RESEARCH ARTICLE OPEN ACCESS

# Public Key Infrastructure Using Wireless Communication Networks

R.Karthikeyan[1], Dr.T.Geetha[2] , Shanmugapriya M[3] , Vimala M[4]
[1,2]Asst.Prof, Dept of MCA, Gnanamani college of Technology, Namakkal, INDIA.
[3,4]P.G.Scholar, Dept of MCA, Gnanamani college of Technology, Namakkal, 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. In addition, different protocols that are used in these networks use their own set of security requirements. 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**

----------**********----------

## I. Introduction

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.

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. A disruption to communications or the state management software can lead to loss of power or in extreme cases injury or loss of life.This interaction between different technologies will introduce new security risks. The Smart Grid will have to support legacy systems. 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.

## II. 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. 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.

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.

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.

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. It presents a comprehensive experimental study on the statistical characterization of the wireless channel in different electric-power-system environments.

## III. 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.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.

## IV. 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.

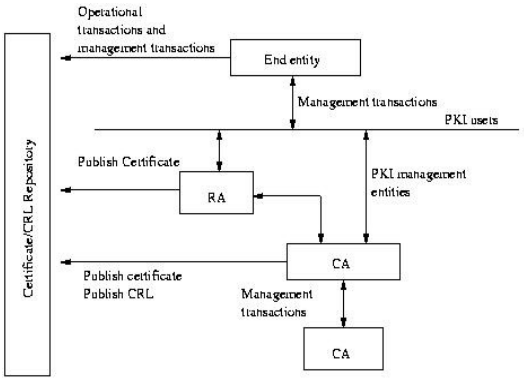



**Figure 1. Block Diagram**

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.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 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.

## V. 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.

## VI. 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.

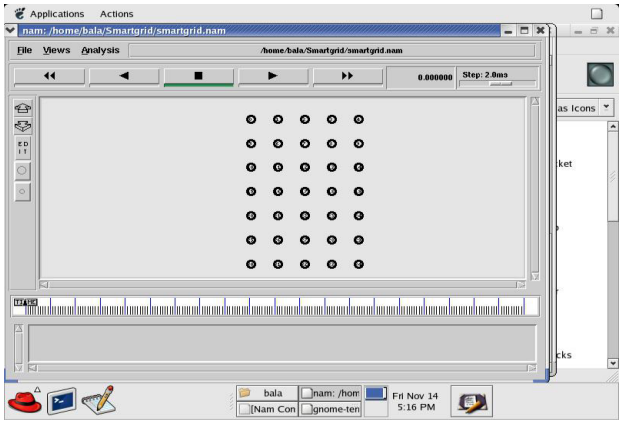



**Figure 1. Normal View**

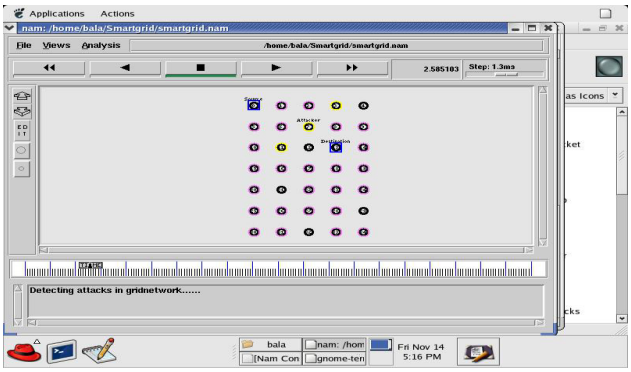
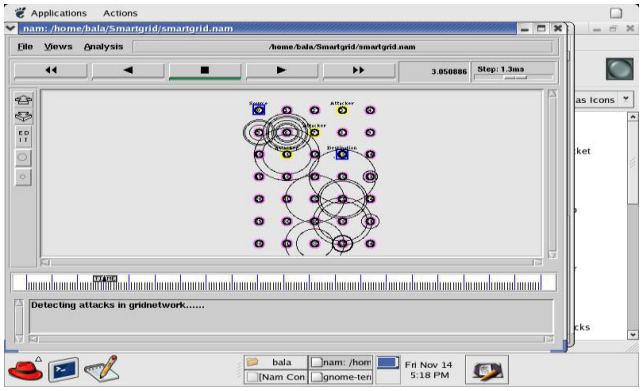



**Figure 2. Detecting Attack in Grid Network 1**




## VII. 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. 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. Yanchao Zhang, Wei Liu, Wenjing Lou, Yuguang Fang, and Younggoo Kwon," AC-PKI: Anonymous and Certificateless Public-Key Infrastructure for Mobile Ad Hoc Networks".

2. T. Sujitha, Dr. T. Hemalatha" Analysis on Certificate Validation mechanisms in Public Key Infrastructure" International Journal of Advances in Computer Science and Technology.

3. Ms. Heena Kharche, Mr. Deepak Singh Chouhan" Building Trust In Cloud Using Public Key Infrastructure" (IJACSA) International Journal of Advanced Computer Science and Applications,

4. R.Karthikeyan," Improved Apriori Algorithm for Mining Rules" in the International Journal of Advanced Research in biology Engineering science and Technology Volume 11, Issue 4, April 2016, Page No:71-77.

5. R.Karthikeyan,Dr.T.Geetha "Honeypots for Network Security", International journal for Research & Development in Technology.Volume 7.Issue 2 ,Jan 2017,Page No.:62-66 ISSN:2349-3585.

6. R.Karthikeyan,"A Survey on Position Based Routing in Mobile Adhoc Networks" in the international journal of P2P Network Trends and Technology, Volume 3 Issue 7 2013, ISSN:2249-2615, Page No.:81-88

7. R.Karthikeyan,"A Survey on Sensor Networks" in the International Journal for Research & Development in Technology Volume 7, Issue 1, Jan 2017, Page No:71-77

8. R.Karthikeyan,Dr.T.Geetha "Web Based Honeypots Network",in the International journal for Research & Development in Technology.Volume 7.Issue 2 ,Jan 2017,Page No.:67-73 ISSN:2349-3585.

9. R.Karthikeyan,Dr.T.Geetha,"A Simple Transmit Diversity Technique for Wireless Communication",in the International journal for Engineering and Techniques. Volume 3. Issue 1, Feb 2017, Page No.:56-61 ISSN:2395-1303.

10. R.Karthikeyan,Dr.T.Geetha "Strategy of Trible – E on Solving Trojan Defense in Cyber Crime Cases", International journal for Research & Development in Technology.Volume 7.Issue 1 ,Jan 2017,Page No.:167-171.

11. .Karthikeyan,Dr.T.Geetha"Advanced Honey Pot Architecture for Network Threats Quantification" in the international journal of Engineering and Techniques, Volume 3 Issue 2, March 2017, ISSN:2395-1303, PP No.:92-96.

12. R.Karthikeyan,Dr.T.Geetha"Estimating Driving Behavior by a smart phone" in the international journal of Engineering and Techniques, Volume 3 Issue 2, March 2017, ISSN:2395-1303,PP No.:84-91.

13. R.Karthikeyan,Dr.T.Geetha" SAMI: Service-Based Arbitrated Multi-Tier Infrastructure for Cloud Computing" in the international journal for Research & Development in Technology, Volume 7 Issue 2, Jan 2017,ISSN(0):2349-3585, Pg.no:98-102

14. R.Karthikeyan,Dr.T.Geetha "FLIP-OFDM for Optical Wireless Communications" in the international journal of Engineering and Techniques, Volume 3 Issue 1, Jan - Feb 2017, ISSN:2395-1303,PP No.:115-120.

15. R.Karthikeyan,Dr.T.Geetha "Application Optimization in Mobile Cloud Computing" in the international journal of Engineering and Techniques, Volume 3 Issue 1, Jan - Feb 2017, ISSN:2395-1303,PP No.:121-125.

16. R.Karthikeyan,Dr.T.Geetha"The Sybil Attack" in the international journal of Engineering and Techniques, Volume 3 Issue 3, May - Jun 2017, ISSN:2395-1303,PP No.:121-125.

17. R.Karthikeyan,Dr.T.Geetha"Securing WMN Using Hybrid Honeypot System" in the international journal of Engineering and Techniques, Volume 3 Issue 3, May - Jun 2017, ISSN:2395-1303,PP No.:121-125.

18. R.Karthikeyan,Dr.T.Geetha "Automated Predictive big data analytics using Ontology based Semantics" in the international journal of Engineering and Techniques, Volume 3 Issue 3, May – Jun 2017, ISSN:2395-1303,PP No.:77-81.

19. R.Karthikeyan,Dr.T.Geetha"A Survey of logical Models for OLAP databases" in the international journal of Engineering and Techniques, Volume 3 Issue 3, May - Jun 2017, ISSN:2395-1303,PP No.:171-181

20. R.Karthikeyan,Dr.T.Geetha"A Client Solution for Mitigating Cross Site Scripting Attacks" in the international journal of Engineering Science & Computing, Volume7,Issue6, June 2017, ISSN(0):2361-3361,PP No.:13063-13067.

21. R.Karthikeyan,Dr.T.Geetha"A Condensation Based Approach to Privacy Preserving Data Mining" in the international journal of Engineering Science & Computing, Volume7,Issue6, June 2017, ISSN(0):2361-3361,PP No.:13185-13189.

22. R.Karthikeyan,Dr.T.Geetha"Biometric for Mobile Security" in the international journal of Engineering Science & Computing, Volume7,Issue6, June 2017, ISSN(0):2361-3361,PP No.:13552-13555.

23. R.Karthikeyan,Dr.T.Geetha"Data Mining on Parallel Database Systems" in the international journal of Engineering Science & Computing, Volume7,Issue7, July 2017, ISSN(0):2361-3361,PP No.:13922-13927.

24. R.Karthikeyan,Dr.T.Geetha"Ant Colony System for Graph Coloring Problem" in the international journal of Engineering Science & Computing, Volume7,Issue7, July 2017, ISSN(0):2361-3361,PP No.:14120-14125.

25. R.Karthikeyan,Dr.T.Geetha"Classification of Peer –To- Peer Architectures and Applications" in the international journal of Engineering Science & Computing, Volume7,Issue8, Aug 2017, ISSN(0):2361-3361,PP No.:14394-14397.

26. R.Karthikeyan,Dr.T.Geetha"Mobile Banking Services" in the international journal of Engineering Science & Computing, Volume7,Issue7, July 2017, ISSN(0):2361-3361,PP No.:14357-14361.

27. R.Karthikeyan,Dr.T.Geetha "Neural Networks for Shortest Path Computation and Routing in Computer Networks" in the international journal of Engineering and Techniques, Volume 3 Issue 4, Aug 2017, ISSN:2395-1303,PP No.:86-91.

28. R.Karthikeyan,Dr.T.Geetha "An Sight into Virtual Techniques Private Networks & IP Tunneling" in the international journal of Engineering and Techniques, Volume 3 Issue 4, Aug 2017, ISSN:2395-1303,PP No.:129-133.

29. R.Karthikeyan,Dr.T.Geetha "Routing Approaches in Mobile Ad-hoc Networks" in the International Journal of Research in Engineering Technology, Volume 2 Issue 5, Aug 2017, ISSN:2455-1341, Pg No.:1-7.