Toward Design a Hybrid Crypto-Scheme for Smart Grids

Raja Mouachi, Fatima Gharnati
Cadi Ayyad University
Morocco
mouachiraja@gmail.com
garnati@ua.ma

Mustaph Raoufi
Cadi Ayyad University
Mozambique
raofi@ua.ma

ABSTRACT: *Smart grid is a term referring to the next generation power grid in which the electricity distribution and management is upgraded by incorporating advanced two-way communications and pervasive computing capabilities for improved control, efficiency, reliability and safety. The smart grid is a network of networks, including a variety of sub-systems. One subsystem which is at the core of smart grid systems is the Supervisory Control And Data Acquisition (SCADA) solution. The objective of the paper is to develop a method uses a hybrid of the advanced Encryption Standard (AES) and the Elliptic Curve Cryptography (ECC) to Secure SCADA in Smart Grid. Because without a secure SCADA system it is impossible to deploy the intelligent smart grid systems.*

Keywords: Smart Grid, SCADA, Security Issues, Encryption Decryption, Hybrid Crypto-scheme

Received: 26 April 2017, Revised 28 May 2017, Accepted 7 June 2017

1. Introduction

The smart grid is envisioned as the next generation power grid that provides advanced electricity generation, distribution and management, utilizing the latest information and communication technologies to enable real-time load and control capabilities from the point of generation to the end user consumption point [1] Smart Grid was built when energy was relatively inexpensive. Infrastructures like electricity which is controlled by SCADA can play a big role on Smart Grids. The utilization of Supervisory Control and Data Acquisition (SCADA) systems facilities the management with remote access to real-time data and the channel to issue automated or operator-driven supervisory commands to remote station control devices, or field devices.

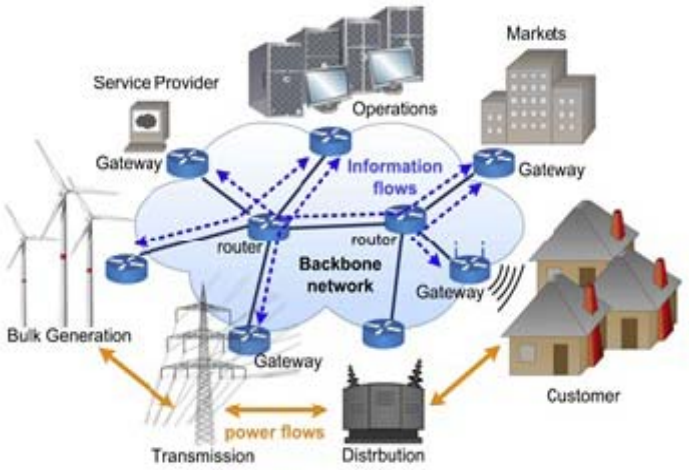

Figure 1. The network architecture in the Smart Grid: backbone and local-area networks

On the Next parts of this paper, we discuss Smart Grid and the integration of SCADA in this system. Advantages which can be attained using the SCADA in Smart Grid are also covered. Security concerns are being pointed. We also suggest a security solution for a Smart Grid using hybrid crypto-scheme.

2. Security Objectives In Smart Grid

The Smart Grid communication network is a mission critical network for information exchange in power infrastructures. It is essential to understand what are the security objectives before providing a comprehensive treatment of cyber security in the context of energy delivery and management to ensure secure and reliable operation. Here, we describe the security objectives for the Smart Grid.

• **Availability:** Accessing information in a timely in the smart grid. Loss of availability could affect the power delivery since access to authorized individuals might be denied. Attacks targeting the system availability are considered Denial of service attacks (DOS) which aim to disturb the data transfer in order to make the resources unavailable.

• **Integrity:** Preventing an unauthorized modification of information or system by illegitimate users. Loss of integrity in the smart grid might modify sensors values and products recipes which in turn can affect the power management.

• **Confidentiality:** Preventing unauthorized users from accessing information in order to protect personal privacy and safety. Smart grid networks carry information that varies in privacy and sensitivity levels; from consumption information all the way to consumer private information.

• **Authentication:** Validating the true identity of the communicating parties. Authentication of humans and machine is of high importance, and a weakness in it can lead to an attacker gaining access to private information, or an illegitimate devices making use of the smart grid resources.

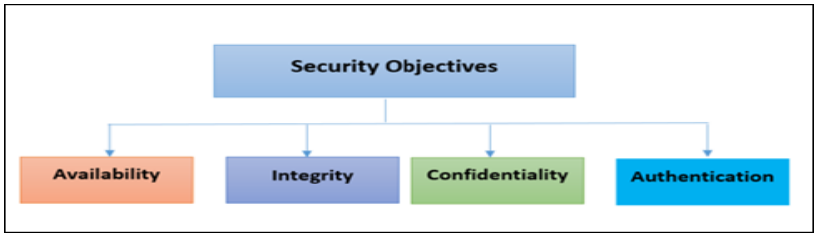

Figure 2. Four high-level security objectives for the Smart Grid

3. Smart Grid And SCADA

3.1 SCADA architecture

The utilization of SCADA systems facilities the management with remote access to real-time data and the channel to issue automated or operator-driven supervisory commands to remote station control devices, or field devices. SCADA is the underlying control system of Smart Grid. The basic architecture of SCADA system. It consists Of:

• **Human Machine Interface (HMI):** These are large components also called as SCADA Master Units, which serve as central processor and provide the Human interface to interact with the systems.

• **Remote Telemetry Units (RTU):** These are computerised units deployed in the specific fields. RTUs serve as collection point for collecting information and delivering the commands to the control relays.

• **Sensors:** These are the devices used for measurement of analog or digital value in the field level of SCADA systems.

• **Communication Network:** Refers to the communication equipment needed to transfer the data to and from different sites to the central station.

• **Intelligent Electronic Devices (IED):** An IED is a smart sensor/actuator containing the intelligence required to acquire data, communicate to other devices, and perform local processing and control. An IED could combine an analog input sensor, analog output, low-level control capabilities, a communication system, and program memory in one device. The use of IEDs in SCADA system allows for automatic control at the local level.

• **Data Historian:** The data historian is a centralized database for logging all process information within a SCADA. Information stored in this database can be accessed to support various analyses, from statistical process control to enterprise level planning.

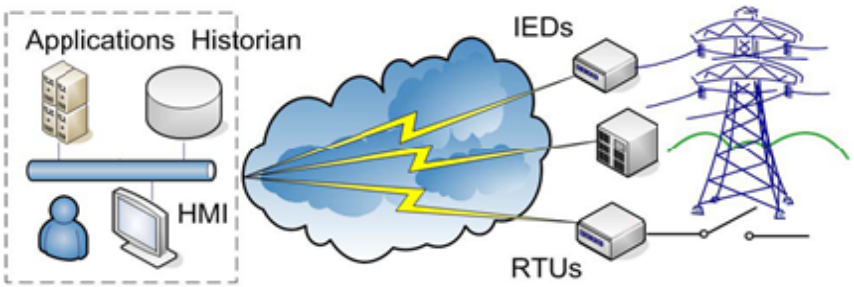

Figure 3. A simplified SCADA architecture

3.2 Advantages of SCADA in Smart Grid

• Self-healing anticipates and instantly responds to system problems in order to avoid or mitigate power outages and power quality problems.

• Empowers the consumer interconnects with energy management systems in smart buildings to enable customers to manage their energy use and reduce their energy costs.

• Accommodates a wide variety of generation options central and distributed, intermittent and dispatchable.

• The Tolerant of attack mitigates and stands resilient to physical and cyber attacks.

4. The Smart Grid And SCADA Security Concerns

The evolution and security issue escalation of the Smart Grid and SCADA due in large part to the advent of the internet and rise in terrorist threats. Additionally, the introduction of new protocols, LAN/WAN architectures, and new technologies such as encryption and information assurance applications on the shared network(s) raise new sets of security concerns. The increased

functionality of Smart Grid and the SCADA architecture leads to control systems that are escalating in complexity and have become time critical, embedded, fault tolerant, distributed, intelligent, large, open sourced, and heterogeneous, all which pose their own program vulnerabilities. Ranked high on the list of government concerns are threats against SCADA systems. Unfortunately, mostly due to the complexities involved and resources required, the threats are too often trivialized and most organizations are slow to implement enhanced security measures to combat these threats. Key requirement areas for addressing these threats are critical path protection, strong safety policies, procedures, knowledge management, and system development skills that place security architecture at the forefront of requirements. SCADA also creates a number of additional security issues since the electrical power network is a critical infrastructure. Without Internet connectivity, SCADA already contends with security issues, and additional methods of penetration via the internet make it more vulnerable.

5. The Hybrid Crypto-Scheme For Scada Communication In Smart Grid

There are two basic techniques for encrypting information: symmetric encryption (also called secret key encryption) and asymmetric encryption (also called public key encryption).

5.1 Asymmetric Encryption

Asymmetric cryptography employs a pair of keys, consisting of a public key and a private key. The advantage of asymmetric is in its functionality. It provides security in awide range of applications that cannot be solved using only symmetric techniques.

5.2 Symmetric Encryption

This method involved two parties who share a joint secret or key. This exclusive knowledge of the key enables private and secure communications between the two parties.

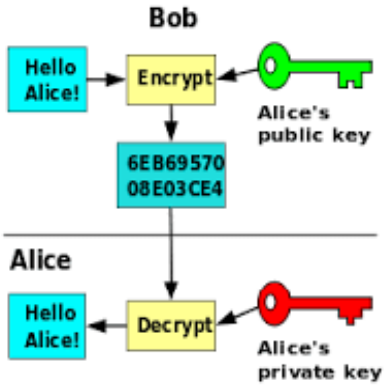

Figure 4. Asymmetric Encryption

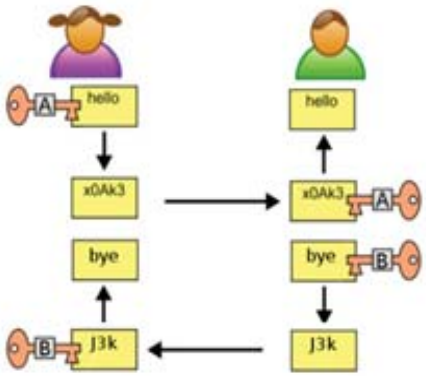

Figure 5. Symmetric Encryption

6. Methodologies

We have an array of symmetric [2] algorithms available such as AES and DES which provide a quick scrambling up of the data using a single key. Whereas asymmetric [2] algorithms such as RSA, Blowfish, ECC [3] etc. use 2 keys to do the same task but provide better security. Both having their equal share of advantages and disadvantages. In some instances, the best possible solution may be the complementary use of both symmetric and asymmetric encryption AES is chosen as the symmetric counter part because it provides the result faster and better than DES whereas ECC is chosen as the asymmetric key counterpart because it does the encryption by using less number of keys as compared to RSA and at a much faster pace [4] [5] [6].

6.1 Advanced Encryption Standard (A.E.S)

Advanced Encryption Standard (AES) is a symmetric-key cryptographic technique. It uses symmetric key concept. AES has a fixed block size of 128-bit and the key length must be 128, 192, or 256 bits. A 128-bit key thus gives a key space of 2128 keys. Number of rounds in AES is determined by the key size used in the process. Number of rounds will be 10, 12, 14 for key sizes of 128, 192, 256 bits respectively. First n-1 rounds contain four distinct transformations: Substitute Bytes, Shift Rows, Mix Columns, and Add Round Key. The final round contains only three transformations: Substitute Bytes, Shift Rows, and Add Round Key. AES offers a very high security and performance.

6.2 Elliptical Curve Cryptography

One of the most popular public-key cryptography approach is Elliptic curve cryptography (ECC). Neal Koblitz [7] and Victor Miller [8]proposed elliptic curves in 1985 to design public key cryptographic systems. Algebraic form of additive group is described by the group or set of solution along with their point at infinity O.

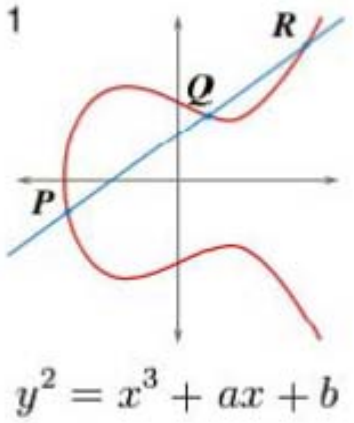

Figure 6. Simple Elliptical Curve

7. Ideas And Processes of Proposed Hybrid Scheme

The proposed approach consists of two processes, encryption process and decryption process. Both processes make use of AES and ECC. The reason we have selected these particular algorithms is discussed as:

• AES is not only a secure cipher but it offers a very high performance and makes better use of resources. Not a single successful brute-force attack on AES has been found till date, the only possible known attack against AES.

• The benefits of ECC are many: Linear scalability, small software footprint.

Figure 7 Shows the proposed methodology to be adopted for encrypting the data in SCADA for Smart Grid. The overall decryption process is as shown below: In this approach the elliptical curve cryptography is utilized to generate the ciphertext of the result which is provided by AES. The cipher text of the message and the cipher text of the key are then sent to the SCADA assets. The system is intended to provide security to a variety of data in Smart Grid specially in SCADA system. Such a hybrid model of encryption provides a much better level of security as compared to a single model applied individually.

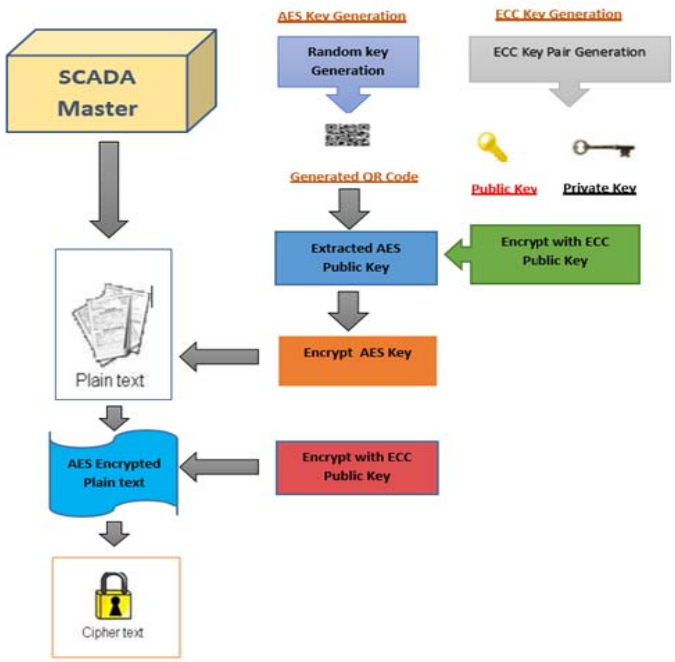

Figure 7. Encryption process using the hybrid crypto-scheme

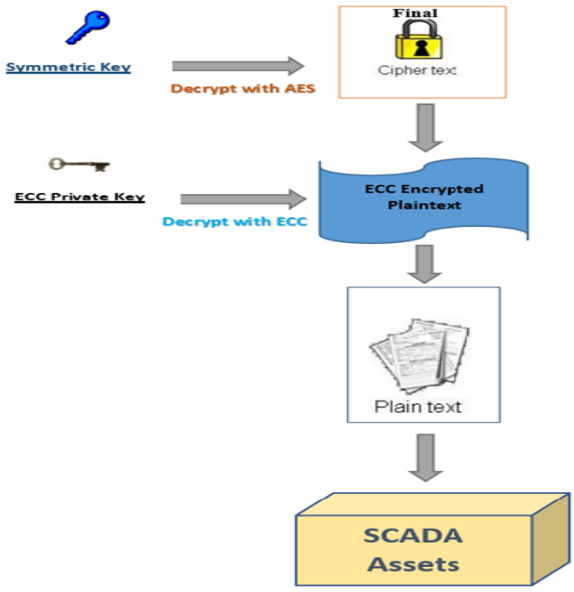

Figure 8. Decryption process using the hybrid crypto-scheme

8. Conclusion

Smart grids have real difficulty with data security, because they do not provide secure exchange of information in SCADA system. In this paper, we proposed a novel technique to provide security to a variety of data in Smart Grid specially in SCADA system. The proposed technique is secure, tough, and efficient due to the use of AES cipher, is having better key management due to the use of ECC technique.

References

[1] U.S. Department of Energy, [online] Available: www.oe.energy.gov.

[2] Jawahar, Thakur., Nagesh, Kumar., DES., AES., Blowfish. (2011). Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis, *International Journal of Emerging Technology and Advanced Engineering*, 1 (2) 6-12.

[3] Celestin, S. M., Muneeswaran, V. K. (2009). Implementation of Text based Cryptosystem using Elliptic Curve Cryptography, *IEEE International Conference on Advanced Computing*, p. 82-85.

[4] Hafid, Mammass., Fattehallah, Ghadi. (2012). Implementation of Smartcard Personalization Software. *International Journal of Future Generation Communication and Networking*, 5 (4) 39-54.

[5] Amounas, F., Kinani, E.H. El. (2013). A Novel Encryption Scheme of Amazigh Alphabet Based Elliptic Curve using Pauli Spin Matrice. *International Journal of Information & Network Security* (IJINS), 2 (3) 190-196.

[6] Abbas, Md. Zaheer., Murthy, JVR. (2012). Authenticated And Policy - Compliant Source Routing. *International Journal of Engineering Research and Applications* (IJERA). 2 (3)1347-1352.

[7] Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of Computation*, 48 p. 203-209.

[8] Miller, V. (1986). Use of elliptic curves in cryptography. Advances in Cryptology CRYPTO 85 (LNCS 218) (483) p. 417-426.