that an attacker will have the opportunity to penetrate into a smart grid network, gain access to control software, and alter load conditions to destabilize the grid in unpredictable ways [4] **.**

Advanced metering infrastructure (AMI) refers to the systems that collect, measure, and analyze energy usage from networks that are connected to next-generation electricity meters, or so-called smart meters.

2. ADVANCED METERING INFRASTRUCTURE

Advanced Metering Infrastructure (AMI) is designed to collect, measure, and analyze energy consumption data of customers through smart meters in order to save the way for dynamic and automatic electricity pricing. Typically, appliances report to a smart meter, smart meters report to a data aggregation point such as a gateway in distribution substation and the aggregation point relays this data to the utility center through the core backbone. AMI data is the most fundamental and crucial part of the traversing every portion

of the SG communications network in two-ways. Thus, AMI is one of the most challenging applications in terms of establishing the routes from appliances to the utility. AMI may be implemented using a wide variety of communication technologies that allow remote configuration, meter reading and appliance control.

2.1 Security Needs

To address the above cyber security threats, the general requirements for AMI security are mainly include Device authentication, Data confidentiality, Message integrity, maintaining secrecy, preventing potential cyber attacks. Security as a major requirement covers all aspects of the SG, from physical devices to routing protocol operations to ensure the availability and reliability of the whole network.[1] Many end-point devices in power transmission and distribution networks, and power generation networks are located in an open, potentially insecure environment which makes them prone to malicious physical attacks. These devices must be protected properly against unauthorized access such as modifying the routing table or some network information stored in the compromised device. These actions as well as spoofing, altering or replaying routing information during information exchange between nodes are examples of attacks against routing protocols. Another major concern in the routing would be the privacy of the power data [3].

2.2 Proposed IAC Protocol

Proposed Integrated Authentication and Confidentiality (IAC) protocol for efficient and secure AMI communications, which can work with current industrial standards such as the American National Standards Institute (ANSI) C12 protocol suite. The proposed IAC protocol includes the following processes:

- Initialization process for authentication
- Meter reading collection process for user data confidentiality
- Control message distribution process for control message confidentiality

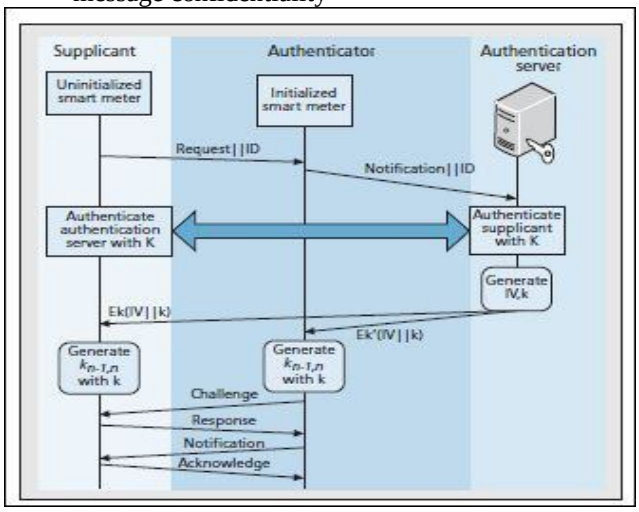

Figure 1: Initialization process and authentication

Before joining the AMI network, each new smart meter must be verified by the remote authentication server located at the local management office as a legal device and terminal customer. The neighboring authenticated smart meters can play as authenticators in the initialization process and relay the authentication process messages between the supplicant and the authentication server.[7] Both the supplicant and the authentication server have an identical key K, which was pre-installed, not concealed to anyone else including the authenticator. Both the mutual authentication identities and the consequent data encryption/decryption between supplicant and authentication server are based on k.

If the supplicant's identity is authenticated as a valid device, in Figure 1 shows, the corresponding credential of the supplicant is established between the authentication server and the supplicant. [3] So the supplicant can decrypt and get its IV and k. Meanwhile, the authentication server sends k to the authenticator encrypted with their own Kc denoted as EK'(IV||k) since the authenticator was authenticated already with K. So the authenticator knows k. With its k, the supplicant and authenticator can individually generate kn-1, n, which is the symmetric key for message authentication code generation and validation between one-hop neighboring nodes n and n-1 on the data forwarding path.

The proposed security protocol performs encryption and message authentication tasks in N repeated operations (with different keys for each operation) from every source smart meter to the collecting node. These operations will be distributed to a subset of smart meter nodes on the wireless backbone. Compared to a basic end-to end security scheme, which performs encryption and message authentication at the source/destination node only, this hop-by-hop data aggregation and forwarding approach can enhance the system security performance by grouping certain intermediate nodes together with a source/destination node. By using this approach, the efficiency and reliability of the multi-hop wireless network for AMI can be improved.

2.3 Proposed Algorithm

The backbone node selection (BNS) algorithm we propose to construct the backbone chain for IAC when the data aggregation and forwarding route is needed. It is equivalent to a wireless mesh network of smart meters to a feeder in AMI. The backbone node selection algorithm should be simple and efficient to select the backbone nodes and construct or rebuild the backbone in a scalable way for the AMI system in case of router error, especially time varying wireless channel errors. The selected intermediate backbone nodes work in a hop-by-hop mode. The corresponding keys Kn (the K of node n) and kn-1, n can be piggybacked in the backward routing messages during the initialization process. Those selected intermediate nodes without an encryption and authentication

process simply relay the packets. Only focus on the selected intermediate nodes with an encryption and authentication process.

3. PERFORMANCE EVALUATION AND SECURITY ANALYSIS

Compare the performance of the proposed IAC protocol with that of a basic security scheme, where each smart meter communicates with the collecting node through a private key and end-to-end encryption through the same multi-hop routing chain of the IAC protocol, which we call the "basic security scheme" or simply "basic scheme." End-to-end delay is crucial for real-time applications such as online meter reading collection for electricity voltage, current, phase, and reactive power status in the smart grid. If the data cannot meet its end-to- end deadline, it might cause serious system faults, especially in the monitoring/protection system by missing fault detection. Packet drop rate is also important for the system to make prompt and proper decisions based on the collected real-time meter readings [9].

Average packet delivery rate, respectively for the proposed IAC protocol and the basic scheme as a function of the total number of hops in the routing chain. When the number of hops increases, the end-to-end packet delay increases and the packet delivery rate decreases for both security schemes. However, the performance of our IAC protocol is consistently better than the basic security scheme for both metrics. The packets generated at the nodes that are less than five hops away from the collection/destination node experience a smaller end-to-end packet delay if a basic security scheme is used. On the other hand, those packets experience a smaller end-to-end packet delay if the IAC scheme is used. The packet delay collected from different nodes belonging to the same routing chain is the same in the IAC scheme. In the IAC protocol, the packets from different nodes are generated synchronously and combined into a super data packet using the proposed hop-by-hop data aggregation and forwarding scheme. The super packet is then received and decoded by the collection node all together.

The packet delivery rate at each smart meter is always higher if the IAC scheme is used. The packet collision rate at each node could be as high as the number of wireless devices goes up. The proposed IAC protocol can arrange the transmission schedule for each participating smart meter at the initialization process. Therefore, all the participating smart meters transmit in a predefined order to reduce collision.

4. CONCLUSION

Energy management for residential homes and/or offices requires both identification and prediction of the future usages or service requests of different appliances present in the buildings. The aim of this work is to identify residential appliances from aggregate reading at the smart meter and predict their states in order to minimize their energy consumption.

The proposed IAC protocol employs mutual authentication between a remote server located in the local management office and a neighboring smart meter as the authenticator to obtain proper cryptography keys for consequent secure data communications. Future work will first focus on how to adapt,

the proposed IAC protocol to multicast and broadcast in smart grid AMI networks. The second direction of future work will investigate the impact of error-prone wireless channel on the proposed IAC protocol and the possible improvement of the IAC protocol under the error-prone wireless channel. Smart Grid is a potential electrical power delivery system, with at least two important components: Firstly, a two-way, real-time, reliable, large capacity communication infrastructure to satisfy the increasing needs of the power grid, such as bill verification from customers, control and management of the power load over the whole grid, optimization of power grid assets, etc. secondly, integrated Information Technology (IT) which processes and handles large amounts of information over the Smart Grid.

REFERENCES

1 Elias Bou-Harb, Claude Fachkha, Makan Pourzandi, Mourad Debbabi. ***Communication Security for Smart Grid Distribution Networks***, IEEE Communications Magazine, pp.42-49, 2012.

2 Amir-Hammed Mohsenian-Rad, Member, IEEE, and Alberto Leon-Garcia, Fellow, IEEE. ***Distributed Internet-Based Load Altering Attacks against Smart Power Grid***s, IEEE Transactions on smart Grid, vol. 2, No. 4, December.

3 Shuva Paul, Memberamo Sajed Rabbani, Ripon Kumar Kundu, Skidder Mohammad Raihan Zaman. ***A Review of Smart Technology (Smart Grid) and Its Features***. IEEE Proceedings, (ICONCE 2014).

4 Zubair Md. Fadlullah, Mostafa M. Fouda, and Nei Kato.***An Early Warning System against Malicious Activities for Smart Grid Communications***. IEEE Network, September/October 2011.

5 Xi Fang, Satyajayant Misra, Guoliang Xue, Fellow, IEEE, and Dejun Yang***. Smart Grid – The New and Improved Power Grid: A Survey,*** IEEE Communications Surveys & Tutorials, VOL. 14, NO. 4, Fourth Quarter 2012.

6 Meikang Qiu, Hai Su, Min Chen, Zhong Ming, Laurence T.Yang. ***Balance of Security Strength and Energy for a PMU Monitoring System in Smart Grid***. IEEE Communications Magazine, May 2012.

7 Adnan Afsar Khan and Hussein T. Mouftah. ***Secured Web Services For Home Automation in Smart Grid Environment***, IEEE Canadian Conference on Electrical and Computer Engineering.

8 Gerald J. Fitzpatrick, Member, IEEE, and David A. Wolman. ***NIST Interoperability Framework and Action Plans, 978***-1-4244-6551-4/10/, 2010 IEEE.

9 Rakpong Kaewpuang, Siva don Chaisiri, Dusit Niyato, Bu-Sung Lee, and Ping Wang, ***Adaptive Power Management for Data Center in Smart Grid Environment***, 2012 10th IEEE International Symposium on Parallel and Distributed Processing with Applications.

10 Anupam A. Tate, Student Member, IEEE, and Le Xie, Member, IEEE. ***Towards a Unified Operational Value Index of Energy Storage in Smart Grid Environment***, IEEE Transactions on smart grid, Vol. 3, No. 3, September, 2012.

11 Yichi Zhang, Student Member, IEEE, Lingfeng Wang, Member, IEEE, and Weiqing Sun, Member, IEEE. ***Trust System Design Optimization in Smart Grid Network Infrastructure,*** IEEE Transactions on smart grid, Vol. 4, No. 1, March 2013.

12 G. A. Taylor, M. R. Irving Member, IEEE, P. R. Hobson, C. Huang, P. Khyber and R. J. Taylor, ***Distributed Monitoring and Control of Future Power Systems via Grid Computing***, 2006 IEEE.

13 Ye Yan, University of Nebraska-Lincoln Rose Qing yang Hu, Utah State University Sajal K. Das, The University of Texas at Arlington, ***An Efficient Security Protocol for Advanced Metering Infrastructure in Smart Grid***, IEEE Network, pp.64-71, July/August 2013.