International Journal of Grid Distribution Computing
Vol. 8, No.3, (2015), pp.35-42
http://dx.doi.org/10.14257/ijgdc.2015.8.3.04

An Implementation of Public Key Infrastructure Using Wireless Communication Networks

Nandhini M [1] and PraveenkumarB[2]

[1]*PG Scholar, Muthayammal Engineering College, Salem, India*
[2]*Assistant Professor, Knowledge Institute of Technology, Salem, India*

Abstract

The Smart Grid is an electrical power infrastructure that makes intelligent decisions about the state of the electrical power system to maintain a stable environment. It is expected that the smart grid will radically add new functionalities to legacy electrical power systems. However, believe that this will in turn introduce many new security risks. With the smart grid's backbone communication networks and sub networks, there are possible scenarios when these sub networks can become vulnerable to attacks. Ensuring security in these networks is challenging because most devices are resource constrained. In addition, different protocols that are used in these networks use their own set of security requirements. In this article, the securities Requirements of smart grid communication networks are firstly identified. The public key infrastructure (PKI) is a viable solution; it has some difficulties to satisfy the requirements in availability, privacy preservation, and scalability. To complement the functions of PKI, introduce some novel mechanisms so that those security requirements can be met. In particular, propose a mechanism to efficiently resist Denial-of-Service (DoS) attacks, and some suggestions to the security protocol design for different application categories.

Keywords: *Smart grid, PKI, DoS*

1. Introduction

The Smart Grid is going to add new functionality to the current electrical power system. However, it will also introduce several new security risks into the system. We rely on the electrical power grid for electricity, and our dependence on electricity makes the electrical power grid a critical asset. Disruption of the electrical power supply will have large societal impacts. The security of the electrical power grid is an important issue. The Smart Grid will introduce several new security risks related to its communication requirements, system automation, new technologies, and data collection.

The backbone of the Smart Grid will be its network. This network will connect the different components of the Smart Grid together, and allow two-way communication between them. Net-Working the components together will introduce security risks into the system, but it is required to implement many of the main functionalities of the Smart Grid. Networking the different components together will increase the complexity of the electrical power grid, which will then increase the number of opportunities for new security vulnerabilities. Also, the number of entry points that can be used to gain access to the electrical power system will increase when all of the components are networked together.

The Smart Grid will use the data transported by the electrical power grid network and software to maintain the power system automatically. Relying on the power grid network to transport system information introduces security risks. Some of the components require real-time data, and latency or data loss can have adverse effects on the electrical power grid. The software managing the system state is also at risk to malicious code that can alter its functionality. A disruption to communications or the state management software

ISSN: 2005-4262 IJGDC

can lead to loss of power or in extreme cases injury or loss of life. Networking the different components of the electrical power system together is going to require that different technologies interact with each other. This interaction between different technologies will introduce new security risks. The Smart Grid will have to support legacy systems. Legacy systems typically do not implement newer security features that modernized systems have, and a system is only as secure as its weakest link. In addition, the new technologies that are being used in the Smart Grid may have security vulnerabilities in them that can be exploited. The Smart Grid will be collecting more data than the current electrical power system. It is estimated that there will be a data increase of an order of magnitude. This increase in data collection can have possible security privacy issues. The Smart Grid will also be collecting new types of information that were not recorded in the past, and this can lead to more privacy issues.

2. Literature Survey

Y. J. Kim *et. al.* as proposed system the power grid has been undergoing transformative changes due to the greater penetration of renewable energy sources and increased focus on power demand shaping. These innovative transformations on the grid require a flexible IP-based communication grid that is reliable and secure. In this article we describe an IP-based decentralized and data-centric information infrastructure that can reliably, securely, and cost-effectively support the operation and innovative applications of the next generation grid. The proposed infrastructure differs from a typical distributed system since it addresses the specific requirements of power applications such as security, distributed data sources, latency sensitive data transactions and real time event updates. The work presented here paves the way for a future data-centric power network infrastructure [1].

J. Liu *et. al.* as described the cyber security in the Smart Grid is a new area of research that has attracted rapidly growing attention in the government, industry and academia. In this paper, presented a comprehensive survey of security issues in the Smart Grid. We introduced the communication architecture and security requirements, analyzed security vulnerabilities through case studies, and discussed attack prevention and defense approaches in the Smart Grid. We also summarized the design of secure network protocols to achieve efficient and secure information delivery in the Smart Grid.

As we have reviewed, cyber security is still under development in the Smart Grid, especially because information security must be taken into account with electrical power systems. Features of the Smart Grid communication network, such as heterogeneous devices and network architecture, delay constraints on different time scales, scalability, and diversified capabilities of embedded devices, make it indeed impractical to uniformly deploy strong security approaches all over the Smart Grid [2].

V. C. Gungor as proposed system is the collaborative and low-cost nature of wireless sensor networks (WSNs) brings significant advantages over traditional communication technologies used in today's electric power systems. Recently, WSNs have been widely recognized as a promising technology that can enhance various aspects of today's electric power systems, including generation, delivery, and utilization, making them a vital component of the next-generation electric power system, the smart grid. However, harsh and complex electric-power-system environments pose great challenges in the reliability of WSN communications in smart-grid applications. This paper starts with an overview of the application of WSNs for electric power systems along with their opportunities and challenges and opens up future work in many unexploited research areas in diverse smart-grid applications. It presents a comprehensive experimental study on the statistical characterization of the wireless channel in different electric-power-system environments [3].

Y. Fan *et. al.* as described the traffic analysis presents a serious threat to wireless network privacy due to the open nature of wireless medium. In multi-hop wireless network (MWN), the mobile nodes relay others' packets for enabling new applications and enhancing the network deployment and performance. Privacy threat is one of the critical issues in multihop wireless networks, where the involves such as traffic analysis can be easily launched by a malicious adversary due to the open air transmission. Network coding has the potential to traffic analysis attacks since the coding /maxing operation is encouraged at intermediate nodes. in this paper we propose a novel network coding based privacy preserving scheme against traffic analysis in multihop wireless networks[4].

D. P. Varodayan *et. al.* as proposed system is the redundant metering is frequently used to verify the integrity of billing data reported by advanced metering infrastructure, but the redundant measurement introduces a potential confidentiality leak. We propose a way to encode the redundant measurement at a bit rate below its entropy, so that it cannot be decoded from the encoded bits alone. In this way, we guarantee information-theoretic confidentiality, regardless of the computational power of an eavesdropper. We provide practical Slepian-Wolf codes to realize security of up to 5 bit/sample for 8-bit samples based on actual power metering experiments [5].

3. Existing System

A statistical characterization of the wireless channel in different electric-power-system environments has been presented. Field tests have been performed on IEEE 802.15.4-compliant sensor nodes (using CC2420 radio chips) in a 500-kV substation, a main power control room, as well as an underground network transformer vault to measure background noise, channel characteristics, and attenuation in the 2.4-GHz frequency band. Various communication links, including both LOS and NLOS scenarios, are also considered.

Traffic analysis presents a serious threat to wireless network privacy due to the open nature of wireless medium. In multi-hop wireless network (MWN), the mobile nodes relay others' packets for enabling new applications and enhancing the network deployment and performance. Privacy threat is one of the critical issues in multihop wireless networks, where the involves such as traffic analysis can be easily launched by a malicious adversary due to the open air transmission .Network coding has the potential to traffic analysis attacks since the coding /maxing operation is encouraged at intermediate nodes. Homomorphism Encryption Functions (HEFs) have the property of homomorphism, which means operations on plaintext can be performed by operating on corresponding cipher text.

PKI allows for a chain of trust, where a first CAs extends trust to a second CAs by simply issuing a CA-certificate to the second CAs. This enables RPs that trusts the first CA to also trust subjects with certificates issued by the second CA. When two CAs issue each other certificates it is referred to as cross signing. In this way, CAs from one organization can extend trust to the CAs from other organizations, thus enabling secure interoperability across domains. CA certificates can contain various constraints to limit the trust being extended by the issuing CA to the subject CA.

4. Proposed System

In very large systems PKI could be significantly more efficient than shared keys in terms of setting up and maintaining operational credential. This is due to the fact that each entity needs to be configured with its own certificate.

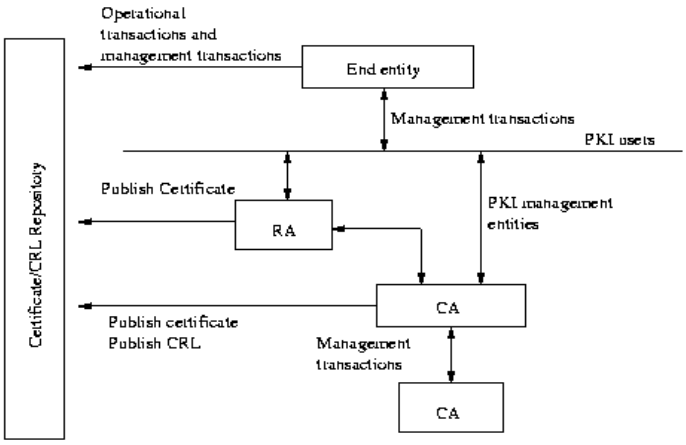

Figure 1. Block Diagram

This is as compared to symmetric key provisioning where each device may need to be configured with a unique key pair for every secure link. The PKI is more than just the hardware and software in the system. It also includes the policies and procedures which describe the setup, management, updating, and revocation of the certificates that are at the heart of PKI and PKI binds public keys with user identities through use of digital certificates. The binding is established through a registration process, where after a registration authority (RA) assures the correctness of the binding, the certificate authority (CA) issues the certificate to the user. Users or 10.The certificate subject, desiring communication with a secure resource [aka relying party (RP)] begins by sending a certificate signing request (CSR) to the RA.

The RA performs a vetting function which determines if the requested bindings are correct, and if so signs the CSR and forwards it to the CA, which then issues the certificate. Later when the certificate subject wishes to access a secure resource, it sends the certificate to the RP. The RP validates the certificate typically by requesting the certificate status from a validation authority (VA), who replies in the positive if the certificate is valid. The PKI allows for a chain of trust, where a first CAs extends trust to a second CAs by simply issuing a CA-certificate to the second CAs. This enables RPs that trusts the first CA to also trust subjects with certificates issued by the second CA. When two CAs issue each other certificates it is referred to as cross signing. In this way, CAs from one organization can extend trust to the CAs from other organizations, thus enabling secure interoperability across domains. CA certificates can contain various constraints to limit the trust being extended by the issuing CA to the subject CA.

5. Software Implementation

The Network simulator 2 (NS2) is an object-oriented, discrete event driven network simulator developed at UC Berkely written in C++ and OTcl. NS is primarily useful for simulating local and wide area networks. Although NS is fairly easy to use once you get to know the simulator, it is quite difficult for a first time user, because there are few user-friendly manuals. Even though there is a lot of documentation written by the developers which has in depth explanation of the simulator, it is written with the depth of a skilled NS user. The purpose of this project is to give a new user some basic idea of how the simultor works, how to setup simulation networks, where to look for further information about network components in simulator codes, how to create new network components.

6. Result

The network simulator is discrete event packet level simulator. The network simulator covers a very large number of applications of different kind of protocols of different network types consisting of different network elements and traffic models. Network simulator is a package of tools that simulates behavior of networks such as creating network topologies, log events that happen under any load, analyze the events and understand the network. Well the main aim of our first experiment is to learn how to use network simulator and to get acquainted with the simulated objects and understand the operations of network simulation and we also need to analyze the behavior of the simulation object using network simulation.

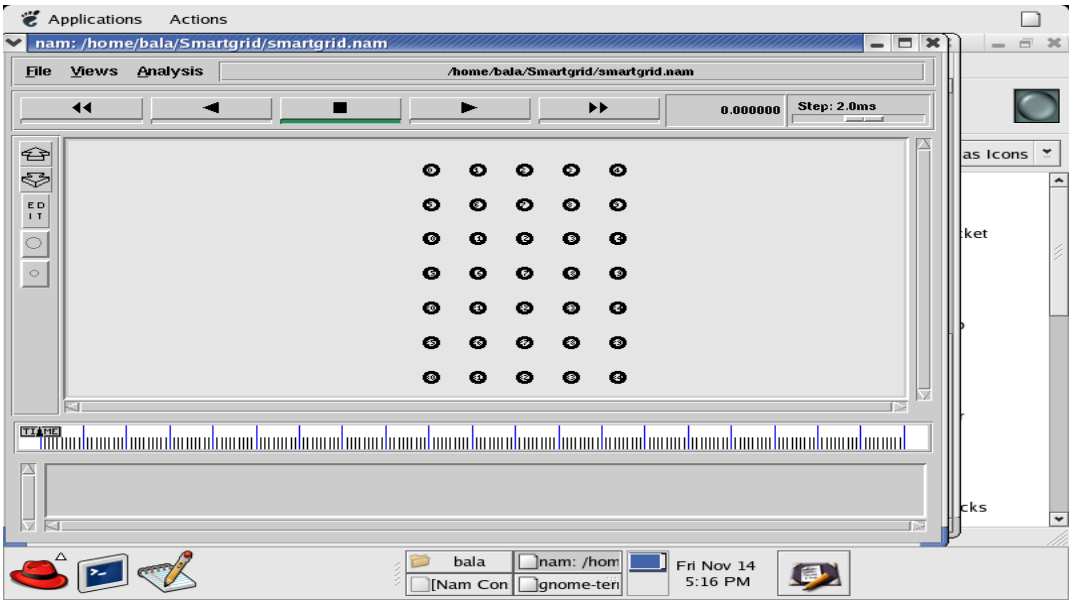

Figure 2. Normal View

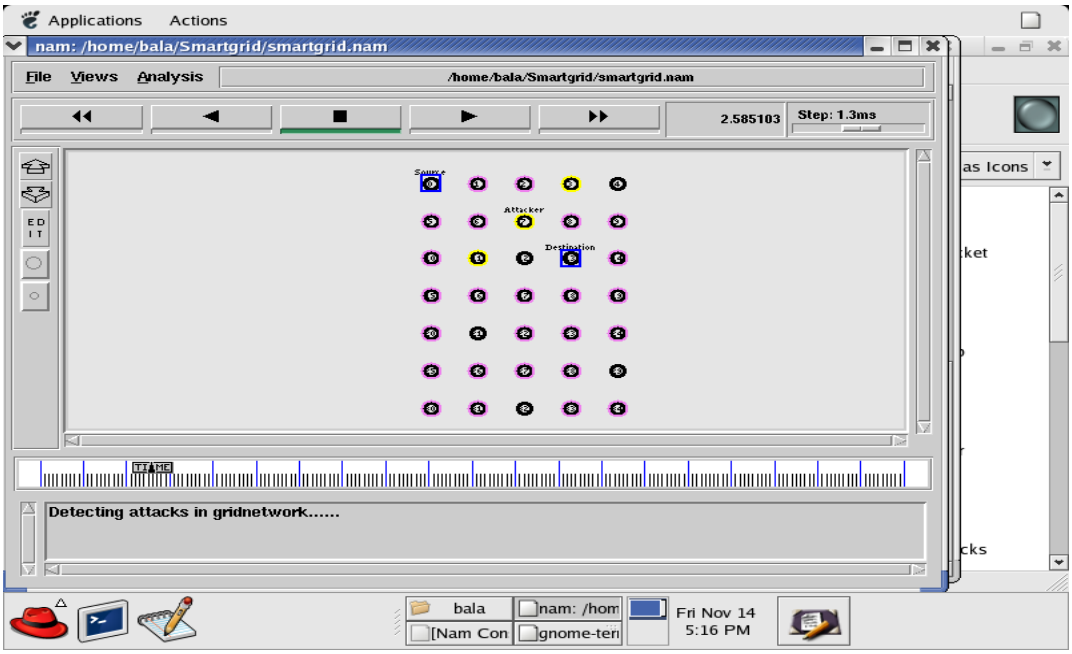

Figure 3. Detecting Attack in Grid Network 1

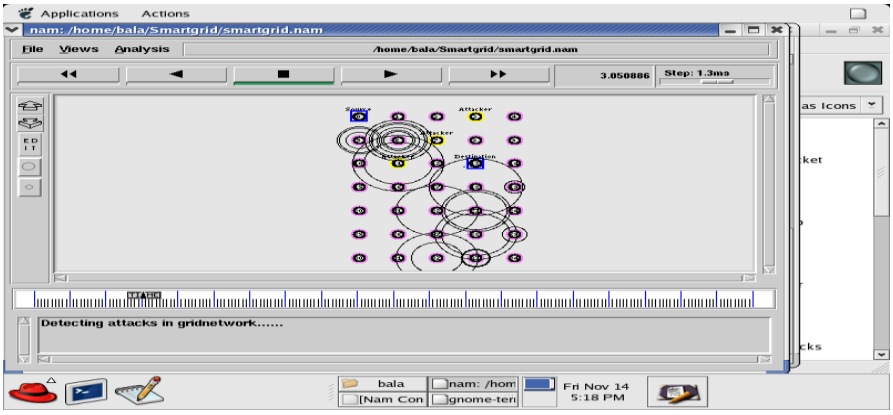

Figure 4. Detecting Attack in Grid Network 1

7. Conclusion

Several security mechanisms have been proposed to complement the PKI security services for availability, privacy preservation and scalability. proposed a mechanism to efficiently resist DoS attacks against adversaries and legitimate insiders. We believe that it can be used as a reference for the research on smart grid security and privacy. For example, when designing a security protocol for a specific application, the designers could check whether the security requirements concluded by this article have been satisfied. Deploying PKI requires manpower from the electric utility to maintain the PKI servers, handles entity software issues and manages the network infrastructure.it will require a considerable number of staff to maintain the PKI environment with a large number (e.g., several millions) of network entities. Future research should consider how to simplify the PKI environment so that less staff is required to manage it smart grid, more third-party service providers will be involved, which will introduce some new security and privacy risks into the system. In the future research should focus on how to complement the enhanced PKI system to prevent these risks.

References

[1] Y. J. Kim,*et. al*., "A Secure Decentralized Data-Centric Information Infrastructure for Smart Grid", IEEE Commun. Mag., vol. 48, no. 11, **(2010)**, pp. 58–65.
[2] T. Baumeister, "Literature Review on Smart Grid Cyber Security," Technical Report, University of Hawaii, **(2010)**.
[3] J. Liu,*et. al*., "Cyber Security and Privacy Issues in Smart Grids," IEEE Commun.SurveysTuts., vol. 14, no. 4, **(2012)**, pp. 981–97.
[4] E. K. Lee, M. Gerla, and S.Y. Oh, "Physical Layer Security in Wireless Smart Grid," IEEE Commun. Mag., vol. 50, no. 8, **(2012)**August, pp. 46-52.
[5] V. C. Gungor, B. Lu, and G. P. Hancke, "Opportunities and Challenges of Wireless Sensor Networks in Smart Grid," IEEE Trans. Ind. Electron., vol. 57, no. 10, **(2010)**October, pp. 3557.
[6] Y. Fan, *et. al*., "Network Coding based Privacy Preservation against Traffic Analysis in Multi-Hop Wireless Networks," IEEE Trans. Wireless Commun., vol. 10, no. 3, **(2011)**, pp. 834–43.
[7] A. Liu and P. Ning, "TinyECC, A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks," Proc. IPSN, **(2008)**, pp. 245–56.
[8] D. P. Varodayan and G.X. Gao, "Redundant Metering for Integrity with Information-Theoretic Confidentiality," Proc. IEEE SmartGridComm, **(2010)**October, pp. 345–49.
[9] C. Blundo, *et. al*., "Perfectly-Secure Key Distribution for Dynamic Conferences,"Advances in Cryptology-Crypto'92, LNCS 740,**(1993)**, pp. 471–86.
[10] D. He *et al*., "Privacy-Preserving Universal Authentication Protocol for Wireless Communications," IEEE Trans. Wireless Commun., vol. 10, no. 2, **(2011)**, pp. 431–36.

Authors

M. Nandhini, is pursuing PG in the discipline of Communication Systems at Muthayammal Engineering college, namakkal, Anna university, Chennai, India. She received her UG degree in the discipline of Electronics and Communication engineering in VSA Group of Institutions, Salem under Anna University, Coimbatore, India. She has published and presented a number of technical papers in Technical symposiums and conferences.

Mr. B. Praveenkumar, is currently working as an Assistant Professor in the Department of Electronics and communication engineering at Muthayammal Engineering college, namakkal (dt). He received his UG degree in the discipline of Electronics and Communication Engineering from J.A Institute of Engineering and Technology, Chennai. , under Anna University, Chennai and got PG degree in Communication Systems discipline at Mahabarathi engineering College, Chennasalem, under Anna University, Chennai. He has presented papers in National and International level conferences. He has guided number of project for students.