ISSN: 2348 - 2117

International Journal of Engineering Technology and Computer Research (IJETCR)
Available Online at www.ijetcr.org
Volume 2; Issue 7; Page No. 15-20

Survey on Authentication Schemes in Smart Grid Network

A.A.Agarkar [1*], Dr. Himanshu Agarwal [2], Shilpa Shelke [3]

[1] PhD Scholar, Symbiosis International University, Pune, Maharashtra, India

*Assistant Professor, Department of IT, Sinhgad College of Engineering, Pune, Maharashtra, India

pratibha26@gmail.com

[2] Associate Professor, Symbiosis Institute of Technology, Pune, Maharashtra, India

himanshu.agrawal@sitpune.edu.in

[3] P.G. Student, Department of IT, Sinhgad College of Engineering, Pune, Maharashtra, India

shilpaajadhao@gmail.com

ABSTRACT

Smart grid is network consist of various devices and networks which provide two way communication between users and service providers. As it has various devices and networks there are chances of unauthorized access of the data due to which security violates in the smart grid also due to extensive use of wireless technologies security is one of the challenging issues in smart grid so there is need to provide security to smart grid network. This paper discusses about security requirements for smart grid and various security solutions which provide security to the smart grid network.

Key Words: Smart Grid, Security, Attacks, Authentication.

1. INTRODUCTION:

Smart Grid is the next-generation power system. It is very complex system consists of various devices also a digital system which provides efficient power supply to the various consumers from utility providers. Smart grid is a network which establish a two way communication between consumer and provider due to which it's very easy for customers to ask for their power demands or express their power requirements to the providers which help to reduce the electricity usage. The figure1 shows the hierarchical model of smart grid which consists of NAN, BAN, HAN networks.NAN (Neighborhood area network) is a network which covers the neighborhood area, which is a collection of BAN networks similarly, BAN covers the building area, which is a collection of various HAN networks and HAN network includes various home appliances like TV, AC, Washing machine, fridge etc.

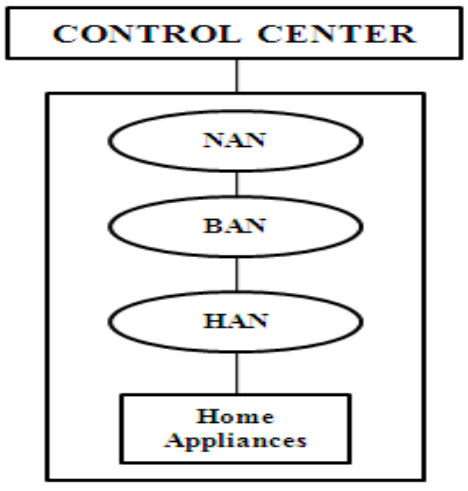

Figure 1: Hierarchical model of smart grid

2. SECURITY REQUIREMENTS IN SMART GRID

For secure and efficient communication it is important to understand the security requirements in smart grid. Wenye wang,Zhuo Lu [3] indicates the security requirements for smart grid network. Since smart grid network has various devices and networks so those devices and networks can be maliciously access due to this there are chances of the attacks like false data injection attack, DOS attack, replay attack, false data injection attack etc. therefore there is need to understand security requirements in smart grid. Following are the security requirements of smart grid.

2.1. Confidentiality

In Smart grid network the private data of various consumers like billing information and smart meter reading should be protected from the unauthorized users to provide confidentiality due to which only authorized person can have access to the confidential data or information.

2.2. Integrity

Smart grid consists of various networks into which information or data flows which can be unprotected from various malicious users or hackers, it may possible that the smart meter reading or information may be updated or changed by the hackers also using software's hackers can damage the functionality of smart grid, therefore some action should be taken against integrity violation so that the data should not be corrupted by the malicious users.

2.3. Availability

Power delivery is important in smart grid, if any disturbance or any threat will occur which effect the service provided by utility to the consumers also harms devices and networks so in that case there should be guarantee of proper service which does not affect the smart grid.

3. CONSTRAINTS IN SMART GRID

Smart grid has various devices like residential meters or smart meters, substations, and communication networks, for reliable and safe communication also to limit the traffic across these networks for faster communication we need to understand the limitations of smart grid following are the constraints of smart grid.

3.1. Communication Overhead

When the data is transmitted between various networks in the smart grid if the packet size is increased then there are chances of congestion due to which the traffic load will increase and hence overhead will increases for example in smart grid various customers can ask for their power requirements at the same time or electricity report for the same time.

3.2. Latency

Latency is the delay in transmitting the data. It can be increased in case of increasing the packet drops in wireless links in the smart grid networks. Smart grid has of millions of devices and networks if networks not able to communicate or there will be communication delay, latency will increase.

3.3. Low cost

For effective service there is need to be cost effective i.e. the storage requirements, memory and computational resources should be limited in the smart grid.

4. SECURITY ATTACKS IN SMART GRID

As smart grid consists of wireless links the confidential data or information across the communication channel on smart grid network can be protected from the outside intruders from maliciously accessing the data which harms the privacy as well as violates the security of the network so attack prevention is necessary in smart grid for secure communication. Xu Li.et.al [1] illustrates the various attacks related to smart grid which affect the security of SG. Following are security attacks in smart grid.

4.1. DOS attack

This attack degrades the performance of smart grid network. Due to this attack there will be delay in the communication in smart grid network. In this type of attack attacker will send various requests to target system due to which target system is overloaded and not able to perform properly which affects the performance of the system. The purpose of this attack is to affect the availability of the smart grid network. Also this attack will send fake request to the network for example wrong price information can affect the power demand.

4.2. Replay attack

In this attack data transmission is frequently repeated by the attacker for this first he understands the sequence of message then attack the system. In replay attack attackers will picks data from the smart grid network and send it repeatedly, in this attack attacker will picks and understands the transmitted data between the smart grid devices and use it repeatedly. In [5] authors proposed scheme which can protect smart grid from replay attack.

4.3. False data injection attack

In this attack the attacker can corrupt the network or system by injecting or modifying the original data. In [9] authors proposed a scheme which is protected against false data injection attack. In this attack original data will change and corrupts the integrity of the network, in smart grid network it is possible that the attacker can copy smart meter reading and can modify it using some malicious software's and hence the originality of data is

damaged by injecting the attackers own data which violates integrity.

4.4. Man-in-the-middle attack

It is a form of eavesdropping in which the attacker makes separate connections with the target systems and replays messages. Erman ayday et.al [7] proposed a scheme which is resilient against man-in-the-middle attack for smart grid network. In this attack attacker makes believe to the target systems that they are having communication with each other but actually attacker is handling the communication between them.

5. AUTHENTICATION SCHEMES IN SMART GRID

Various solutions are introduced for providing the integrity and confidentiality. But there is still a scope for research in authentication for smart grid network. As the electricity data collected from various devices are personal, it should have authenticated access. Various authentication schemes are available for wireless networks but they are not directly applicable to smart grid network because of the constraints. This section gives details of various authentication schemes designed for smart grid network.

Encryption is the cryptographic technique for secure communication; in smart grid for secure and effective communication between the various networks it should have some cryptographic schemes for better security and reliable operations. Encryption techniques help to protect the private data or information from unauthorized access and hence help to achieve security. Following are some security solutions in smart grid.

5.1. Symmetric Key Cryptography

Symmetric key uses same key for encryption and decryption thus it requires less computations also it has better energy efficiency than asymmetric key cryptography for example AES(Advanced encryption standard) ,DES (Data encryption standard) are Symmetric key cryptographic algorithms which are faster than the asymmetric key cryptographic algorithms. In [6] authors use authentication mechanism for smart grid security using symmetric key cryptography. Following figure shows Symmetric Key Cryptography technique.

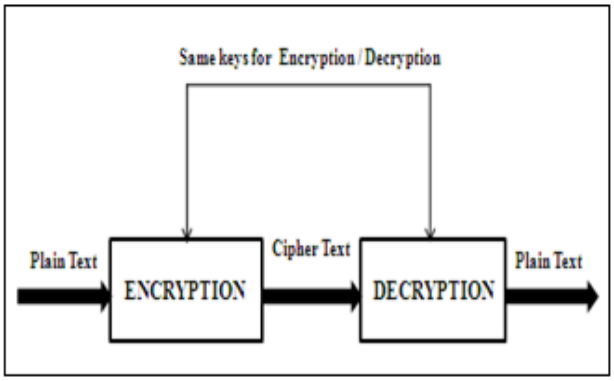

Figure 2: Symmetric Key Cryptography technique

5.2. Public Key Cryptography (PKI)

PKI or Asymmetric key cryptography uses two keys one for encryption and another is for decryption (e.g.RSA).In [2] author suggest that PKI is efficient for smart grid networks. In PKI public keys are managed by certificate authorities and registration authorities due to whom keys are more secure. This technique requires more computations than symmetric key cryptography due to which there is problem in fast authentication since two keys needs to manage for large networks. Following figure shows Public Key Cryptography technique.

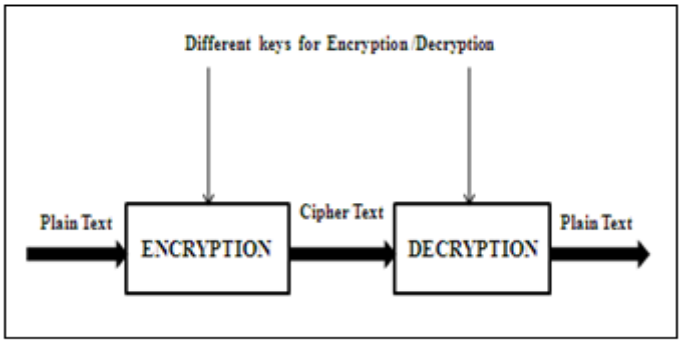

Figure 3: Public Key Cryptography technique

5.3. Identity Based Cryptography (IBC)

Identity based cryptography is public key encryption technique. The mechanism proposed in [4] is based on identity based cryptography. IBC has Private Key generator (PKG) which generates individual's private key. In this technique public key can be calculated from identity. Here the sender doesn't hold the recipient's public key prior to sending the message, because sender will calculate key. Following figure shows Identity based cryptography technique.

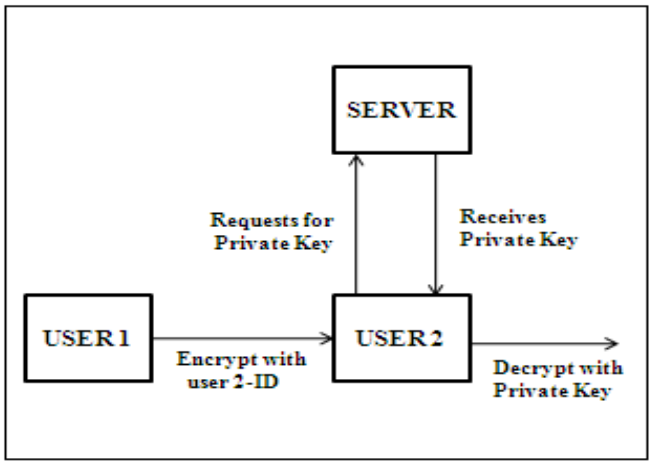

Figure 3: Identity based Cryptography technique

6. SURVEY OF VARIOUS AUTHENTICATION SCHEMES TO PROVIDE SECURITY TO SMART GRID

Table1: Survey of authentication schemes using Symmetric key cryptography technique

Symmetric Key Cryptography					
SN	**HANDLING ISSUE**	**ATTACK**	**METHOD**	**ADVANTAGES**	**DISADVANTAGES**
1	Framework with security and reliability[6]	Man-in-middle, replay attacks.	Uses Diffie-Hellman protocol .The Communication management use AES algorithm for message encryption and decryption process.	This scheme Provide Security and reliability. Authentication will be secure	Use of symmetric keys is vulnerable. If number of nodes increases then there will be problem for managing large number of keys.
2	Three secure and intuitive authentication schemes for the HAN part of smart grid network[7]	Man-in-middle attack.	Uses Symmetric key scheme.	Low computation and communication overhead. Intuitive and low cost device mechanism.	Uses Symmetric keys i.e. single key use for encryption and decryption it breaks the security
3	Authentication Scheme for the Smart Grid[9]	Message injection attack. Replay attack.	Follows symmetric cryptography Algorithm scheme and technique of Merkle-tree.	Computational cost and complexity is low.	Using Symmetric keys for entire smart grid is not scalable due to the large number of devices and nodes.

Table2: Survey of authentication schemes using PKI and IBC cryptography technique

Public Key Cryptography					
SN	**HANDLING ISSUE**	**ATTACK**	**METHOD**	**ADVANTAGES**	**DISADVANTAGES**
1	A Key management mechanism[5]	Man-in-middle, replay attacks.	Key management scheme which uses symmetric key technique and elliptic curve technique.	It is secure, Scalable, also fault tolerant, and efficient.	Using PKI will essentially increase compilation for smart grid because their protocol needs at least two different kinds of servers for PKI and the trusted anchor respectively.
2	One time signature scheme[10]	Replay attack	Uses HSLV(Heavy signing light verification) with LSHV(light signing heavy verification) and obtain the scheme turntable signing and verification(TSV),Design a multicast authentication protocol	TSV generates much smaller signature and generates much lower storage requirement. Reduce storage overhead	The security of the proposed scheme is based on PKI (public key Infrastructure). PKI has drawbacks related to certificates which will be big concern.
Identity Based Cryptography					
1	Authentication Scheme and Key Management protocol for Home Area Network[4]	DOS -attack, Man-in-middle, replay attacks.	Public/Private key-pair technique based on identity based cryptographic technique.	Reduce overhead	It uses private key generator which manages the private key so privacy is major concern.

7. CONCLUSION:

Smart grid is the future of electricity grid. It is already implemented in European countries. Security in the Smart Grid is a new topic of research. Security is under development in the Smart Grid which must be taken into account .Solutions available for Security at present are not directly applicable to smart grid because of basic constraints of Smart grid. The Smart Grid requires effective security solutions designed specifically for different network applications.

REFERENCES:

1. Xu Li, Inria Lille,Xiaohui Liang, Rongxing Lu, and Xuemin (Sherman) Shen, Xiaodong Lin, Haojin Zhu,"Securing Smart Grid: Cyber Attacks, Countermeasures, and Challenges" IEEE Communication Magazine, pp.38-45, August 2012.
2. Anthony R. Metke and Randy L. Ekl "Security Technology for Smart Grid Networks," IEEE Transaction on Smart Grid, vol. no.1, pp.99-107, June 2010.
3. Wenye wang, Zhuo Lu,"Cyber security in the smart Grid: Survey and challenges", pp.1344- 1371, 2013.
4. Hasen Nicanfar,Paria Jokar,Victor C.M.Leung,"Efficient Authentication and Key Management for the Home Area Network" IEEE Trans. pp.878-882, 2012
5. Dapeng Wu and Chi Zhou, "Fault-Tolerant and Scalable Key Management for Smart Grid," IEEE

Transaction on Smart Grid, vol. 2, no. 2, June 2011, pp. 375–81

6. Mostafa M. Fouda ,Zubair Md.Fadlullah,Nei Kato,Rongxing Lu and Xueimin(Sherman)Shen,"A Light-Weight Message Authentication Scheme for Smart Grid Communications," IEEE Transaction on Smart Grid, vol. 2, no. 4, pp. 675–85, December 2011.
7. Erman Ayday,Sridhar Rajagopal, "Secure, Intuitive and Low-Cost Device Authentication for Smart Grid Networks"IEEE , 2011.
8. Isaac Ghansah,"Research and Development Issues for Cyber Security in the Smart Grid", California State University Sacramento, May 2014.
9. Hongwei Li, Rongxing Lu, Liang Zhou,Bo Yang and Xuemin (Sherman) Shen," An Efficient Merkle-Tree-Based Authentication Scheme for Smart Grid", IEEE system Journal, pp1-9, 2013.
10. Qinghua Li and Guohong Cao,"Multicast Authentication in the Smart Grid with One-Time Signature" IEEE
    Transaction on Smart Grid, vol. 2, no. 4, pp. 686–696, December 2011.