International Journal of Latest Engineering and Management Research (IJLEMR)
ISSN: 2455-4847
www.ijlemr.com || Volume 03 - Issue 03 || March 2018 || PP. 91-96

A Review and Techniques in Smart Grid for Authentication of Messages

Asma Siddiqua[1], Saba Begum[2], Mirza Younus Ali Baig[3], C Atheeq[4]
(CSE Department, DCET, OU, India)[1,2,3,4]

Abstract: Smart grid is an electricity supply network that uses digital communication technology to detect and react in local changes in usage. Deployment of Digital Technology in smart grids ensures the reliability, efficiency and accessibility to the consumers regarding all utilities which count towards the economic stability of the nation. However, a smart grid enables the two-way communication between the electricity supplier and users, which brings security challenges as Confidentiality, Real time Authentication, Replay-attack Resistance, low storage and communication cost. The further issues of smart grid terms of information and communication technologies, sensing, measurement, control and automation technologies, power electronics and energy storage technologies. This chapter presents the development of smart grids and an analysis of the methodologies, milestones and expected evolutions of grid technologies that will transform society in the near future.

Keywords: Authentication, Confidentiality, Security, Sensors, Smart grid.

I. INTRODUCTION

Smart Grid is a concept regarding digital technology application and electric power network. It offers a lot of valuable technologies that can be used within the near future or are already in use today. Smart Grid includes electric network, digital control appliance, and intelligent monitoring system. All of these, can deliver electricity from producers to consumers, control energy flow, reduce the loss of what, and make the performance of the electric network more reliable and controllable. In the short term, a smarter grid will function more efficiently, enabling it to deliver the level of service we have come to expect more affordably in an era of rising costs, while also offering considerable societal benefits – such as less impact on our environment. In longer term, we can expect the Smart Grid to spur the kind of transformation that the internet has already brought to the way we live, work, play and learn.

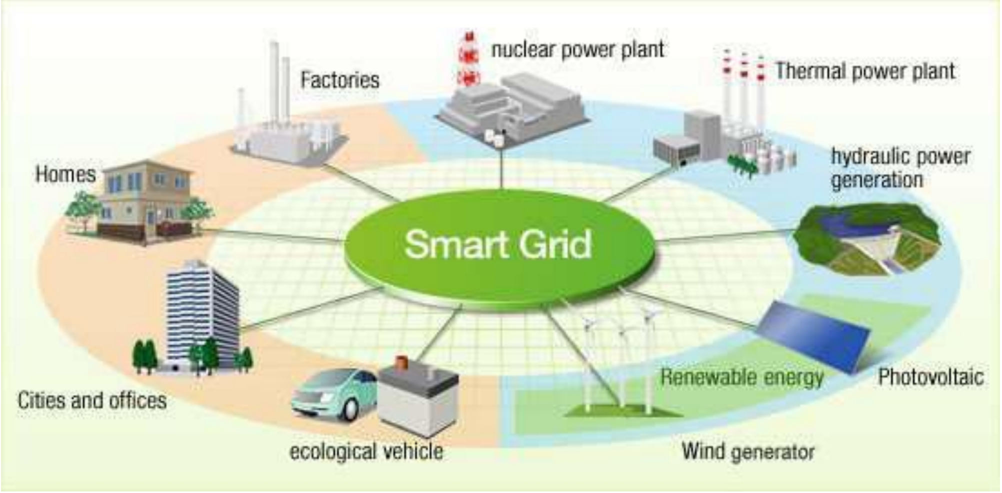

Fig1: Smart grid

Smart Grid can offer a lot of potential economic and environmental benefits and Significance:

1. Improve reliability of power quality and transmission
2. Increased power distribution efficiency and conservation
3. Reduced costs for electric utilities
4. Reduced expenditures on electricity by households and businesses
5. Lower Greenhouse Gas(GHG) and other gas emissions

Reliability: because of the requirement of power increasing, the slow response time of mechanical switches, a lack of automatic analytics, more and more blackouts and brownouts happen. Take US as an example [1], as we know, in the past 40 years, there have been 5 massive blackouts, and three of them occurred in the past 9 years.

However, Smart Grid can solve these problems, today. As technology evolves, people can make power more controllable and planned centrally. Now, with Smart Grid's help, we avoid this kind of risks before they happen.

Efficiency: according to research data, if the power grid can be more efficient by just 5%, it will save us the energy as the same as 53 million cars' GHG emission [2].Think about it, if every American family takes off one incandescent bulb, and use a compact fluorescent bulb instead. The whole country will conserve enough electric energy to light 3 million homes and save at least $600 million annually [2].Therefore, we really get the great reason to improve Smart Grid.

The design goals are listed as follows.

1. Confidentiality
   Confidentiality ensures that nobody can obtain others' electricity usage data if the protocol is correctly executed.
2. Real-time authentication
   The transmitted message can be real-timely authenticated by the receiver, which is vital to resist against the denial-of-service (DoS) attack.
3. Replay attack-resistance
   The receiver can check whether the received authentication messages are the replay of previous used messages.
4. Low storage and communication cost
   The storage and communication cost of the smart meter should be low due to the sensor's limited resource.

II. RELATED WORK

From the IEEE P2030 SG standards, three task forces are formulated to carry out the smart grid agenda, namely power engineering technology (task force 1), information technology (task force 2), and communication technology (task force 3), where information technology (task force 2) is related to dig-ital security of SG communications. In other words, this task force is responsible for designing system and communications protection policies and procedures to fend off malicious attacks against SG. However, the main shortcoming of these policies consists in the broad and coarse design directions that they provide. A utility computer network security management and authentication system for SG is proposed by Hamlyn et al. [3]. However, it is limited to the authentication between host area electric power systems and electric circuits.

In [4], power system communication and digital security issues are taken into account as critical components of SG. It suggests that a number of digital security issues need to be addressed for SG communication. For example, it was pointed out that combining SCADA/EMS (Supervisory Control and Data Acquisition/Energy Management System) with information technology networks leads to significant security threats. In addition, this work indicated that broadband Internet technologies may enable intruders to access smart meters and even the central system by which they may collect metering data. Indeed, the metering data, along with price information, special offers, and so forth, may contain sensitive data of the client which may lead to breach of privacy.

Metke et al. indicated in [5] that SG deployments must meet stringent security requirements. For example, they consider that strong authentication techniques is a requisite for all users and devices within the SG. This may, however, raise to scalability issue. In other words, as the users and devices in SG are expected to be quite large, the strongest authentication schemes may not necessarily be the fastest ones. As a consequence, scalable key and trust management systems, tailored to the particular requirements of the utility provider and users, will be essential as far as SG communication is concerned .Kursawe et al. present the need for secure aggregation of data collected from different smart meters . They present four concrete protocols for securely aggregating smart meters data readings, namely interactive protocols, Diffie-Hellman Key-exchange based protocol, Diffie-Hellman and Bilinear-map based protocol, and low-overhead protocol. Interestingly, the last three protocols rely upon the original Diffie - Hellman key exchange protocol in its securest form or its more relaxed variants. The computation and communication overheads with the relaxed variants of Diffie-Hellman based security aggregation schemes on smart meters are verified to be lower. However, this work does not consider smart meters authentication, for which, we also can extend Diffie-Hellman based approaches.

Three methods are compared in [6] for authenticating demand response messages in SG, namely Bins and Balls (BiBa), Hash to Obtain Random Subsets Extension (HORSE), and Elliptic Curve Digital Signature Algorithm (ECDSA). It is demonstrated that ECDSA offers higher security in contrast with BiBa and HORSE, at the expense of increased computational complexity, particularly at the receiver-end. In this paper, by first providing a broad SG communications framework, we envision a secure and reliable framework comprising a lightweight message authentication scheme, which is customized to the specific needs of SG.

In a smart grid, the utility company considers the correctness of the calculated bills as the most important issue. However, from the customer's point of view, privacy is the main concern. Researchers have designed privacy-preserving data aggregation protocols using advanced cryptographic techniques such as zero knowledge proof and homomorphic encryption. Bohil and colleagues proposed a privacy model for smart metering, in which a trusted third-party proxy is introduced to collect meter readings from individual customers and aggregate data before forwarding it to the utility company.

There are a number of proposals on the use of a homomorphic cryptosystem for privacy-preserving data aggregation. For example, Li et al. proposed an in network aggregation scheme that uses SMs to aggregate users' encrypted data en-route for an authorized entity, but their scheme only protects against passive attacks. Deng et al. overcame this by signing each encrypted data. Li et al. further improved the work in by using the Boneh-Lynn-Shacham (BLS) signature scheme that allows a batch verification of signatures. To reduce overheads, Lu et al. proposed a scheme that packs user's multidimensional data into a single encrypted one, whereas Ruj et al. proposed a decentralized aggregation method. Existing homomorphic encryption to achieve privacy preserving is based on the computational expensive operations, which may not be desirable for smart grids with limited resources in terms of both bandwidth and computation. On other hands, several researchers focused on privacy preserving aggregation in different conditions by using multiparty computation differential privacy, and the aggregated pseudo status variation Sign encryption, now an international standard for data security (ISO/IEC 29150, Dec 2011), was invented by Zheng and disclosed to the public at CRYPTO 1997 . It is a cryptographic primitive by which confidentiality is provided through encryption and authenticity is achieved through digital signature, seamlessly at the same time. Performing these two services simultaneously is far more efficient that performing each separately. This allows smaller devices, such as radio frequency identifiers (RFIDs) and wireless sensor networks, to perform high-level security functions. Therefore, sign encryption is very suitable for key management in Smart Grid and other resource constrained networks.

Adi Shamir introduced the concept of identity based cryptography IN The idea of identity based cryptography is to enable a user to use any identity-related string (such as name, Identity number, Email address, etc.) as his public key. Identity based cryptography serves as an efficient alternative to Public Key Infrastructure (PKI) based systems. ID-based sign encryption was first studied by Malone-Lee et al. As ID-based cryptography does not require public key authentication, it has a higher efficiency of computing and communications, and more suitable for Smart Grid communication security. In order to further improve the safety and efficiency of the Smart Grid communication, this paper provides the use of secure sign encryption algorithm based on the identity and timestamps. Timestamps is introduced to ensure message freshness, hence, combats against replay attack. The computation and transmission costs of the algorithm are small, which addresses the needs of the Smart Grid that having distributed management and resource-constrained environment.

Cryptography plays a significant role in improving the integrity and confidentiality of the data in SG. Many existing standard encryption algorithms and authentication schemes are adopted in SG. Symmetric cryptographies, such as DES (Data Encryption Standard), Triple DES, AES (Advanced Encryption Standard), are widely employed in SG to efficiently defend against possible threats. For example, ZigBee employs 128-bit AES encryption for security. Compared with the asymmetric cipher, symmetric cipher handles large amounts of data more efficiently, but often has a shorter lifespan. It is recommended to change the symmetric cipher periodically. However, it becomes an importance challenge in SG, because there are millions of wide-spread entities [7].The asymmetric encryption is also applied to meet their specific requirements. Nguyen and Rong employ the identity-based cryptography to secure ZigBee communication. The sender uses the receiver's identification as the public key to encrypt the message; the receiver obtains the corresponding private key from the private key generator to decrypt the message [8]. Li et al. present a secure information aggregation approach for smart grids. When the smart meters submit their own data and forward other's data, the homomorphic encryption is employed to ensure that intermediate results are not revealed to any device en route

As they mentioned "asymmetric encryption is more computationally expensive than symmetric encryption," the cost of device and power consumption should be considered in cryptography design The management of the encryption key is a challenging and necessary issue in utilizing cryptographic algorithms for the smart grid. PKI is considered as the basis of most effective key management solution in smart grid. Wu and Zhou propose a new key management scheme for smart grid, combining the public key and symmetric key. The elliptic curve cryptography is applied as public key to securely establish the symmetric keys for the agents to communicate; the Needham- Schroeder authentication protocol is employed as symmetric key [9]. Xia and Wang propose a secure key distribution protocol for smart grid. A trust anchor which is set up in the third party environment, can work as a Lightweight Directory Access Protocol (LDAP) server. They show their method is secure against impersonation attack, replay attack, man -in -the-middle attack and so forth. Kim and Choi introduce an efficient and scalable key management protocol for secure unicast, multicast, and broadcast communications in smart grids, based on a binary tree to manage secret keys shared among entities. All of these methods rely on a third party for identity authentication or key generation. It might cause additional equipment cost and communication traffic.

Many researchers focus on the special characteristics of the smart grid systems and propose lots of novel methods. Focus on the privacy aspect of smart metering data, Efthymiou and Kalogridis propose a solution for anonym zing high-frequency metering data which need to be transmitted to the control center often enough but doesn't need to be attributable, by employing a pseudonymous ID without compromising the operations of the utility and/or distribution network . To protect the home area network (HAN), Yan et al. propose a secure data aggregation and dispatch scheme. The orthogonal chip code is employed to keep the confidentiality and anonymity for collecting the reading-data of smart home devices to the household smart meter and for distributing the control message [10]. To improve the efficiency and security of advanced metering infrastructure (AMI), Li et al. propose a new wireless communication scheme. The measurements are transmitted only when there is a significant change in the power consumption to improve the spectrum efficiency. And the artificial spoofing packets are sent to pre-vent the attackers from analyzing user behaviors by monitoring communication traffic. A lightweight message authentication scheme is proposed by Fouda et al . The Diffie-Hellman exchange protocol is applied to achieve mutual authentication and establish the shared session key between the smart meters; the hash-based authentication is used to authenticate the subsequent messages. To secure the information aggregation in SG, Lu et al. proposed an efficient and privacy-preserving aggregation scheme, using a super -increasing sequence to structure multi-dimensional data and encrypt the structured data by the homomorphic Paillier cryptosystem technique [11].

Li and Xiong proposed a sign encryption scheme to provide secure communication between sensor nodes and the Internet host considering the wireless sensor network as a part of the Internet of things [12].

The privacy-preserving aggregation scheme allows one to compute over the encrypted data without the decryption key, to be specific, each smart meter encrypts the usage data in a way such that the energy supplier can decrypt their aggregation with the corresponding key, but no one can decrypt the individual usage data without the key owned by each smart meter. The promising techniques include homomorphic encryption [13] and secret sharing. Recently, a virtual ring architecture and tree structure are proposed to hide a single meter's usage data and collection time, respectively, in which the electric consumption information of a certain region is sent to the power management center instead of the usage data of a single smart meter.

To meet the requirements of communication latency and large volume of messages, a secure communication framework for smart grid was proposed in [14], in which the session keys are shared between smart meters and NG with the Diffie-Hellman (DH) key agreement protocol. In [15], a key management scheme is proposed using symmetric key and elliptic curve public key techniques to resist the man-in-the-middle attack and the replay attack.

In order to monitor the power grid more accurately in real time, an authenticated communication (AC) scheme was presented to achieve replay attack detection and message authentication. AC guarantees that each meter's information is real-timely collected and securely transmitted to the management center. However, the storage cost in the AC scheme cannot be neglected. To be specific, we assume that every 15 minutes a smart meter collects the electricity consumption reports, i.e., each day 96 reports need to be sent to the NG by the smart meter. In order to securely transmit these 96 reports, the AC scheme requires that the smart meter construct a 7-level Merkle hash tree (MHT) with 128 leaf nodes, which is used to authenticate the message sender with the corresponding authentication path information (API). Although only 96 APIs are to be appended with the encrypted form of 96 electricity usage reports, all the 128 APIs are stored in the smart meter including the remaining 32 APIs for the urgent need. Since each API consists of 7 outputs of a 128-bit cryptographic secure hash function, the storage cost of a smart meter in each day is $128 \cdot 7 \cdot 128$ bits = 14 KB. Moreover, if the smart meter collects the usage data every 5 minutes to get more accurate real-time electricity consumption report, the storage cost of a smart meter in each day is $512 \cdot 9 \cdot 128$ bits = 72 KB. Due to the fact that the smart meters own limited storage resources, such as the 8 KB RAM and 120 KB Flash memory set in [16], it is unacceptable to put so much storage resource on the APIs. Furthermore, AC cannot achieve the two-way authenticated communication since the hash of API is one-way.

III. AUTHENTICATION

Authentication is the act of confirming the truth of an attribute of a single piece of data claimed true by an entity. In contrast with identification, which refers to the act of stating or otherwise indicating a claim purportedly attesting to a person or thing's identity, authentication is the process of actually confirming that identity. It might involve confirming the identity of a person by validating their identity documents, verifying the authenticity of a website with a digital certificate, determining the age of an artifact by carbon dating, or ensuring that a product is what its packaging and labelling claim to be. In other words, authentication often involves verifying the validity of at least one form of identification.

In this study, authentication method and access control method for privacy protection are proposed so that remote user can securely access HAN and perform the work in home network based smart grid environment.

The privacy subgroup within CSWG (cyber security working group) of NIST divides the privacy largely into 4 categories that are privacy of personal information, privacy of person, privacy of personal behavioural, and privacy of personal communications. Among them, privacy of personal information refers to the rights to control and access the personal information which enables the identification of certain individual and others. Privacy of person is a right to control the integrity of user's body and it includes the matters that are physically necessary. Privacy of personal behaviour includes the right to maintain the fact of certain individual behaviour as confidential to others. Then, privacy of personal communications refers to the right for communication without censorship such as unjust monitoring. For the privacy within smart grid, all of the above 4 aspects should be considered. In order to achieve this, authentication method that can control the service access of remote user and encryption process for important data is necessary. This study provides the privacy within smart grid through secure access service through authentication process performed for user who accesses the system.

IV. CONCLUSION

Smart grid security tackles more difficulties compared to basic network security. This is due to the fact that it requires the power security, IT security, and telecommunication system security. Also, it requires reliability, defence on cyber-physical attack, and privacy protection, in addition to confidentiality, integrity, and availability security. Smart grid is intelligent electrical grid of the next generation that optimizes the energy efficiency by applying IT technology to the existing electrical grid so that supplier and consumer can exchange real-time information both ways. However, in such smart grid environment, there is a high possibility of various security threats including data disclosure and data piracy that exist in the two-way communication using smart devices such as smart meter and AMI.

Particularly, it is necessary to conduct studies on service access authentication process of user in regard to various attacks on privacy within smart grid. Living information, personal information, and payment information are gradually becoming the big data and there is increase in concern for the security of data.

Secure authentication method for the protection of user's privacy in home network based environment can also be done by using cryptography key generation technique. the smart meters only need to execute the bitwise exclusive-OR operation to encrypt collected usage data, and Lagrange interpolation formula is used to authenticate the sender; and cryptography symmetric/asymmetric key is used to encrypt or decrypt the transmitted messages that can be real-timely authenticated. The proposed authentication method protects security against replay attack, impersonation attack, entity mutual authentication, and others by performing the authentication process for user who accesses personal information created and transmitted from home network and AMI. In the future work, we will try to find more efficient solutions for security challenges and authentication techniques in smart grid.

REFERENCES

[1] Some Alternative Energy Names Are Ready to Power Up, (2010-4-10),http://finance.yahoo.com/news/Some-Alternative-Energy-Names-indie-988756486.html?x=0&.v=1

[2] The Smart Grid: An introduction, (2008),Association: Litos Strategic Communication,http://www.oe.energy.gov/DocumentsandMedia/DOE_SG_Book_Single_Pages.pdf

[3] A. Hamlyn, H. Cheung, T. Mander, L. Wang, C. Yang, and R. Cheung, "Network Security Management and Authentication of Actions for Smart Grids Operations", in Proc. IEEE Electrical Power Conf erence, Montreal, Que, Canada, Oct. 2007.

[4] G. N. Ericsson, "Cyber Security and Power System Communic ation-Essential Parts of a Smart Grid Infrastructure", IEEE Trans. Power Delivery, vol. 25, no. 3, pp. 1501-1507, Jul. 2010.

[5] K. Kursawe, G. Danezis, and M. Kohlweiss, "Privacy-friendly Aggregation for the Smart-grid", available online at http://research.microsoft.com/apps/pubs/?id=146092.

[6] M. Kgwadi and T. Kunz, "Securing RDS Broadcast Messages for Smart Grid Applications", in Proc. 6 TH Int. Wireless Commun. and Mobile Computing Conference, Caen, France, Jun. 2010.

[7] J. Kim and H. Choi, "An efficient and versatile key management pro-tocol for secure smart grid communications," in Proc. IEEE Wireless Commun. Netw. Conf. (WCNC), Apr. 1–4, 2012, pp. 1823–1828.

[8] S. Nguyen and C. Rong, “ZigBee security using identity-based cryp-tography autonomic and trusted computing,” in Proc. 4th Int. Conf. Autonomic Trusted Comput. (ATC’07), 2007, vol. 4610, Lecture Notes in Computer Science, pp. 3–12.

[9] W. Dapeng and Z. Chi, “Fault-tolerant and scalable key management for smart grid,” IEEE Trans. Smart Grid, vol. 2, pp. 375–381, 2011

[10] Y. Ye, Q. Yi, and H. Sharif, “A secure data aggregation and dispatch scheme for home area networks in smart grid,” in Proc. 2011 IEEE Global Telecommun. Conf., pp. 1–6.

[11] L. Rongxing, L. Xiaohui, L. Xu, L. Xiaodong, and S. Xuemin, “EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications,” IEEE Trans. Parallel Distrib. Syst., vol. 23, pp. 1621–1631, 2012.

[12] F. Li and P. Xiong, “Practical secure communication for integrating wireless sensor networks into the Internet of Things,” IEEE Sensors J., vol. 13, no. 10, pp. 3677–3684, Oct. 2013.

[13] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, “EPPA: An effi-cient and privacy-preserving aggregation scheme for secure smart grid communications,” IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 9, pp. 1621–1631, Sep. 2012.

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

[15] D. Wu and C. Zhou, “Fault-tolerant and scalable key management for smart grid,” IEEE Trans. Smart Grid, vol. 2, no. 2, pp. 375–381, Jun. 2011.

[16] H. Li, R. Lu, L. Zhou, B. Yang, and X. Shen, “An efficient Merkle-tree-based authentication scheme for smart grid,” IEEE Syst. J., vol. 8, no. 2, pp. 655–663, Jun. 2014.