Journal of Advances in Science and Technology
Vol. 12, Issue No. 25, (Special Issue) December-2016, ISSN 2230-9659

Encryption and Authentication in Smart Grid Communication Security

Mr. Arvind P. Kadam[1]*, Dr. S. G. Ankaliki[2]

[1]Research Scholar- EEE, SDMCET, Dharwad

[2]Professor, Dept. Of EEE, SDMCET, Dharwad

Abstract – Smart Grid technology can increase the efficiency of energy management. Conventional power grid systems are being replaced with new advanced Smart Grid systems. These Smart Grid systems rely on current Information and Communication Technology (ICT) to provide advanced services to both users and service providers. Due to increased use of ICT especially wireless communication makes Smart Grid system more vulnerable to physical layer attack such as Eavesdropping, Jamming, Restricting Access, Injecting and internal attacks. In this paper we are proposed encryption techniques for device authentication to protect from physical attacks. Device authentication is first step of data communication. We propose an efficient encryption key management for end to end security between two grids and algorithm steps secures the communication between the grids and maintains integrity of data.

Keywords- Smart Grid, ICT, Physical Attack, Encryption, Authentication

----------♦----------

1. INTRODUCTION

Smart Grid is an electricity supply network which is digital communication technology. It uses a two way digital communication. It establishes communication path between supplier and consumers. This allows the Smart Grid system to monitor analysis and control the efficiency, cost, reliability and sustainability of the production and distribution of electricity.

Conventional power grid employs dedicated power devices. There is only one access point to the grid management system. Power devices is traditionally located at protected place and controlled through protocols via dedicated wired communication links.

Next generation power grid depends on digital technology. It is vulnerable to different types of security issues. In recent time different research have been conducted to explore and solve the security issues and challenges of Smart Grid network. The infrastructure of Smart Grid consists of management and protection system.

The management system provides advanced management and control services. They are improving energy efficiency, demand profile, utility and cost based on the infrastructure. Digital communication technology introduces wireless technology. It introduces additional vulnerability. This deteriorates network performance and threatens desirable operations of the Smart Grid. It can steal private and confidential information. Proper detection solutions must be carried out before deploying wireless technologies in the Smart Grid. Wireless technology is more vulnerable to physical attacks. It can inject bogus signals into wireless medium which prevents legitimate users in the radio range from receiving wireless signals correctly. In this paper we investigate the

- Wireless technology deployed in Smart Grid communication.
- Physical layer attacks
- Device authentication to protect from attacks.
- Efficient encryption key management for security between two grids.

2. COMMUNICATION NETWORK ARCHITECTURE IN THE SMART GRID

According to NIST[1] conceptual model , the Smart Grid consists of seven logical domains: Bulk Generation, Transmission, Distribution, Customer Markets, Source Provider and Operations.

The two way power and information flows as shown in Fig.1[2]. The backbone network is established for inter domain communication. It consists of infrastructure nodes, which can be either gateways for local area networks or high bandwidth routers to forward messages across a variety of domains I the Smart Grid. In the backbone network conventional

wire line communication technologies such as fiber optic can be used to achieve high speed data. A LAN is used for intra domain communication.

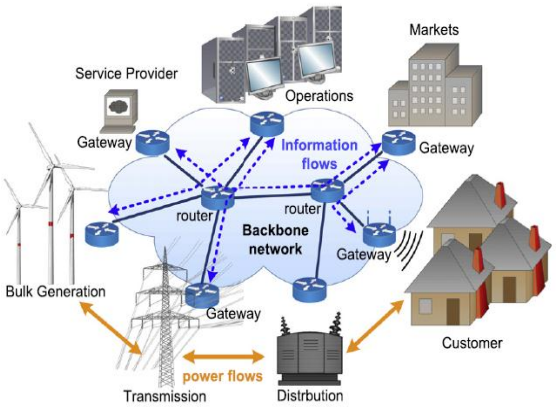

Fig. 1 The network architecture in the Smart Grid: Backbone and local-area network [2]

A local area network consists of ad hoc nodes which are meters, sensors or IED's (Intelligent Electronic Devices). They are equipped with limit bandwidth and computational ability for certain monitoring and protection purposes. These ad hoc nodes are using wireless technologies. There are advantages of using wireless technologies including untethered access to utility information, mobility, reduced cost, low complexity.

3. UNDERSTANDING WIRELESS COMMUNICATION

In order to identify physical layer vulnerability and devise optimal solutions, it is fundamental to understand the principle of wireless communication. We are taking a brief overview of the two lowest networking layers, the data link and PHY layers, which are directly associated with PHY layer attacks. In particular, we review a MAC protocol used in IEEE 802.11 and 802.15 families, and discuss the implication of power strength in signal propagation. This implies that an application prepares data to send and a network layer determines the location of the communication partner in the network. Once receiving the packet from the upper layer, the MAC protocol determines when to start transmitting packet and then the PHY layer actually emits analog signals representing the packet over the wireless.

Medium Access Control- All nodes in the network share the wireless medium (or channel), MAC protocols have a scheduling algorithm that controls nodes' resource access. The IEEE defines specifications of carrier sense multiple access with collision avoidance (CSMA/CA) protocols for 802.11 and 802.15 families. In CSMA/CA, when a node is ready to transmit a packet, it listens to a wireless channel — *carrier sensing* — to see whether another node is transmitting data on the channel. If the channel is "idle," the node is allowed to transmit the packet. Otherwise, the node defers its transmission until the existing transmission stops and a further random period of time — random backoff. After the backoff, it retries packet transmission by resuming carrier sensing. After several trials more than a predefined threshold, the node gives up transmission and notifies communication failure to the upper layer. In any case, postponed transmission increases network latency, which can lead to violation of application requirements.

Physical Layer -Once the node is allowed to transmit data, the PHY layer modulates the digital representation of the packet to (analog) signals, each of which consists of a sequence of discrete complex symbols in the form of sinusoid (or sine wave). Each symbol can represent or convey one or several bits of data according to the modulation scheme used. Suppose that *n*th complex symbol transmitted from a sender is denoted as $x[n]$. When a receiver receives the signal, say $y[n]$ and its interpretation is same to $x[n]$, the transmission is said to be successful. However, due to unexpected wireless environment, the transmitted signal is often blocked or distorted over the air. In communications theory, the receiver sensitivity and the standard signal- to-interference-plus-noise ratio (SINR) model are used to determine the ability of successful data recovery. That is, a signal is transmitted with standardized power level at the sender and its strength attenuates as travelling. When the signal arrives at the receiver and its remaining power level is greater than a threshold, recover the signal. If the signal is too weak, then the receiver cannot derive correct bit information from it. Noise and interferences also affect the capability of signal reception. When a signal propagates, it is affected by unexpected radios. They alter the original form of the signal. The degree of distortion is computed as the ratio of the received signal power to the combined power of noise and interference at the receiver, i.e., SINR. The SINR value is used to compute the bit error rate (BER): a large SINR implies a stronger signal and thus few bit errors. Then, the BER is used to calculate the packet error rate (PER). The receiver can decode the transmitted packet if the SINR value is above a given threshold. Otherwise, it handles the signal as an error.

4. PHYSICAL (PHY) LAYER ATTACKS

A physical layer attack [3] is defined as malicious behavior disturbing legitimate communication on a wireless network. It disrupts the wireless medium by simply injecting false messages into the network and disables all data transmissions within radio range. In this sense, the PHY attack is regarded as a wireless

version of a Denial of Service (DoS) attack. We classify the PHY attacks into four groups according to objectives and behaviors: eavesdropping, jamming, restricting access, and injecting.

a. Eavesdropping

Wireless signal propagates over open space, any network node within radio range is able to capture the signal. Moreover, as legitimate nodes follow communication standards, the neighboring nodes can obtain meaningful information from the captured signal. This openness and these standards are misused. That is, an unauthorized node eavesdrops on data transmission and accesses credential information. By doing so, the eavesdropping attack violates the confidentiality requirement. The attack is not easily detected because the adversary does not expose its activity..

b. Jamming

Jamming attack fills the wireless medium with noise signals. This affects a legitimate node in two ways. First, when the node performs the carrier sense before transmitting a packet, the channel is always sensed "busy." This defers its transmission, and the node eventually gives up communication. Second, the node may fail to receive packets. Suppose it is receiving packets from a legitimate communication partner. The noise signal can distort the data signal and the node cannot recover messages out of the damaged packets. The goal of jamming is to deteriorate availability.

Proactive jamming: A jammer can emit noise signals continuously to completely block a wireless channel. The proactive jammer is easily detected due to its suspicious behavior.

Reactive Jamming: the jammer listens to the radio channel first and launches a jamming attack only when sensing signals on the channel. In this situation, the legitimate node cannot clearly distinguish whether its packet error results from attacks or normal collision.

c. Restricting Access

This type of attack tries to disrupt the MAC protocol by simply preventing nodes from initiating legitimate MAC operations or causing packet collisions. This is conceptually similar to reactive jamming; that is, a jammer starts an attack only when necessary to block a wireless channel. The attacker sets its own back off timer very short so that it occupies the wireless channel first all the time. Other nodes will sense the channel busy and postpone their transmission. This portion is similar to the proactive jamming. In this way, the attack disturbs legitimate communication.

d. Injecting

An injecting attack inserts *formatted messages* into the wireless network, whereas the two previous attacks can use bogus signals. Impersonation and replay attacks fall into this category. The adversary impersonates either a legitimate sender or a receiver to obtain unauthorized access to a wireless network. A typical impersonation is device cloning. In terms of the PHY layer, the cloning is done via MAC address spoofing. The unauthorized access can cause a secondary vulnerability such as de-authorization

5. RELATED RESEARCH WORK

According to recent work, key management mechanisms for securing the Smart Grid communication based on the Public Key Cryptography (PKC). We reviewed the previous work approaches to encryption to secure communication.

[4]Three task forces have been created for IEEE P2030 Smart Grid Std. to implement Smart Grid. One of the task force is pertaining to cyber security which describes system and communication protection policies and procedures to combat cyber attacks against Smart Grid.

Hamlyn et.al.[5] proposed a utility computer network security management and authentication for actions and commands request in Smart Grid operation

Their work focused on securing host area electric power systems and electric circuits.

Metake A R et.al.[6] proposed power system communication and cyber security issues are considered to be crucial components of Smart Grid. Integrated SCADA/ energy management systems and administrative office Information Technology (IT) environments may lead to evolving security threats.

Ekl RL et.al.[7] Smart Grid deployments must satisfy strict security requirements. Strong authentication is considered to be requisite for all users and devices of the Smart Grid.

Fouda M M et.al.[8] proposes to the address the potential security issues and light weight and secure message authentication mechanism. Detailed security analysis to satisfy the desirable security requirements.

Nikanfar et.al.[9] proposed a kay management protocol for the Smart Grid password authentication and identity based cryptography.

Hayden k h So et.al [10] proposes the use of an identity based signcryption system to provide a zero configuration encryption and authentication solution for end to end secure communications.

Bekara C et.al.[11] proposed an identity based authentication protocol for the AMI. They assume the existence of 't' trusted entities PKGi, i = 1,….t in the Smart Grid.

They utilize a variant of identity based cryptography. Their scheme has the certificate management problem as each PKGi must issue cross domain certificates to each remaining PKGj. Two entities belonging to different keying domains must each verify the certificate of the other for inter-domain communication.

Xia et.al.[12] proposed a key distribution protocol and demonstrate it is secure and efficient for Smart Grid network. By using Kerberos to Smart Grid may lose authentication from the third party due to power outages. Proposed protocol is secure against interpersonation attack, replay attack, man in the middle attack.

In order to address the drawbacks of previous approach, we propose a new encryption key management scheme based on RSA and AES 256 encryption algorithm.

6. AUTHENTICATION

The reliability and security of smart grid are subject to the integrity and authenticity of devices and data traffic in the grid. Device authentication is normally the first step of a data communication session, and its result is often a shared session key for encrypting and authenticating subsequent data packets and ensuring data integrity[13]. Because of the delay-sensitive and traffic- intensive nature of smart grid communication, an authentication scheme should involve minimal message exchange between grid devices. Conventional encryption is Public key encryption and it uses in message authentication and key distribution. The security any encryption scheme depends on length of the key and the computational work involved in breaking cipher.

Requirements for public key Cryptography

Diffie and Hellman postulated this system.

- It is computationally easy to generate a pair (Public key Pub, Private key PRb)
- It is computationally easy for a sender A, knowing the public key and the message to be encrypted M, to generate the corresponding ciphertext: C = E(Pub, M)
- It is computationally easy for the receiver B to decrypt the resulting ciphertext using the private key to recover the original message.

M = D(PRb, C) = D[PRb, E(PUb, M)]

- It is computationally infeasible for an opponent, knowing the public key PUb to determine the private key PRb.
- It is computationally infeasible for an opponent, knowing the public key PUb and a ciphertext C to recover the original message M.

Public Key Cryptography Algorithms

The most widely used public key algorithm is RSA.

The RSA Public –Key Encryption Algorithm

The RSA cryptosystem is a public key cryptosystem that offers both encryption and authentication. One of the first public key schemes was developed by Ronald Rivest, Adi Shamir and Leonard Adleman at MIT.

Encryption

Suppose Alice wants to send the message m to Bob in such a way that Bob is assured the message is both authentic, has not been tampered with and from Alice. Alice creates a authentication C by exponentiating: $C = M^e \mod n$ where e and n are Alice's private key. She sends M and C to Bob. To verify the authentication, Bob exponentiates and checks that the message M is recovered: $M= C^d \mod n$ where d and n are Alice public key.

Thus encryption and authentication take place without any sharing of private keys, each person uses only another's public key or their own private key. Anyone can send an encrypted message or verify a signed message but only someone in possession of the correct private key can decrypt a message.

RSA is a block cipher in which the plaintext and ciphertext are integers between 0 and n-1 for some n.

Encryption and decryption are of the following form period for some plaintext block M and ciphertext block C:

$$\mathbf{C = M^e \mod n}$$

$$\mathbf{M = C^d \mod n = (M^e)^d \mod n = M^{ed} \mod n}$$

Both sender and receiver must know the values of n and e and only the receiver knows the value of d. This is public key encryption algorithm with a public key of KU = {e, n } and private key of KR = { d, n }

The following requirements must be met for this algorithm

- It is possible to find values of e, d , n such that M^{ed} mod n = M for all M < n
- It is relatively easy to calculate M^e and C^d for all values of M < n
- It is infeasible to determine d given e and n

RSA algorithm involves three steps**:** key generation, encryption and decryption.

Key Generation

RSA involves a public key and private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can be decrypted in a reasonable amount of time using the private key. The keys for the RSA algorithm are generated the following way:

Choose two different prime numbers p and q- For security purpose, the integer p and q should be chosen at random and should be similar bit length.

Compute n= pq - n is used as the modulus for both the public and private keys.

Compute Φ(n) = Φ(p) Φ(q) = (p-1) (q-1) = n-(p + q-1), where Φ is Euler's totient Function

Choose an integer e such that 1< e < Φ(n) and gcd (e,Φ(n)) = 1 e is released as the public key exponent.

Determine d as d = e^{-1} (mod Φ(n)) i.e. d is multicative inverse of e (modulo Φ(n)).

D is kept as private key exponent.

Encryption

Alice transmits her public key (n, e) to Bob and keeps private key secret. Bob then wishes to send message M to Alice.

Decryption

Alice can recover M from C by using private key exponent d via computing.

7. PROPOSED ENCRYPTION SCHEME

We are proposing encryption scheme to communicate between the two Grids. Message is send by the Grid 1 and the same secured message is recovered at the Grid 2.

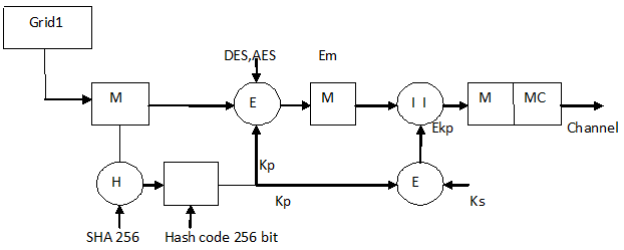

Fig.2 Message Transmission from Grid 1

In Fig.2 Grid 1 has sent one secrete message M to Grid 2. The message M must be secure while travelling through communication channel. We are recommending here the encryption technique AES-256 algorithm. The key for AES- 256 algorithm is generated through hashing function called SHA-256. The message digest generated from SHA-256 function. It is passed as key Kp for AES 256 algorithm. The message M is encrypted using AES 256 algorithm. The encrypted message is Em. The encryption key Kp is again encrypted using shared key Ks and Ekp is generated. This Ekp is attached with encrypted message Em. Ekp and encrypted message Em is travelled through communication channel.

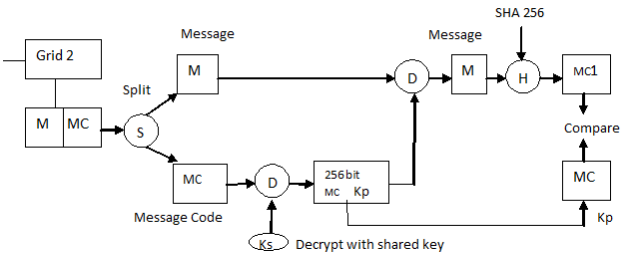

Fig.3 Message Reception at Grid 2

Fig.3 represents the recovery of the message sent by the Grid 1. Grid 2 receives the encrypted message Em and encrypted key Ekp. These meaasge Em and Key Ekp are separated. Encrypted key Ekp is first decrypted using shared key Ks. Then this key is used to decrypt the message M received from Grid1. Now we have to check the correct message is received or not. Message digest of 256 bit is calculated from message M and compare with key Kp. If match found then correct message is received at Grid 2 from Grid 1.

CONCLUSION

In this paper we have investigated the Wireless communication deployed in Smart Grid communication, Physical layer attacks. We have implemented the RSA algorithm for device authentication to protect from attacks. We have proposed efficient encryption key management scheme using AES 256 algorithm for secure communication between two grids.

Our message is highly secured due to this proposed encryption scheme.

REFERENCES

Office of national Co-ordinator for Smart Grid interoperability NIST framework and Roadmaps for Smart Grid interoperability Std. release 1.0 NIST special publication 1108(2010) 1-145

Wenye Wang, Zhuo Lu 'Cyber Security in the Smart Grid: Survey and Challenges' ELSEVIER 2013, Computer Networks

Eun-Kyu, M.Gerla ' Physical Layer Security in wireless Smart Grid' 2012, IEEE Communication Magazine

sites.google.com/site/ieeep2030/sqenergysources/cybersecurity

Hamlyn 'Network security management and authentication of actions for Smart Grid operations'

Metke A R 'Cyber Security Technology'

Metake, Ekl R L ' Security Technology for Smart Grid Networks' 2010 IEEE Trans. On SG June 2010

Fouda M M , Zubair M F ' Towards a light weight message authentication mechanism tailored for Smart Grid Communications' 2011 IEEE International workshop on security in computers, networking and communications.

Nikanfar H 'A tailored authentication and key management for Smart Grid' IEEE System Journal

Hayden K H Sammy 'Zero configuration Identity based signcryption scheme for Smart Grid

Bekara C 'A privacy preserving and secure authentication protocol for the advanced metering infrastructure with non-rudiation service.' Proceedings of energy 2012.

Xia, Y Wang 'Secure key Distribution for the Smart Grid' IEEE Trans. On Smart Grid SEPT 2012.

Xu Li, X Liang, X Lin ' Securing Smart Grid: Cyber Attacks, Countermeasures and challenges

Corresponding Author

Mr. Arvind P. Kadam*

Research Scholar- EEE**,** SDMCET, Dharwad

E-Mail – karvind1972@gmail.com