UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Tecnura

http://revistas.udistrital.edu.co/ojs/index.php/Tecnura/issue/view/687

DOI: http://doi.org/10.14483/udistrital.jour.tecnura.2014.DSE1.a06

Investigación

Authenticated encryption of pmu data

Criptoautenticación de datos en una PMU

Elvis Eduardo Gaona García*, Sergio Leonardo Rojas Martínez**,
Cesar Leonardo Trujillo Rodríguez***, Eduardo Alirio Mojica Nava****

Fecha de recepción: June 10th, 2014 **Fecha de aceptación:** November 4th, 2014

Citation / Para citar este artículo: Gaona García, E. E., Rojas Martínez, S. L., Trujillo Rodríguez, C. L., & Mojica Nava, E. A. (2014). Authenticated encryption of PMU data. *Revista Tecnura, 18* (Edición especial doctorado), 70–79. doi: 10.14483/udistrital.jour.tecnura.2014.DSE1.a06

ABSTRACT

This paper presents the implementation of an encryption board in order to provide confidentiality, authenticity and integrity of data collected at any point in a power grid, as a potential solution to the Smart Grid cyber security issues. This board consists of a Freescale microcontroller which enables the connection between a PMU (Phasor Measurement Unit) and a ZigBee transmitter. Encryption is done using the SHA256, HMAC-SHA256, KDF-SHA256 and AES256-CBC algorithms. This architecture makes reading and transmission of voltage and current phasors, energy consumption, frequency, power, power factor and power outages measurements, and sends this information in real time to a data concentrator where display and subsequent storage are possible.

Keywords: cyber security, hash function, phasor measurement, smart grids, symmetric cryptography unit.

RESUMEN

Este artículo muestra la implementación de una tarjeta de encriptado con el fin de proporcionar confidencialidad, autenticidad e integridad de los datos recolectados en cualquier punto de una red eléctrica, como posible solución a las dificultades que presenta el cibersecurity en las Smart Grid. Esta tarjeta está compuesta por un microcontrolador Freescale que permite la conexión con una PMU (Phasor Meter Unit) y dispositivos ZigBee. La encriptación se realiza empleando los algoritmos SHA256, HMAC-SHA256, KDF-SHA256 y AES256-CBC. Esta arquitectura realiza lectura y transmisión de mediciones de los fasores de voltaje y corriente, consumo de energía, frecuencia, potencias, factor de potencia e interrupciones de energía y los envía a un concentrador de datos en tiempo real, donde es posible su visualización y posterior almacenamiento.

Palabras clave: ciberseguridad, criptografía simétrica, función hash, redes inteligentes unidad de medición fasorial.

* He is a Ph.D. student in Engineering at Distrital University, Bogotá D.C. Colombia. He earned a M.Sc. in Information Science and communications at Distrital University, Colombia. He is professor at Engineering Faculty of Distrital University. His research interests are network and communications, microgrids. Contact: HYPERLINK "mailto:egaona@udistrital.edu.co" egaona@udistrital.edu.co

** He earned Electronic Engineer at the Distrital University. Contact: HYPERLINK "mailto:slrojasm@correo.udistrital.edu.co" slrojasm@correo.udistrital.edu.co

*** He earned a Ph.D. in Electronic Engineering at Polytechnic University of Valencia in Madrid, Spain. He earned a M.Sc. in Electrical Engineering at Distrital University, Colombia. He is professor at Engineering Faculty Distrital University. His current research interests include Electrical Power, Microgrids. Contact: HYPERLINK "mailto:cltrujillo@udistrital.edu.co" cltrujillo@udistrital.edu.co

****He earned a Ph.D. in Automation and Industrial Informatics at École des Mines de Nantes in France, Nantes. He earned a M.Sc. in Electrical Engineering and Computer at Andes University, Colombia. He is associate professor at the Department of Electrical and Electronics Engineering, National University of Colombia, Bogotá. His current research interests include Distributed Control Systems, Smart Grid. Contact: HYPERLINK "mailto:eamojican@unal.edu.co" eamojican@unal.edu.co

INTRODUCTION

Reliability and security of data collected by electric meters on the consumer side and the utilization of these data for pricing and consumption profiles require solutions for data transmission between the meter and the energy providers protecting customer privacy and ensuring accurate readings without modification of others.

For this purpose, it is necessary to establish a security system fulfilling integrity, authenticity and confidentiality requirements in order to prevent data alteration and unauthorized access to the network. Breaching channel confidentiality allows inferring consumption information revealing personal habits such as if someone was in a place for a particular time. Likewise, measuring and pricing process requires a secure transmission procedure where data integrity and authenticity are certified, since validity of user pricing method and power grid state estimation depend on it (NIST, 2010). Authors like DAI & YAN (2010), Peng, Elkeelany, & Layton, (2010), Seshabhattar, Priyanka, Krier, & Engels (2011), Gangil & Rakesh (2013) and Stallings (2011) present solutions including symmetric algorithms and HASH functions as a proposal to the Smart Grid security issues, fulfilling information confidentiality, authenticity and integrity purposes.

De Craemer & Deconinck (2010), Fan, *et al*. (2012), Luan, Teng, Chan, & Hwang (2009) and Khalifa, Naik, & Nayak (2011) have postulated the Zigbee protocol as a potential solution to obtain simultaneous measurements in real time from multiple connected devices similarly to AMR (Automatic Meter Reading) networks; this, given the smooth implementation of short-range networks with low energy consumption and data transfer rates up to 250 Kbits/s.

This paper shows a possible solution to the Smart Grid cyber security issues by means the implementation of an encryption board which provides confidentiality, authenticity and integrity of data collected anywhere on the power grid. The paper is organized as follows: section 2 describes the methodology used for the design and implementation of the encryption board and its role within the reading system, as well as the transmission of data measured by a PMU. In section 3 the obtained simulation results, the designed HMI interface and the implementation of the encryption board are presented. Finally, in section 4 conclusions are shown.

METHODOLOGY

Proposed Architecture

Figure 1 shows the proposed architecture for reading, transmission and storage of information related to the power grid state and energy consumption in different points; the proposed system is divided in two parts, the data concentrator and the meter; in this case, the meter is composed by a PMU and an encryption board. The PMU performs the measurements related to the power grid variables, and the encryption board captures the information from the PMU converting it into confidential information, performing the integration and authentication by means of a security scheme; wireless transmission is made using a Zigbee network with star topology where the concentrator has the role of network coordinator and each of the meters is an end device.

On the meter side the PMU 1133A Power Sentinel of company ARBITER SYSTEMS is used, which collects the voltage and current phasor, energy consumption, frequency, power, power factor and power outages measurements. The measured values are stored in internal registers, and the MODBUS RTU protocol is used via an RS232 serial connection to route them externally.

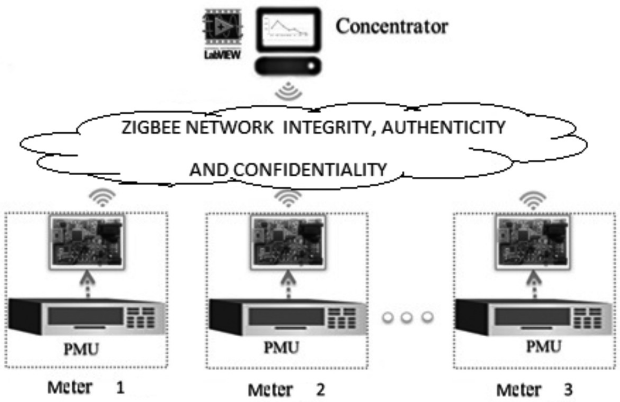


Figure 1. Measurement system architecture

Source: Own work.

The encryption board is composed by a Freescale microcontroller of ColdFire V1 family, which allows the connection to the PMU and the ZigBee transmitter through two asynchronous serial modules and the connection to the ATSHA204 cryptographic keys storage device through the I2C (Inter-Integrated Circuit) synchronous serial module. The microcontroller software contains subroutines to implement the MODBUS-RTU protocol, from the SHA256 (NIST, 2012), HMAC-SHA256 (NIST, 2008), KDF-SHA256 (NIST, 2011) and AES256-CBC (Daernen & Rijrnen, 2002), (NIST, 2001) algorithms used in four main processes: i) Reading and transmission of PMU information, ii) data encryption, addition of authenticity and integrity to the information, iii) verification of information authenticity and integrity and iv) key derivation.

The concentrator consists of a ZigBee communication module, a user interface designed in Labview, and the software including subroutines for the SHA256, HMAC-SHA256, KDF-SHA256 and AES256-CBC algorithms used for the meters administration, data validation and information display and storage.

Security Scheme

In the implementation of the security scheme the recommendations of the National Institute of Standards and Technologies (NIST) and Cyber Security (CS) in Smart Grid (SG) (NIST, 2010) were taken into account, approving the use of existing cryptographic functions and algorithms, as well as configurations and parameters to get a better performance and an adequate security level. There are three families of cryptographic algorithms —HASH functions, symmetric algorithms and asymmetric algorithms; for the three families NIST approves only the use of the algorithms listed in Easter & Bryson (2012).

Each algorithm can be used for a specific purpose or to fulfill several objectives in the same process. Table 1 shows the algorithms used to provide confidentiality, integrity or authenticity to a communication channel; at the same time, they can be used to generate cryptographic keys (KDF Key Derivation Function) or distribute them (KD - Key Distribution) and in the process of random number generation (RNG - Random Number Generator).

Table 1. Functions available for each of the families of cryptographic algorithms

Function	Symmetric	Asymmetric	HASH
Confidentiality	YES	YES	-
Integrity	YES	-	YES
Authenticity	YES	YES	YES
KDF	-	-	YES
RNG	-	YES	YES
KD	YES	YES	-

Source: (NIST, 2007).

The security scheme proposed in this paper addresses the need to protect the data confidentiality, integrity and authenticity by means of symmetric cryptographic algorithms, since the keys for these algorithms are smaller than those of an asymmetric algorithm with the purpose of obtaining the same level of security requiring less time to process information. In addition, less resources in a communication channel are required, since the encrypted text has the same size than the plaintext, ensuring that all the sent information will be useful, which does not occur with asymmetric algorithms, which add bits to the encrypted text increasing the size with the same useful information (Khurana et al., 2010).

The implemented security system is divided in two parts: i) the process of key generation and distribution, where only the SHA256 algorithm is used and ii) the authenticated encryption scheme where the HMAC-SHA256 algorithm is used to calculate the MAC (Message Authentication Code) and therefore to determine the information integrity and user authenticity, and the AES256 algorithm to protect the information confidentiality.

Key generation and distribution scheme

The proposed security system fulfills the following requirements:

- It does not compromise the security of any objective (authenticity, integrity and confidentiality) when one in particular is compromised.
- It does not compromise the security of any node when the security of one in particular is compromised.

To fulfill the first requirement, independent keys are used for each of the objectives; the keys used in the security system are listed below:

- Symmetric key for authentication k_A: Key used in the HMAC algorithm to generate the HASH code that allows obtaining the message authentication code.
- Symmetric key for information encryption k_s: Key used by AES-256 to protect the information confidentiality in the communication channel.
- Master symmetric key k_m: Key used by the KDF algorithm to derivate other keys (k_A, k_s).

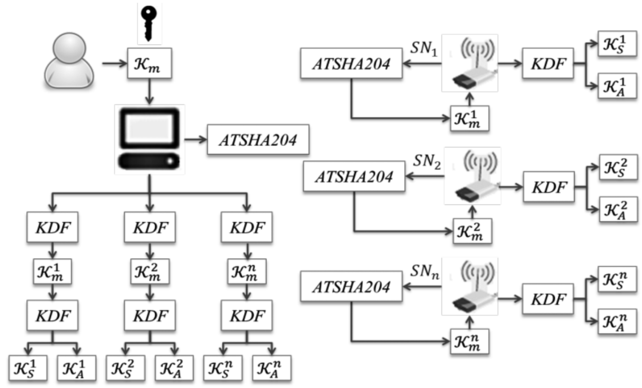


Figure 2. Key derivation and distribution scheme

Source: Own work.

To simultaneously fulfill both requirements, the scheme of figure 2 is implemented, where a different key set is used for each of the meters associated to the network. The initial master key k_m is introduced in the concentrator and in the key transportation device ATSHA204. In each of the meters a key set $\mathcal{K}_{\mathrm{m}}^{\mathrm{n}}, \mathcal{K}_{\mathrm{A}}^{\mathrm{n}}$ and $\mathcal{K}_{\mathrm{S}}^{\mathrm{n}}$ is derived; in the first step $\mathcal{K}_{\mathrm{m}}^{\mathrm{n}}$, is derived by executing the equation (1) over the device ATSHA204, where is the indicator of the selected meter, SN is the serial of the ZigBee module, MAESTRA is the label indicating that the key is derived. In this case, with value 0x00 and KDF is defined by equation (2).

$$K_m^n = KDF\left(K_m, MAESTRA, 0x00, SN^n, 0xFF\right) \quad (1)$$

$$y = KDF(x) = SHA256(x); |x| < 2^{64} bits; |y| = 256 bits \quad (2)$$

To derivate K_A^n and K_S^n, equations (3) and (4) are executed over the microcontroller, where

AUTENTICACION=0x01 and *ENCRIPTACION=0x02*.

$$K_A^n = KDF(K_m^n, AUTENTICACION, 0x00, SN^n, 0xFF) \quad (3)$$

$$K_S^n = KDF(K_m^n, ENCRIPTACION, 0x00, SN^n, 0xFF) \quad (4)$$

Simultaneously, the same process is executed over the concentrator; in this way, the concentrator and each meter have the same key set.

Authenticated Encryption Scheme

The authenticated encryption scheme uses the AES-256 and HMAC-SHA256 algorithms together to fulfill confidentiality, integrity and authenticity objectives. The AES-256 algorithm is used in the CBC (Cipher- Block Chaining) configuration where each of the encrypted blocks depends on the previous blocks allowing encrypted text blocks are indistinguishable between them.

The HMAC-SHA256 algorithm is a variation of the SHA256 algorithm described by equation (5), which allows generating a message authentication code (MAC) from a HASH function, where *ipad* is 0x36 repeated 64 times and *opad* is 0x5c repeated 64 times.

$$HMAC = H\big((K_0 \oplus opad) \,\|\, H((K_0 \oplus ipad) \,\|\, M)\big) \quad (5)$$

From Katz & Lindell (2007), the EtM (Encrypt then MAC) configuration is used, which simultaneously utilizes both algorithms, first perform the encryption of the plaintext and then the MAC is computed protecting directly the encrypted text against integrity or authenticity attacks and indirectly the plaintext.

Figure 3 summarizes the process to perform in order to send the information protecting its confidentiality, integrity and authenticity, and Figure 4 shows the process to verify the integrity and authenticity and additionally decrypt the received information.

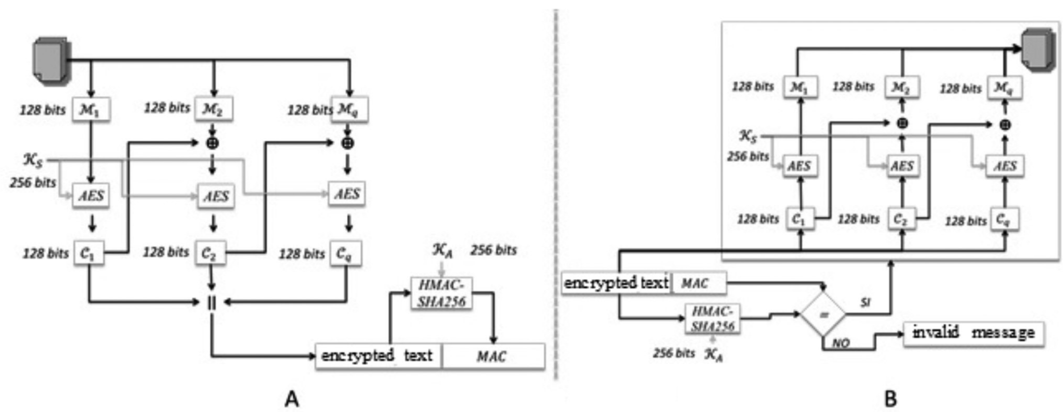


Figure 3. CryptoAutentication Scheme for (A)information transmission and (B) information receiving and validation

Source: Own work.

Network architecture based on Zigbee technology

Transmission is done through a Zigbee network with star topology, where each network device has an associated Zigbee module. In this case, the concentrator manages the network and communicates with each of the meters. For this reason, the Zigbee module is configured as coordinator, and meters have a module configured as end device.

Each time the information is sent from the coordinator to the meter or vice versa, the process of Figure 3 is executed, and the information is encapsulated in the frame structure provided by the Zigbee API operating mode.

# Bytes	Serial	Datos	MAC
1 byte	8 Bytes	16*n Bytes	32 bytes

Figure 4. Payload structure of Zigbee API frame

Source: Own work

Figure 4 shows the distribution of the payload field of the API frame, the data field has a size multiple of 16 bytes given by the AES256 algorithm, always encrypted and which sends the frames of figures 6 and 7; the MAC field is the result of running the HMAC-SHA256 algorithm over the data field.

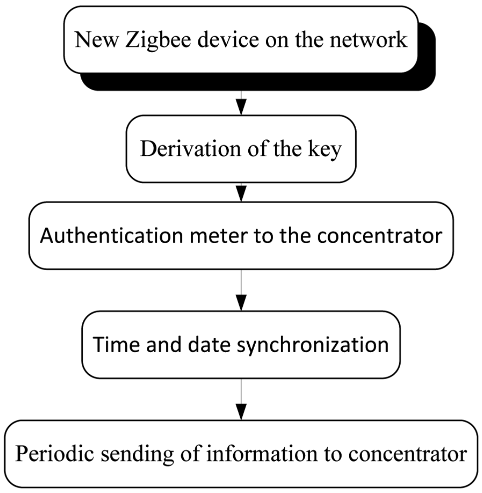


Figure 5. Flowchart for starting the encryption board and information transmission

Source: Own work.

Figure 5 shows the flowchart that a meter follows when the encryption board is started. In the first step the coordinator executes the admission process of a new Zigbee device on the network, then the derivation of the key set is done in the microcontroller and it proceeds to send the request for authorization of figure 6, where the result of calculate $\mathrm{SHA256}(\mathcal{K}_A^n \,||\, \mathcal{K}_S^n)$ *is sent*.

When the concentrator receives the request, it performs the same calculation with the keys derived inside and compares the result, checking the MAC it is verified that the keys generated by the two parties are the same without having to send them by the communication channel and simultaneously the identity of the meter sending the information is verified. Once keys and identity are confirmed, the confirmation of authorization of figure 7 including actual date and time is sent, the meter is authorized and synchronizes date and time, with this the setup process finalizes and the periodic sending of information starts as requested by the concentrator.

Valor	0x00	-	-	-	-	-	-	-	-	-	-	0x00
Nombre	Comando	Fecha	V	Fase V	I	Fase I	P. Activa	P. Reactiva	P. Aparente	Factor de P.	Frec	Ceros
# Bytes	1	7	2	2	2	2	2	2	2	2	2	6

Valor	0x01	-	-	-	-	-	-	-
Nombre	Comando	Fecha	E. Activa	E. Aparente	E. reactiva C1	E. Reactiva2	E. reactiva C3	E. reactiva C4
# Bytes	1	7	4	4	4	4	4	4

Valor	0x02	-	0x00
Nombre	Comando	SHA256(Ka, Ks)	Ceros
# Bytes	1	32	15

Figure 6. Types of frames sent from the meter to the concentrator

Source: Own work.

Peticion Iniciar Medicion Tiempo Real		
Valor	0x00	0x00
Nombre	Comando	Ceros
# Bytes	1	15

Peticion Detener Medicion Tiempo Real		
Valor	0x01	0x00
Nombre	Comando	Ceros
# Bytes	1	15

Peticion Iniciar Medicion De energia		
Valor	0x02	0x00
Nombre	Comando	Ceros
# Bytes	1	15

Borrar claves		
Valor	0x03	0x00
Nombre	Comando	Ceros
# Bytes	1	15

Confirmacion autoricacion envio de fecha y hora						
Valor	0x04	-	-	-	-	0x00
Nombre	Comando	Ano	Mes	Dia	Hora	Ceros
# Bytes	1	1	1	1	4	8

Figure 7. Types of frames sent from the concentrator to the meter

Source: Own work.

Figure 6 shows the structure of the information sent from the meter to the concentrator. This information is divided in two types: the first for voltage and current phasors measurements, frequency and power, which is sent in real time and the second for sending energy consumption which is done by request from the concentrator. Figure 7 shows the frame structure used for a request from the concentrator to each of the meters.

RESULTS

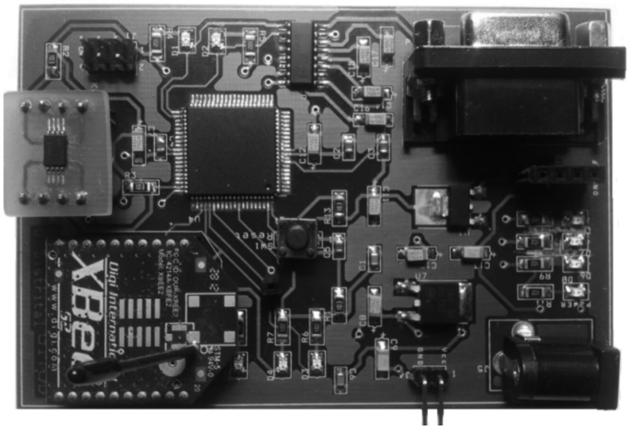
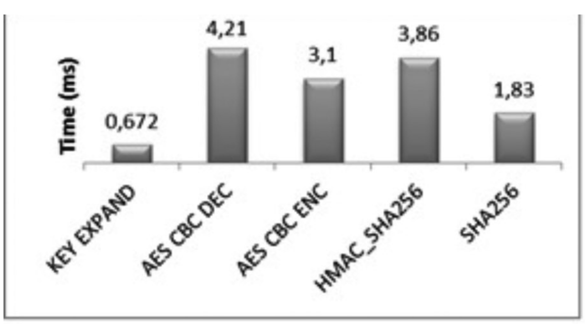


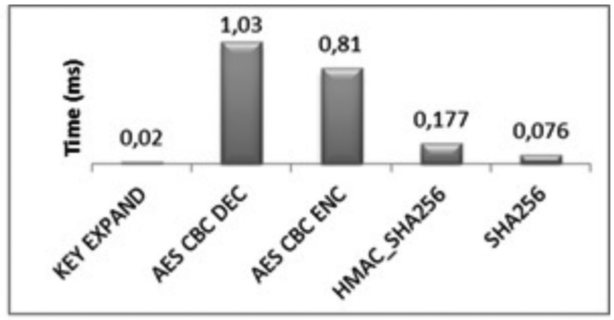
Figure 8. Encryption board

Source: Own work.

The encryption board shown in figure 8 was implemented for reading, transmission and storage of information related to the power grid state using a ZigBee transmitter. It includes information security parameters such as confidentiality, integrity and authenticity, through the implementation of the SHA256, HMAC-SHA256, KDF-SHA256 and AES256-CBC algorithms in the microcontroller included in the encryption board. Figure 9 (A) presents the measurements of running times achieved by implementing the AES256 algorithms representing 32 bits and SHA256 in the MCF51QE128 Freescale microcontroller, and figure 9 (B) shows these results in Labview under a 32 bit platform.



A



B

Figure 9. Runtimes of cryptographic algorithms in (A) microcontroller and (B) Labview

Source: Own work.

The system is controlled by the HMI in Figure 10 developed in Labview, which allows to start and stop sending real time data from each meter, to request energy consumption, to request key change, to observe measured variables in real time and to store historical measurements from each meter. Starting the encryption board the authentication and synchronization process starts, which is notified in the HMI, successfully completed this process it is possible to do the requests of figure 8 over the chosen meter.

A simulation using OPNET Modeler was carried out in order to estimate the number of meters that can be connected to the concentrator and to perform transmission of real time simultaneous information without losing data, where the following parameters were configured:

- Star topology with data transmission only from the meter to the network coordinator.
- Packet size of 512 bits per meter in the application layer.
- Transmission time between packs of 82,16 ms per meter, which includes the time employed to read information from the PMU (75,2 ms) plus delay of the authenticated encryption scheme (6,96 ms). These are enough times for electric energy management in terms of generation and consumption.

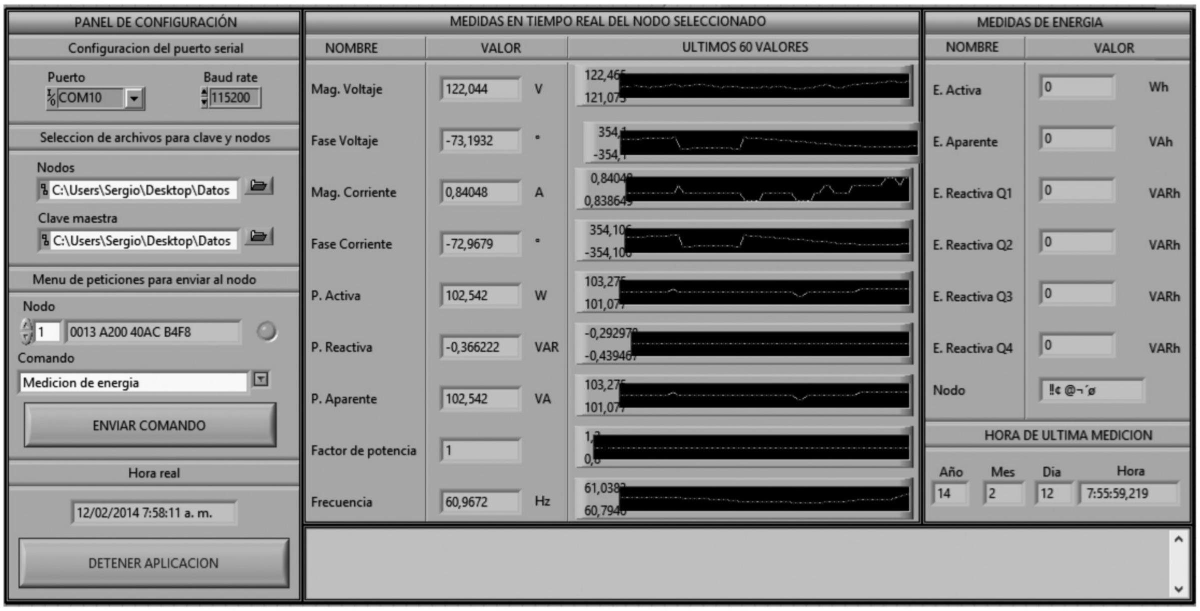
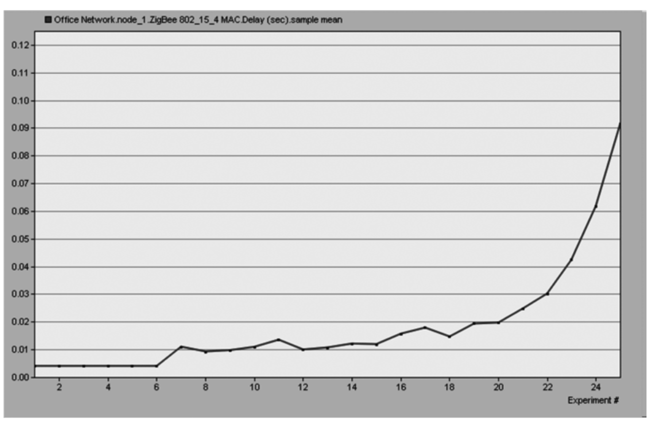


Figure 10. HMI (Human Machine Interface)

Source: Own work.

Simulation result is shown in Figure 11 (A), where the vertical axis is the time in seconds. It takes the meter to access the channel and the horizontal axis presents the number of meters in the network; the figure shows that by using simultaneously 25 meters, average delays of 90 milliseconds are obtained, being greater than the time between packs, causing loss of data. Figure 11 (B) shows the traffic received by the concentrator and channel saturation is identified from 24 meters.



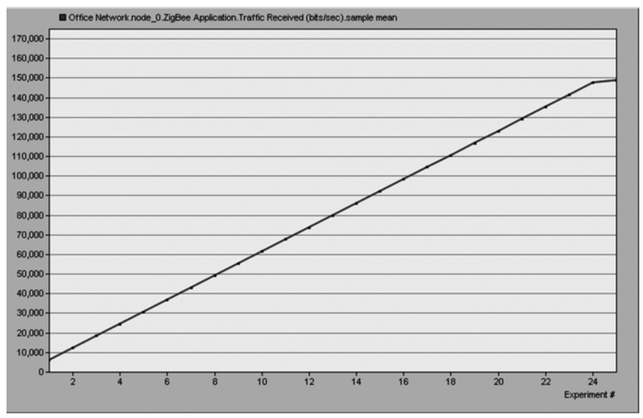


Figure 11. (A) Average access time from the meter to the channel, (B) Traffic received by the concentrator in the application layer for each of the scenarios in bits/s

Source: Own work.

Each meter is waiting for a request from the concentrator to start a real time or energy consumption information transmission after performing the authentication and synchronization process. Figure 12 (A) shows the encapsulated request in a Zigbee API frame sent from the concentrator, by implementing the figure 3 process.

In the first step, the data field is encrypted with AES256 under the key k_s, then the MAC is calculated with the HMAC-SHA256 algorithm based on the key k_a and finally the frame is sent to the meter. When the meter receives the frame, first runs the HMAC-SHA256 algorithm to validate the MAC and then decrypts the data field with the AES256 algorithm, the result indicates the start of real time information transmission because in the "command " field a " 0x00 " was received.

Figure 12 (B) shows the measurement performed by one of the meters using a load of 132 W required by the concentrator, there the encrypted data field and the MAC, encapsulated in the same frame structure, are included. After receiving this frame, the concentrator validates the source address through the MAC, then decrypts the data field including the descriptor of frame "0x00" with the date and time of data measurement, current and voltage phasors, power and frequency.

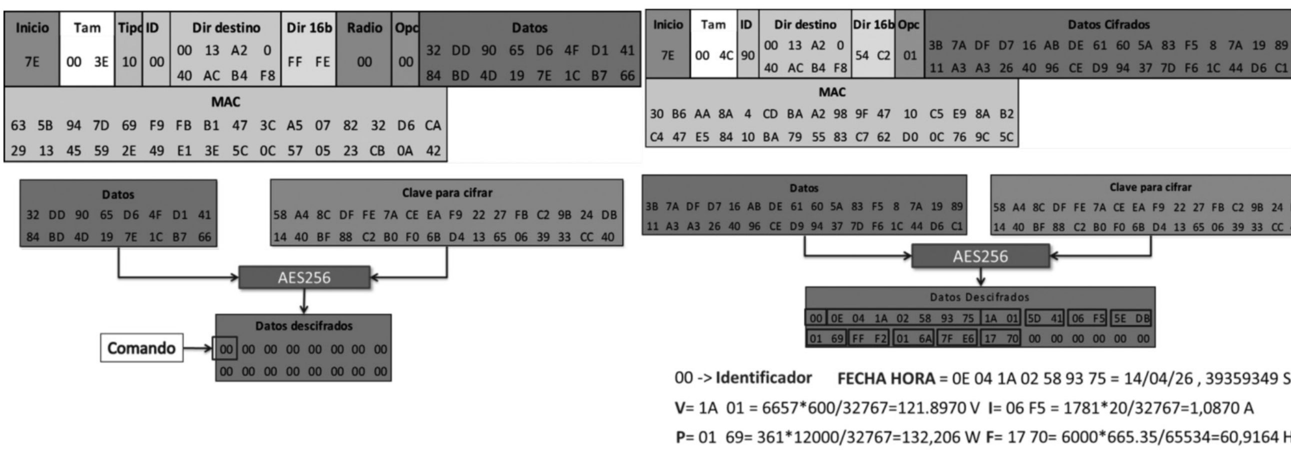


Figure 12. (A) Request from the concentrator to the meter to start real time measurement, (B) Response from the meter

Source: Own work.

CONCLUSIONS

A collector-meter communication system was implemented that allows monitoring energy consumption and real time state of the power grid in each of the meters associated to the network. The security of this system was achieved in two levels, the first with the design and implementation of the encryption board which protects data authenticity, integrity and privacy at the point of measurement in the power grid through the PMU, and the second level for data transmission integrating the security system with security mechanisms that Zigbee technology incorporates. This combination in the security system implemented as last mile solution for secure and reliable access to information is the first of its kind, because it is made from the client side.

The implemented security scheme fulfills the information confidentiality, integrity and authenticity requirements using symmetric cryptographic algorithms with keys smaller than asymmetric algorithms, providing less time for information processing with the same security level.

The time employed for encryption and transmission of data collected from the PMU is enough for electric energy management in terms of generation and consumption. However, it is not recommended to use encryption when sending voltage or frequency references to the inverters for certain events because they are greater than half cycle of the sine wave.

ACKNOWLEDGEMENT

This work was supported by the CIDC (Centro de Investigación y Desarrollo Científico) of Universidad Distrital Francisco José de Caldas in Bogotá D.C. Colombia. Project Number 2-195-405-1 (Metodología para la implementación de un sistema de comunicaciones en microrredes eléctricas), and LIFAE Research group (Laboratorio de fuentes alternativas de energía).

REFERENCES

Daernen, J. & Rijrnen, V. (2002). *The Design of Rijndael, AES - The Advanced Encryption Standard*. Springer.

Dai, J.-j. & Yan, M. (2010). The design and implementation of 128-bit AES encryption in PRIME. *2010 3rd International Conference on Computer Science and Information Technology*, 345-348.

De Craemer, K. & Deconinck, G. (2010). *Analysis of State-of-the-art Smart Metering Communication Standards*. Obtenido de Ku Leuven Repository: https://lirias.kuleuven.be/bitstream/123456789/265822/1/SmartMeteringC.Easter, R., & Bryson, J. (2012). Security Requirements for Cryptographic Modules. *Approved Security Functions for FIPS PUB 140-2*.

Fan, Z. et al. (2012). Smart Grid Communications: Overview of Research Activities. *Communications Surveys & Tutorials, IEEE*, 21-38.

Gangil, G. & Rakesh, N. (2013). Advanced Security Algorithm for Power Grid, 409-417.

Katz, J., & Lindell, Y. (2007). *Introduction to Modern Cryptography*. Chapman & Hall/.

Khalifa, T., Naik, K. & Nayak, A. (2011). A Survey of Communication Protocols for Automatic Meter Reading Applications. *IEEE Communications Surveys & Tutorials*, 168-182.

Khurana, H., Bobba, R., Yardley, T., Agarwal, P. & Heine, E. (2010). Design Principles for Power Grid Cyber-Infrastructure Authentication Protocols. *2010 43rd Hawaii International Conference on System Sciences*, 1-10.

Luan, S.-W., Teng, J.-H., Chan, S.-Y. & Hwang, L.-C. (2009). Development of a smart power meter for AMI based on ZigBee communication. *2009 International Conference on Power Electronics and Drive Systems (PEDS)*, 661-665.

NIST. (2001). Advanced Encryption Standard (AES) Federal. *Federal Information Processing Standards Publication FIPS PUB 197*, 47.

NIST. (2007). Recommendation for Key Management. *NIST Special Publication 800-57*, 142.

NIST. (2008). The Keyed-Hash Message Authentication Code. *Federal Information Processing Standards Publication FIPS PUB 198-1*, 8.

NIST. (2010). *Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid*. From the National Institute of Standards and Technology: www.nist.gov

NIST. (2010). *Nistir 7628 Guidelines for Smart Grid Cyber Security*. Form The National Institute of Standards and Technology: http://csrc.nist.gov/publications/nistir/ir7628/introduction-to-nistir-7628.pdf

NIST. (2011). Recommendation for Existing Application-Specific Key Derivation Functions. *Federal Information Processing Standards Publication FIPS PUB 800-135*.

NIST. (2012). Secure Hash Standard (SHS). *Federal Information Processing Standards Publication FIPS PUB 180-4*.

Peng, Z., Elkeelany, O. & Layton, M. (2010). An implementation of secured Smart Grid Ethernet communications using AES. *Proceedings of the IEEE SoutheastCon 2010 (SoutheastCon)*, 394-397.

Seshabhattar, S., Priyanka, Y., Krier, P. & Engels, D. (2011). Hummingbird Key Establishment Protocol For Low- Power ZigBee. *IEEE Consumer Communications and Network*, 447-451.

Stallings, W. (2011). *Network Security Essentials: Applications and Standards*.