SURVEY ON SMART GRID SECURITY: THREATS, CHALLENGES AND AUTHENTICATION MECHANISM

Prof. Pavan D.Mahendarkar[1], Adiba Maniyar[2]

[1]Prof., [2]PG Scholar, Dept. of Computer Science Engineering, BLDEA's College of Engineering and Technology (India)

ABSTRACT

The primitive electrical power grid is revolutionalized into the smart grid. Smart grid integrates the traditional electrical power grid with information and communication technologies (ICT). Such integration empowers the electrical utilities providers and consumers, improves the efficiency and the availability of the power system while constantly monitoring, controlling and managing the demands of customers. A smart grid is a massive network composed of millions of devices and entities connected with each other. This paper proposes an effective 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. Further, the proposed authentication mechanisms are intuitive and require no (or minimum) user effort.

Keywords: Enhanced Identity-Based, Key Management, Cryptography (EIBC), Smart Grid (SG) Mutual Authentication, and Secure Remote Password (SRP).

I. INTRODUCTION

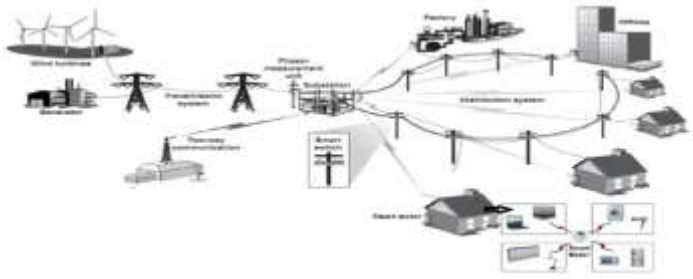
Smart grids provide electricity demand from the centralized and distributed generation stations to the customers through transmission and distribution systems. The smart grid is an evolved electrical power grid infrastructure for better efficiency, reliability, with possible integration of renewable and alternate energy sources. The grid is operated, controlled and monitored using information and communications technologies (ICT).The ICT infrastructure in the smart grid environment needs to be reliable, highly-available, scalable, secure, and easy-to-manage. Power engineering society, along with its counterparts in ICT, has developed the first smart grid conceptual model which consists of three layers: energy and power systems layer communications layer, and information technology layer [1-2].But where as in existing power grid, the electricity is provided to a large amount of customers from a few central generators but the smart grid uses two-way communication and flows of electricity and information to make an automated and distributed advanced energy delivery network. There are many benefits for smart grid such as improving electric power reliability and quality. In addition improve grid security and self-healing [3]

"Fig. 1," Smart Grid

The remainder of this paper is organized as follows. Section 2 gives a brief idea about smart grids architecture. Section 3 addresses the grid's security challenges in proposing smart grid security solutions. Section 4 talks about the various attackers and the types of attacks they come across. Section 5 points out the authentication mechanism in smart grid network. Section 6 states the literature review. Section 7 details future scope and Section 8 summarizes the paper conclusion.

II. SMART GRIDS ARCHITECTURE

The major components in smart grid architecture are Electric Household Appliances, Renewable Energy Resources, Smart Meter, Power utility Centre and Service provider [4], as illustrated in Fig.2 [5].Electrical Household Appliances (smart and legacy) are suspected to be able to communicate with smart meters via a House Area Network (HAN) assisting efficient energy intake control to all home devices. Renewable energy resources are solar and wind power that provides home devices through local generate electricity. Smart meter contains a microcontroller that has memory, digital ports, timers, real-time, and serial communication facilities. Smart meters sign-up the power intake generally and transmit it to the utility server, connect or detach a customer source of energy and send out alarms in case of a problem. Power utility communicates with smart meters to control energy intake. Service provider's suppliers identify contracts with customers to provide electricity for individual devices companies interact with internal devices via messages carried by the smart meter. To identify such interaction, service providers should sign-up with the electric utility and obtain electronic accreditations for their details and public keys. The accreditations are then used to facilitate secure marketing communications with customers [4].

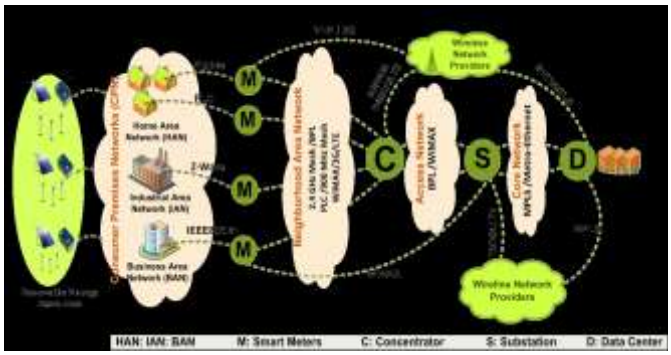


"Fig. 2," Smart Grid Architecture

Smart grids are characterized by two types of communication: Home Area Network (HAN) and Wide Area Network (WAN).

A HAN connects the in-house smart devices across the property with smart meters. The HAN can connect using Zigbee, wired or wireless Ethernet, or wireless Bluetooth.

A WAN, on the other hand, is a bigger network that joins the smart meters, companies, and energy application. The WAN can connect using WiMAX, 3G/GSM/LTE, or fibre optics. A smart meter functions as an entrance between the in-house devices and the exterior parties to provide needed information [4].



"Fig. 3," Basic Network Architecture

III. SECURITY CHALLENGES IN SMART GRID

3.1 Access Control and Identity Management

It is important to ensure that data transmitted via smart grids is kept confidential and that no one but the intended receiver is able to see the message. In addition, the smart grid contains many components that are interconnected. Because of security concerns related to this, authentication is needed to verify the identity of the receiver in order to avoid any disruption or exploitation. Access to the control centre, transmission, and distribution grids is allowed only for authenticated users, groups, and services [7].

3.2 Privacy and Security Policies

There is a huge necessity for suitable security policies to establish relationships among consumers, utilities, and third parties, although applying security and privacy policies should not result in unsatisfactory latencies.

3.3 Threat Defence

There is much vulnerability inherent to target smart grids; therefore, it is necessary to protect the grids from defined threats by building an effective, layered defence system to function broadly across the entire grid infrastructure. Threat defence provides network segmentation and access control to defend against denial-of-service (DoS). In addition, it provides a suite of security technologies such as firewall, intrusion prevention system (IPS) and virtual private network (VPN) [7].

3.4 Physical Security

Smart grid systems can have thousands, and often even millions [5] of remote points and field area networks. This makes it challenging to maintain the physical security of the smart grid. The geographical dispersion of these systems also means that it may be difficult to access all of the terminals for maintenance.

3.5 Connectivity

Communications connectivity in smart grids implies a transition towards an Internet-like distributed environment in which huge numbers of devices are interconnected. This is one of the emerging challenges in this area and as such the application of protective techniques is important [7].

IV. ATTACKERS AND TYPES OF ATTACKS

There are various vulnerabilities that can ruin smart grid by typical attackers with different motives and expertise and could cause different levels of damage to the network. Attackers could be script kiddies, elite hackers, terrorists, employees, competitors, or customers. The authors in [8] group attackers into: 1) Nonmalicious attackers who view the security and operation of the system as a puzzle to be cracked. Those attackers are normally driven by intellectual challenge and curiosity. 2) Consumers driven by vengeance and vindictiveness towards other consumers making them figure out ways to shut down their home's power. 3) Terrorists who view the smart grid as an attractive target as it affects millions of people making the terrorists' cause more visible. 4) Employees disgruntled on the utility/customers or ill-trained employees causing unintentional errors. 5) Competitors attacking each other for the sake of financial gain.The various types of attacks are:

4.1 Network Availability

Malicious attacks on intending network availability can be called as DoS attacks. They attempt to slow down, block, or even manipulate information transmission so as to make network resources unavailable to terminals that are in need to exchange information in SG. As shown out by NIST [9], the high priority is of designing the information transmission networks that should be robust to attacks which are targeting network availability, because the network unavailability may outcome in the loss of real-time monitoring of critical smart grid infrastructures and power system disasters.

4.2 Data Integrity

Data integrity attacks generally intend to deliberately manipulate or corrupt information shared within the SG, its elements and may be highly damaging in the SG

4.3 Privacy of Information

Information privacy attacks just intend to eavesdropping on communications in SG elements so as to acquire desired information, like consumer account number and their energy usage. Initially, the work was done by Li et al. [10], who investigated the fundamental limit, i.e., how much channel capacity is essential to promise the secured communications among SG elements, from the perspective of information theory, and found the situation of a single meter and or Gaussian noise communication channel with an eavesdropper.

V. AUTHENTICATION MECHANISM FOR SMART GRID NETWORK

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

5.1 Authentication Management

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

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

5.1.2 What the subject knows e.g. a password;

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

5.1.4 What the subject has biometrically e.g. fingerprints.

The key can be symmetric, supported by a private key cryptography system, or asymmetric, supported by a public key cryptography system [11]. The secure communication channel using a security key for data encryption, to protect their data from unauthorized parties.

5.2 SRP Protocol

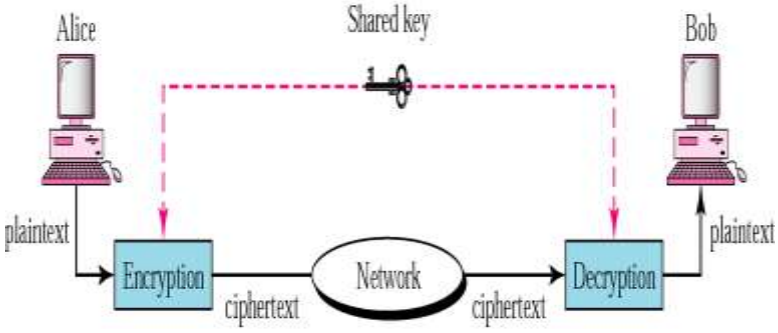
SRP is an authentication and key exchange protocol for secure password verification and session key generation over an insecure communication channel. SRP utilizes asymmetric key exchange (AKE) [12]. and stores verifiers instead of the passwords. AKE uses a one-way (hash) function to compute the verifier 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.

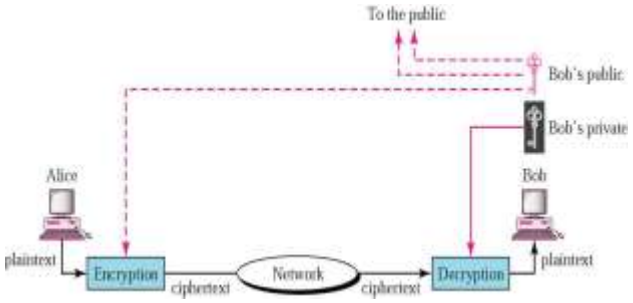
The secure remote password (SRP) protocol [11] also utilizes a predefined password and the identifier to construct a key, which delivers most of the characteristics that are expected from an authentication scheme. SRP is a fast mutual authentication scheme that uses the session key in the mechanism and resists the dictionary attacks. Furthermore, in the SRP protocol, compromising the server does not make it easy to find the password, compromising the password does not lead to revealing the past session keys (forward secrecy), and finally, compromising the session key does not lead to compromising the password

5.3 PKI

In the PKI [13], 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.



"Fig.4," Privacy using Symmetric-Key Encryption



"Fig.5," Privacy using Public-Key Encryption

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.

VI. LITERATURE REVIEW

Metke and Ekl power grid, uses two-way flows of electricity and information to create a widely distributed automated energy delivery network. In this article, we survey the literature till 2011 on the enabling technologies for the Smart Grid. We explore three major systems, namely the smart infrastructure system, the smart management system, and the smart protection system. We also propose possible future directions in each system. Specifically, for the smart infrastructure system, we explore the smart energy subsystem, the smart information subsystem, and the smart communication subsystem. For the smart management system, we explore various management objectives, such as improving energy efficiency, profiling demand, maximizing utility, reducing cost, and controlling emission. We also explore various management methods to achieve these objectives. For the smart protection system, we explore various failure protection mechanisms which improve the reliability of the Smart Grid, and explore the security and privacy issues in the Smart Grid.

Wong et al. [17] proposed the logical key hierarchy protocol, which is based on constructing a logical tree of keys. From its leaf to the root, every node shares symmetric keys. Whenever a member wants to join/leave the session, all the symmetric keys are revised in the tree. The proposed key management scheme is scalable; however, the main drawback of the scheme is that the keys are hashed rather than encrypted and distributed if a new member joins the session [18]. Choi et al. [19] proposed a key management scheme named as Advanced Key Management Architecture (ASKMA), a scheme they proposed that supports message broadcasting and secure communications. The scheme performance well and minimizes the burden on low power nodes. Their scheme uses a logical key hierarchy. The scheme has many benefits; however, it may be less efficient during the multicast communication process. Another issue for ASKMA is its lack of availability, that is, the continuity of the security processes when there is a node failure or when a new node joins in. Choi et al. [18] proposed ASKMA+, an improved and modified of ASKMA and is more efficient. This new scheme reduces the number of stored keys and provides efficient and protected multicast and broadcast communications. However, the availability issue of ASKMA+ is still not resolved. National Laboratories [20] proposed the SKE (Secure Key Establishment) scheme to secure SCADA system. SKE started with classifying the keys exchange on the SCADA network into two parts. The first is Controller-to-Subordinate (C-S) MTU-RTU, and SUB-MTU-RTU which uses symmetric keys. The second classification is a Subordinate-to-Subordinate (SS) communication,

which works as a peer-to-peer communications using public key cryptography. However, SKE cannot support RTU-to-RTU communications. Furthermore, broadcast and multicast scenarios are also not supported by SKE.

VII. FUTURE SCOPE

In this section we have discussed about security of SG to ensure reliable operation of it and mitigate the security attacks with perspection on privacy preservation.

7.1 Interoperability Between Cryptographic Systems in SG Elements

Since there will be different cryptography requirements and security needs of each of various communication protocols and technologies used in SG, employing interoperability between cryptographic systems are not a easy task. Before employing cryptography, It is very essential for us to have a method of securely communicating the cryptographic keys between the SG elements possible solutions can be is to design, as suggested in [15],[14], a public key infrastructure approach, which can use the layered based approach in communication models. A whole solution based on this these idea is needed.

7.2 Clash in Between Privacy Preservation and Information Usage

Balancing privacy preservation and information accessibility is not easy. Assume, for example, group of users. On one side, the large information about demand patterns such users are intending to disclose, the smart decisions a management system can take so as to optimize profits. However, more accessibility of information usually demands more privacy leaks, which can quickly reveals user profiles and behaviors. We advice that to issuing numerous privacy preservation levels similar to these in access control, each of which describes a tolerable amount of data leak. On each level, we can define the management objectives based on the information which can be used,. For example, single privacy policy within a group of users may allow full information exchange. Hence, such group of users can increase their profits by employing their shared information. Other mechanisms accomplishing advanced encryption techniques like AES, Homomorphism may also be applicable.

7.3 Effect of Increased System Complexity and Spreaded Communication Paths

The advanced infrastructure used in SG is a double-edged sword. On one side, it puts the foundation for the future advanced power grid that can serve better. On the another side, high complexity of system and spreaded communication networks can easily lead to an increment in vulnerability to cyber security attacks and system failures. A wholly implemented SG may contain of millions of nodes. This system large scale makes it hectic to expect how attacks may be made by an unpredictable and clever adversary, and which resultant failures could happen because of many dependent or independent factors [16]. One possible direction to overcome this challenge is to split the whole system into many individual sub-grids so that the system complexity can be declined easily. Therefore, the effect of system failures and attacks can be at a too limited level as much as possible.

VIII. CONCLUSION

Traditional power systems are moving towards digitally enabled smart grids which will enhance Communications, improve efficiency, increase reliability, and reduce the costs of electricity services. Power generations, transmissions, distributions and consumptions enabled with the ICT empower the shareholders for

better communicate in two directions and manage the grid efficiently. 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?? this paper, we surveyed the authentication mechanism in smart grid networks, the types of attacks and attackers, the challenges present in designing new security solutions, and the current and needed solutions.

REFERENCES

[1] G. J. Fitzpatrick and D. A. Wollman, "NIST interoperability framework and action plans," the 2010 IEEE Power and Energy Society General Meeting, 2010, pp. 1-4.

[2] Saifur Rahman, "What is a Smart Grid and What Can it Do for us?", invited talk, the IEEE Power & Energy Society Chapter, Abu Dhabi, UAE, www.saifurrahman.org, accessed March 2012, pp. 1-23.

[3] M. Merabti, M. Kennedy, and W. Hurst, "Critical Infrastructure Protection A 21sst Century," in Communications and Information Technology (ICCIT), 2011 International Conference on, 2011, pp. 1-6.

[4] Fadi Aloula, A. R. Al-Alia , Rami Al-Dalkya, M. Al-Mardinia, and a. W. El-Hajjb, "Smart Grid Security: Threats, Vulnerabilities and Solutions " International Journal of Smart Grid and Clean Energy vol. 1, 2012.

[5] E. D. Knapp and R. Samani, "Chapter 1 - What is the Smart Grid?," in Applied Cyber Security and the Smart Grid, ed Boston: Syngress, 2013, pp. 1-15.

[6] Al-Omar B, Al-Ali AR, Ahmed R, et al. Role of information and communication technologies in the smart grid. Journal of Emerging Trends in Computing and Information Sciences, 2012; 3(5):707-716.

[7] M. B. Line, I. A. Tondel, and M. G. Jaatun, "Cyber security challenges in Smart Grids," in Innovative Smart Grid Technologies (ISGT Europe), 2011 2nd IEEE PES International Conference and Exhibition on, 2011, pp. 1-8.

[8] Flick T and Morehouse J. Securing the Smart Grid: Next Generation Power Grid Security. Syngress, 2010.

[9] The Smart Grid Interoperability Panel - Cyber Security Working Group. Guidelines for Smart Grid cyber security: Vol. 1, Smart Grid cyber security strategy, architecture, and high-level requirements. NISTIR 7628.

[10] H. Li, L. Lai, and R. C. Qiu. Communication capacity requirement for reliable and secure state estimation in smart grid. IEEE Smart Grid- Comm2010, 2010.

[11] 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.

[12] Z. Fadlullah, N. Kato, R. Lu, X. Shen, and Y. Nozaki, "Towards secure targeted broadcast in smart grid," IEEE Common. Mag.,vol. 50, no. 5, pp. 150–156, May 2012 [Online]. Available: http

[13] 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.

[14] V. Dehalwar, R. K. Baghel, M. Kolhe. Multi-Agent based Public Key Infrastructure for Smart Grid, The 7th International Conference on Computer Science & Education (ICCSE 2012) July, 2012. Melbourne, Australia.

[15] T. Baumeister. Literature review on smart grid cyber security, Technical Report, http://csdl.ics.hawaii.edu/techreports/10-11/10-11.pdf. 2010.

[16] Department of Energy, Office of Electricity Delivery and Energy Reliability. Study of security attributes of smart grid systems - current cyber security issues 2009, http://www.inl.gov/scada/publications/d/securing the smart grid current issues.pdf.

[17] S. Mittra, "Iolus: a framework for scalable secure multicasting," presented at the Proceedings of the ACM SIGCOMM '97 conference on Applications, technologies, architectures, and protocols for computer communication, Cannes, France, 1997.

[18] W. Chung Kei, M. Gouda, and S. S. Lam, "Secure group communications using key graphs," Networking, IEEE/ACM Transactions on, vol. 8, pp. 16-30, 2000.

[19] C. Donghyun, L. Sungjin, W. Dongho, and K. Seungjoo, "Efficient Secure Group Communications for SCADA," Power Delivery, IEEE Transactions on, vol. 25, pp. 714-722, 2010.

[20] C. Donghyun, K. Hakman, W. Dongho, and K. Seungjoo, "Advanced Key-Management Architecture for Secure SCADA Communications," Power Delivery, IEEE Transactions on, vol. 24, pp. 1154-1163, 2009.

[21] C. L. Beaver, D.R. Gallup, W. D. NeuMann, and a. M. D. Torgerson. Key Management for SCADA [Online]. Available:http://energy.sandia.gov/wp/wp-content/gallery/uploads/013252.pdf