Review Article | Impact Factor: 0.621 | ISSN: 2319-507X
Priti Jasud, IJPRET, 2014; Volume 2 (9): 1165-1171 | IJPRET

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

AUTHENTICATION PROVIDED USING KEY REFRESHMENT TECHNIQUE FOR SMART GRID NETWORK

PRITI V. JASUD[1], PROF. MANISH D. KATKAR[2], PROF. S. D. KAMBLE[3]

1. M. Tech Scholar, Department of computer science and engineering, G. H. Raisoni Institute of Engineering and technology for Womens Nagpur, India.
2. Asst. Professor, Department of computer science and engineering, G. H. Raisoni Institute of, Engineering and Technology for Womens Nagpur, India.
3. Asst. Professor, Department of computer science and engineering, Yashvantrao Chavhan College of Engineering, Nagpur, India.

Accepted Date: 27/02/2014 ; Published Date: 01/05/2014

Abstract: The Smart Grid is formed by many sub-networks such as the Home Area Network (HAN), service providers, transmission, distribution, and bulk generation, operations and market which are at risk and can be attacked remotely. Smart grids that is supports data aggregation and access control. Data can be aggregated by home area network (HAN and neighboring area network (NAN) in such a way that the privacy of customers is protected. Smart grid designing a mutual authentication scheme and a key management protocol. This paper proposes an efficient scheme that mutually authenticates a smart grid and an authentication server in SG by decreasing the number of steps in the secure remote password protocol. In this paper we propose an efficient key management protocol based on our enhanced identity-based cryptography for secure SG communications using the public key infrastructure.

Keywords: Enhanced identity-based, key management, cryptography, smart grid (SG) mutual authentication, and secure remote password (SRP).

Corresponding Author: MS. PRITI V. JASUD

Access Online On:

www.ijpret.com

How to Cite This Article:

Priti Jasud, IJPRET, 2014; Volume 2 (9): 1165-1171

PAPER-QR CODE

1 INTRODUCTION

The Smart Grid is designed to provide the security in which has gained substantial attention in the research community [1]. SG is a combination of different systems and subsystems and is vulnerable various attacks that may cause different levels of harms to the devices and even to the society at large [2].An important problem which is associated with smart grid is the problem of security and privacy. It is very important to secure the smart grid, not only from terrorist attacks, but also from customers and building authorities who can tamper with various devices. The Key management is one of the important security requirements to achieve data confidentiality and integrity in smart grid system. The Smart Grid is designed to provide consumers with reliable, efficient, and safe electric energy. Security in the Smart Grid is not only important to securing the new communications and systems on the Internet, but also to ensuring safety and reliability for the critical utility of power. Providing an authentication scheme and providing key management protocols are the required first steps of designing and implementing system security in SG [3].

This work is focused on authentication and key management over the AMI. Although power line communication (PLC) has gained much attention in Europe, North America, wireless mesh networks (WMNs) are a more popular and dominant solution for the AMI [4] proposed a mesh-based architecture for the last mile SG, in which the neighborhood area network supports communications between SMs and AMI head-end via data aggregation points and mesh relay stations if required. The WMN is more complicated so, in this paper we used concept of client server network.

Contributions: In this paper, we propose a secure and efficient SG mutual authentication (SGMA) scheme and an SG key management (SGKM) protocol. SGMA provides efficient mutual authentication between SMs and the security and authentication server (SAS) in the SG using passwords; it reduces the number of steps in SRP. Research in smart grid is very important and involves a broad range of problems. An important problem is to design an architecture integrating all the components, which can efficiently use in security. The improved efficiency results from our key refreshment protocol in which the SAS periodically broadcasts a new key generation to refresh the public/private key pairs of all the nodes as well as any required multicast security keys.

2. RELETED RESEARCH WORK

A. Authentication Management

Authentication means binding an identity (ID) to a subject .It can be accomplished by showing-

1) What the subject is capable of doing e.g.performing a digital signature;

2) What the subject knows e.g. a password;

3) What the subject possesses, e.g. a smart card; or

4) What the subject has biometrically e.g. Finger prints.

B. SRP Protocol

SRP is an authentication and key exchange protocol for secure password verification and session key generation over an insecure communication channel. SRP utilizes asymmetric key exchange (AKE) [7]. and stores verifiers instead of the passwords. AKE uses a one-way (hash) function to compute the verifier and stores it in the server system.

In SRP, the client first enters a password, and then, the server computes a verifier from the password using a randomly generated key and stores the client's ID. Subsequently, the client is authenticated to the server by providing the password to the server, which computes the verifier again using the salt stored against the client's ID and checking it against the one stored in its database. Furthermore, each party generates a random number and then calculates the session key based on the password, verifier, and random numbers as well as verifies the key utilizing a one-way hash function.

C. PKI

In the PKI [4], two keys, public key and private key, are associated with each entity. The sender uses her private key to sign the message and the public key of the recipient used to encrypt the message. The recipient uses her private key to decrypt the message and the sender's public key to authenticate the sender's ID.

A private key generator (PKG)/ certificate authority issues to each entity an individual certificate consisting of the private key of the entity and makes the public key of the entity available to the public. The PKG is required to refresh these keys periodically per system security.

3. SMART GRID APPLICATION

i) Advanced metering infrastructure (AMI): Establish two-way communications between advanced meters and utility business systems.

ii)Cyber security: Ensure the confidentiality, integrity and availability of the electronic information.

iii)Demand response and consumer energy efficiency: Provide mechanisms and incentives for customers to cut energy use during times of peak demand.

iv) Distribution grid management: Maximize the performance of feeders, transformers and other components of distribution systems.

v) Electric transportation: Enable large-scale integration of plug-in electric vehicles.

vi) Energy storage: Provide the means to store energy.

vii)Network communications: Identify performance metrics and core Operational requirements of various Smart Grid applications.

viii) Wide-area situational awareness: Monitoring and display of power-system components over large geographic areas in near real time to optimize management of grid components and performance and respond to problems before disruptions arise.

4. SMART GRID MUTUAL AUTHENTICATION (SGMA)

A. System Setup

It support the required authentication and key management mechanisms. We also cover the key management for unicast, multicast, and broadcast communications that may be needed to support any application over SG.

B. Mutual Authentication

In this it provide the authentication between sender and receiver. Sender uses her private key to sign the message and the public key of the recipient used to encrypt the message, and the recipient uses her private key to decrypt the message and the sender's public key to authenticate the sender's ID. The key is generated randomly.

C. Key Refreshment

The key is randomly generated using generate key module. The key size is 64bit.

1) Short-Term Refreshment Process:- PKG generate a new function and makes it publically accessible along with a valid time.

2) Medium-Term Refreshment Process:- PKG renews the function parameters along with the required valid time and shares them with all the parties to be used the starting at valid time.

3) Long-Term Refreshment Process:- PKG reselect the system not shared secrete values along with the system shared secrete values, and updates one-way function, in order to refresh the keys i.e. public and private keys of all parties.

D. Multicast Key Mechanism

SMK (Source Multicast Key) is used by a group source to encrypt the multicast packets. Furthermore, RMK (Receiver Multicast Key) is used by all group receivers to decrypt the messages that are encrypted by SMK.

1) Establishing a Multicast Group:

An MGS that wants to form a multicast group sends a request to SAS. SAS provides MGS with the group initial parameter set.

2) Joining Multicast Group

3) Key Refreshment Process: The reasons for the key refreshments in case of multicasting situation are different from the unicast situation and consist of two cases:

A member joining or leaving causes the system to refresh the keys in order to maintain forward and backward secrecy.

Providing overall multicast key secrecy.

E. Broadcast Key Mechanism

Referring to our unicast medium-term key refreshment process, the public key of SAS is dynamic and changes periodically according to the function and state of the system, only the parties authenticated by the SAS, who receive their key management service from the SAS, have the live public key of SAS.

5. PERFORMANCE ANALYSIS

In this section, we evaluate the security of our proposed SGMA and SGKM mechanisms using the Automated Validation of Internet Security Protocols and Application (AVISPA) security analyzer [8]. Furthermore, we review the adversary models including adversary interests and capabilities to attack the system. Then, we review the system security against attacks. Our analysis shows that SGMA is fast, robust, and secure. It implementing the private key cryptography system in a distributed environment causes providing a symmetric key between every two nodes that need to communicate to each other. Moreover, increasing the number of nodes that want to communicate with a single node requires that the node keeps and manages a large number of keys (one per peer node), which is the case in the SG context. However, PKI requires only one key pair per entity in spite of a larger key size. In fact, while a node has its own private/public key pair, it is sufficient for the node and others to exchange secure communications.

6. CONCLUSION

In this paper, we have presented a secure framework in smart grids which provide mutual authentication and key management mechanisms. The proposed mechanism addresses the required security aspects by the SG system and, at the same time, manages the process in an efficient manner. In this paper we propose multiple secure, intuitive and low cost authentication mechanisms for the Smart Grid enabled HANs. In order to enjoy the security benefits of PKI, SG has to endure the inefficient resource utilization due to the large key sizes as well as the large key distribution overhead. The savings in resource consumption as the result of our mechanism can be used to handle more data delivery and/or to increase the security of the system by refreshing the keys, which brings to SG the opportunity to utilize keys of smaller sizes.

7. REFERENCE

1. Z. Fan, P. Kulkarni, S. Gormus, C. Efthymiou, G. Kalogridis, M. Sooriyabandara, Z. Zhu, S. Lambotharan, and W. H. Chin, "Smart grid communications: Overview of research challenges, solutions, and standardization activities," IEEE Commun. Surveys Tuts., vol. 15, no. 1, pp. 21–38,2013.

2. J. Wang and V. Leung, "A survey of technical requirements and Consumer application standards for IP-based smart grid AMI network," in Proc. ICOIN, 2011, pp. 114–119.

3. H. Nicanfar, P. Jokar, and V. Leung,"Smart grid authentication and key management for unicast and multicast communications, " in Proc. IEEE PES ISGT, 2011, pp. 1–8.

4. D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk, "Internet X. 509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," Internet Engineering Task Force, Fremont, CA, USA, 2008.

5. M. Amin, "Challenges in reliability, security, efficiency, and resilience of energy infrastructure: Toward smart self-healing electric power grid," in Power and Energy Society General Meeting – Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE, Jul. 2008, pp. 1–5.

6. A. Metke and R. Ekl, "Security technology for smart grid networks," Smart Grid, IEEE Transactions on, vol. 1, no. 1, pp. 99 –107, Jun. 2010.

7. Z. Fadlullah, N. Kato, R. Lu, X. Shen, and Y. Nozaki, "Towards secure targeted broadcast in smart grid," IEEE Commun. Mag., vol. 50, no. 5, pp. 150–156, May 2012 [Online]. Available: http://bbcr.uwaterloo.ca/h8liang/sg/Papesg commx.pdf

8. J. Xia and Y. Wang, "Secure key distribution for the smart grid," IEEE Trans. Smart Grid, vol. 3, no. 3, pp. 1437–1443, Sep. 2012.

9. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. S. Shen, "A light-weight message authentication scheme for smart grid communications," IEEE Trans. Smart Grid, vol. 2, no. 4, pp. 675–685, 2011.

10. S. R. Rajagopalan, L. Sankar, Mohajer, and H. V. Poor, "Smartmeter privacy: A utility-privacy framework," Proc. IEEE SmartGridComm, 2011.