Bulletin of Electrical Engineering and Informatics
Vol. 9, No. 2, April 2020, pp. 777~784
ISSN: 2302-9285, DOI: 10.11591/eei.v9i2.2086

A lightweight security scheme for advanced metering infrastructures in smart grid

S. M. Salim Reza[1], Afida Ayob[2], Md Murshedul Arifeen[3], Nowshad Amin[4], Mohd Hanif Md Saad[5], Aini Hussain[6]
[1,2,5,6]Department of Electrical, Electronic & Systems Engineering, Faculty of Engineering and Built Environment, The National University of Malaysia, Malaysia
[3]Department of Information and Communication Technology, Bangladesh University of Professionals, Bangladesh
[4]Institute of Sustainable Energy, University Tenaga Nasional, Malaysia

Article Info

Article history:

Received Oct 30, 2019
Revised Dec 28, 2019
Accepted Feb 11, 2020

Keywords:

Advanced metering
Infrastructure
Authentication
Chacha20
Logistic map
Smart grid

ABSTRACT

Smart Grid (SG) enlarges the traditional power grid into a new dimension where millions of electronic devices relate to each other through Advanced Metering Infrastructures (AMI) network using information and communication technology (ICT). The integration of ICT to the traditional power grid opens the path for the adversaries to invade through various cyber-attacks. Resource constrained electronic devices connected in AMI with the SG claims for faster, low power, less processing time and overall lightweight security schemes to prevent the cyber-attacks and to make the grid secure from adversaries. In this paper, a lightweight security scheme has been proposed consolidating ChaCha20 data encryption method, chaos based key generation and public key-based authentication scheme. Mathematical analysis shows that the proposed scheme is suitable to be used in SGs in terms of low power, less processing time and high throughput which makes it lightweight and faster. This scheme also prevents any kind of timing attacks such as replay attack.

Corresponding Author:

Afida Ayob,
Department of Electrical, Electronics and Systems Engineering,
Faculty of Engineering and Built Environment,
The National University of Malaysia, Malaysia.
Email: afida.ayob@ukm.edu.my

1. INTRODUCTION

Smart Grid (SG) is visualized as the next generation power grid system which integrates the renewable energy sources (solar power, wind power, bio gas) with the long-established power grid system. It builds an enormous high speed bi-directional communication infrastructure by incorporating millions of electronic devices among the consumers or subscribers and the utility providers which is also known as AMI. Enriching the traditional power grid, SG offers real time monitoring of energy consumption, ensures power flow optimization, understanding consumers energy consumption behavior, enhancing power transmission reliability and quality, reducing costs for electrical appliances, reduces green house gas emissions [1, 2]. These significant advantages provide the utility providers to manage and handle the distribution of electric power in a more efficient and robust way through analyzing customers demand response. Various types of advanced technologies including advanced metering infrastructure (AMI), wide area network, private area network is forming these huge grids connected two-way communication network. AMI is one of the principle functional element of SG. It is responsible for collecting data from the customers

and makes a bridge between utility company and consumers. It consists of smart meter (SM) at customers end, communication network, meter data management system (MDMS), software applications, interfaces. Everyday millions of data are exchanging from customer end to the service provider end and vice versa. This heavy dependability on smart communication network connected with power grid opens the loophole for the adversary or intruders to trespass the network and the inherent vulnerabilities of the information and communication network of power grid allows the attackers to launch cyber attacks which can lead to hazardous situation in SG. Due to the security vulnerabilities and cyber attacks the SG is suffering from grid instability, utility fraud, and loss of user information and energy-consumption data [3]. The communication between different entities in this network need to be secured or otherwise the privacy of the network will be breached through exposing private data to the intruders.

Cyber attacks including wormhole attack, black hole attack, jamming attack, phishing attack etc can be classified as insider and outsider attacks. In case of insider attacks, the intruder takes control over the legitimate electronic devices to manipulate raw data, inject false message or can drop all received packets and also compromising legitimate devices he can launch various attacks like packet dropping attack or sink hole attack. In case of outsider attacks, the adversary tries to interrupt the network operation without accessing the network. The former one can be mitigated through trust management model but for the later one resource efficient security mechanism is required. However, the conventional cryptography mechanisms like digital signatures, PKI based scheme imposes extensive computational cost, processing delay and overhead [4]. It is a challenge to design efficient, robust, faster and affordable cryptography mechanism for AMI network in SG satisfying data confidentiality, integrity, low communication and computational overhead and less processing time.

Recently, several authors have proposed that lightweight security mechanism is suitable for SG network and proposed various types of security mechanisms discussed in detail in review section. But most of the methods are proposed for only some sub infrastructures like between smart meter (SM) and service provider (SP) or between Cunsumer and substation. Also, some authors proposed highly complex security scheme like advanced encryption standard (AES) in [5] which is not resource efficient or lightweight to be used in AMI low cost devices. Thus, in this paper a lightweight security scheme has been proposed to ensure security in SG. The proposed scheme consists of data encryption scheme ChaCha20 encryption technique [6]. ChaCha20 is a simple stream cipher which is is secure and faster designed by Daniel J Bernstein [6]. The principle advantage of ChaCha20 is that it is designed based on ARX (Addition, Rotation and XOR) cryptography technique which provides faster performance, less complexity and eliminates timing attack. ChaCha20 introduces simpler round functions compared to other conventional cryptography techniques which makes it well-suited and lightweight to be used in SG network. A chaotic map (one dimensional logistic map) based random number generation has been introduced. The random numbers generated from logistic maps are used to produce secret keys for ChaCha20 encryption algorithm. Different techniques are used to generate secret keys but keys based on non linear system provide better cryptography. As chaotic maps are non-linear, chaos based key generation increases security level and ensures good cryptography properties and it is difficult to crack any cipher generated through chaos based secret key [7]. The proposed method consists of two phase- initialization phase and information exchange phase. In initialization phase, the smart devices are assigned private and public keys. Before starting any information exchange the paired devices first authenticate themselves through exchanging public and private key. After verifying each other, they exchange data using lightweight strong secure cryptography scheme called ChaCha20.

To provide authentication and integrity, the authors in [8] proposed a mechanism that uses low cost hardware named physically unclonable function (PUF) and CSI based encryption mechanism. Due to scalability of Smart Grid (SG), traditional security based on PKI are not suitable. Thus the literature proposed a non cryptography mechanism based on PUF and CSI. The proposed mechanism only focuses the security between smart meter and concentrator. A security mechanism is needed to be designed which can focus not only the security between smart meter and concentrator but also other sub infrastructures. A lightweight security and privacy preserving scheme based on electricity forecasting has been proposed. This scheme reduces communication and computation overhead. The proposed scheme is based on predicting the expected electricity demand for a HAN cluster. The scheme restricts the connection with the provider when the demand needs to be adjusted [9]. It is required to design security scheme addressing communication and computation overhead which is signified in this paper. The main contribution of [10] this paper is, the authors proposed an authentication mechanism between utility company and SM which enhances security of the smart grid by providing low overhead. But other parts of the smart grid network is not considered for security. Anonymised authentication framework has been proposed in [11] which consists of an authentication scheme and an anonymisation mechanism to protect the privacy of the data. The proposed scheme is more resilient in terms of privacy preserving purpose in SG. To achieve

the authentication between SM and service provider (SP), an anonymiser entity performs anonymisation process between them. Security mechanisms should be developed to be used in other substructures such as between SM and electronic devices connected with electrical appliances as well as SM and SP. The proposed method in [12] ensures source authentication, data integrity, message confidentiality and non repudiation as it is based on public key based approach. However, Public key cryptography is complex which is not suitable for limited memory and processing capability of SM. It must be ensured that the designed security scheme is lightweight, less complex and compatible to be used in low cost electronic devices such as SM. A lightweight authentication protocol based on shared secret key and random number has been proposed in [13] for two way communication between supervisory node and control node. This method can effectively prevent man in the middle attack and replay attack and also improves certification security of SG. PUF and one way hash function based lightweight cryptography scheme has been proposed in [14] that ensures secure communication between SM and SP. Ensures resilience against DoS attack, Man in the middle attack and forward secrecy. Also the authors have introduced fuzzy extractor to reduce noise from PUF. A bi-linear map pairing based authentication mechanism has been proposed in [15] which can overcome the limitations faced by the methods propose in [16]. Besides eliminating the problems, the proposed scheme can also ensure perfect forward privacy, message integrity, private key privacy and resiliency against replay attacks. To ensure mutual authentication and session keys, the authors in [17] uses bi-linear pairing technique.which ensures confidentiality of the communication between electrical vehicle and SG. The protocol eliminates centralization problems and it has comparatively better computational and communication costs. Elliptic curve cryptography based authentication scheme has been proposed in [16] for secure communication between consumers and substations. The proposed scheme provides mutual authentication with low computation and communication costs. But the scheme can not ensure forward secrecy and private key privacy [15]. An anonymous message authentication scheme has been introduced in [5] to overcome the problems faced by the methods proposed in [18]. However, here the authors proposed AES which is a computationally expensive encryption mechanism that requires high resources. The smart meters are unable to provide the resources needed by AES. Thus lightweight mechanism is required.

In this paper, the issues that are being emphasized are extra computational cost, huge processing delay, overhead and resource (energy, memory) consuming security scheme for smart devices of AMI architecture of SG is not acceptable. A lightweight, energy efficient and faster security scheme comprising of ChaCha20 encryption in SG has been proposed and compared with the proposed AES based security method in [18]. This claim has been proven mathematically and also that ChaCha20 performs better in terms of computational cost, processing time and throughput than AES. Also, this scheme can be used between any paired devices in AMI.

2. SMART GRID NETWORK ARCHITECHTURE

In this section a brief overview of SG communication network architecture is presented. According to National Institute of Standards and Technology (NIST) the SG is comprised of seven interconnected domains including Bulk Generation, Transmission, Distribution, Customer, Markets, Service Provider and Operations [19, 20]. The first four domains are responsible for power distribution and information flows from tow ends. The last three are responsible for market data collection and power management. A simple architecture is demonstrated in Figure 1. In lower layer, home area network (HAN), building area network (BAN) and industrial area network (IAN) is connected. In this layer all the electrical appliances are connected with the smart meter (SM). The SM acts as a gateway to these devices by collects electricity consumption data, customers demand or response data and forwards them to the power management authority and vice versa. The communication between the SM and the electrical appliances can be established through wireless or wired communication. In the middle layer, different networks from the lower layer are connected to a single aggregator node also known as neighborhood area network (NAN). NAN is responsible for forwarding all the data collected from different networks to the top layer through substation. In the top layer power generation unit, power distribution unit and other units like MDMS, demand response management system (DRMS), load management system (LMS) are situated. This domain distributes power, analyze customers demand, provide billing information.

3. RESULTS METHOD

The proposed solution comprises of three distinguished stages: Initialization Phase, Information Exchange Phase and Key Generation Phase. The overall security scheme is depicted in Figure 2.

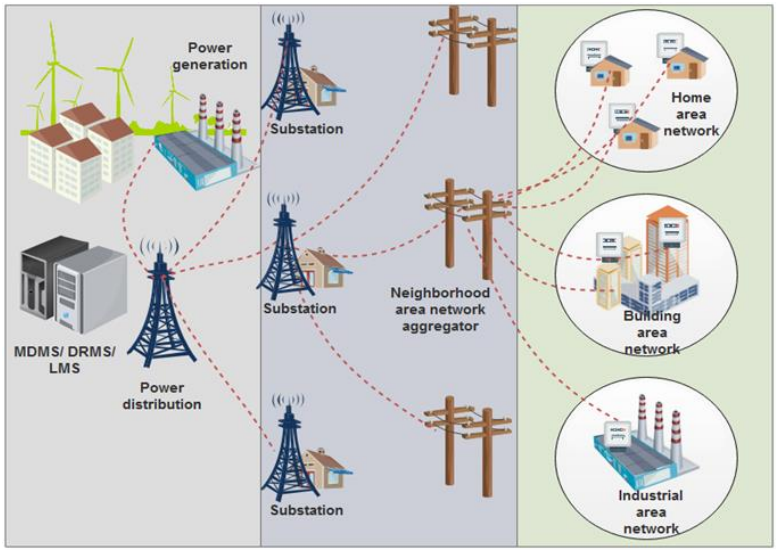


Figure 1. Architecture of smart grid network

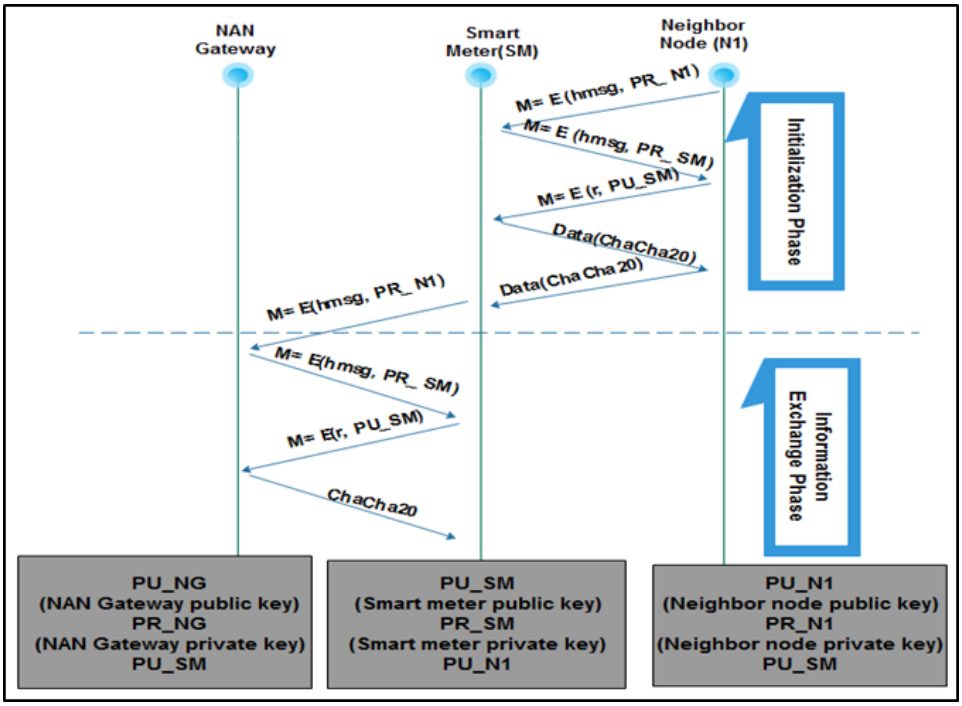


Figure 2. Overall security scheme

3.1. Initialization phase

In initialization phase, each device is assigned with a public *PU_i* and a private key *PR_i* for authentication purpose. The SM will identify whether a device is legitimate or not through authentication scheme. During any session, the nodes (smart devices) connected with the electrical appliances will send hello message hmsg encrypted with his private key *PR_i* to the SM. The SM has the corresponding public key *PU_i* of that smart device. The SM will decrypt the message and send response message rmsg encrypted with its private key *PR_i*. In this way, by using simple public key and private key exchanging the devices will be authenticated with each other. After that, the nodes connected with the electrical appliances will share the secret value of parameter of the chaotic system "r", described in key generation phase. Based on this value the SM and the node will generate encryption and decryption keys and will use these keys in ChaCha20

cipher algorithm for data encryption and decryption purpose. Any paired device in the AMI network of SG will follow this procedure.

3.2. Information exchange phase

For information exchange, ChaCha20 cipher algorithm is suggested for its resource efficient behavior with less complexity. ChaCha20 stream cipher is the variant of Salsa20 cipher proposed in [6] by Daniel J Bernstein. ChaCha20 stream cipher takes plain text as input of length \$16\$ words and outputs a cipher text of length 16 words. That is cipher text (*C_i*)=plaint text (*P_i*) ⊗ ChaCha20 key stream and the decryption is performed in the reverse way of encryption as plain text (*P_i*)=cipher text (*C_i*) ⊗ ChaCha20 key stream. The key stream of ChaCha20 is generated through ChaCha20 block function where the ChaCha20 block function performs some round function on some initial 4× 4 matrix consisting of four 4 bytes constants, eight 4 bytes key (chaotic logistic map is used to generate keys), one 4 bytes counter value and three 4 bytes Nonce. The algorithm operates on four 4 bytes words at a time. ChaCha20 scrambles the 64 bytes (16 words) initial block through quarter round function. 20 rounds (10 column rounds and 10 diagonal rounds) are performed on each 16 words of a packet. Each round itself performs 4 quarter round operation on four 4 bytes words as follows:

a+=b; d^=a; d <<<=16; (1)

c+=d; b^=c; b <<<=12; (2)

a+=b; d^=a; d <<<=8; (3)

c+=d; b^=c; b <<<=7; (4)

The ChaCha20 algorithm block diagram is depicted in Figure 3.

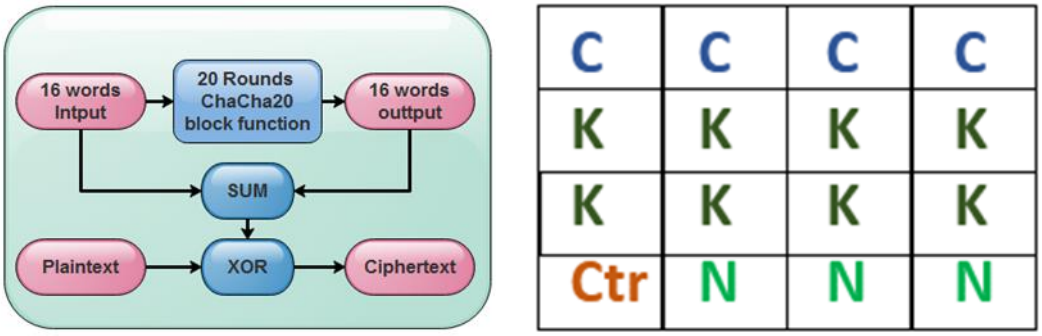


Figure 3. ChaCha20 algorithm block diagram

3.3. Key generation

The logistic map is a polynomial equation which demonstrates chaotic behavior. There are various types of logistic maps including continuous and discrete. One dimensional logistic map which is a discrete time chaotic system for key generation purpose in ChaCha20 algorithm has been considered. The following equation demonstrates the one-dimensional logistic map [21]:

$$X_{n+1} = r\, X_n (1 - X_n) \quad (5)$$

here, r is the system parameter and it takes value between 3.5699 to 4 because for these values the system enters into chaos. Figure 4 demonstrates value for various "r".

For key generation purpose, the value of *r*=3.99 and initial value *X_0*=0.6 (its value is always between 0 to 1) are considered. As the ChaCha20 algorithm requires 8 number of keys, the first 8 number of values from the sequence generated by the logistic map equation is taken for consideration. For examp le-0.600, 0.958, 0.162, 0.543, 0.990, 0.038, 0.145, 0.496. As each key in ChaCha20 encryption algorithm is 32 bit length, to convert the above values in 32 bit binary value each of them has to be multiplied with (2^{32} -1) equivalent decimal value and then rounded to the nearest possible number. Table 1 demonstrates this.

Table 1. Encryption and decryption key generation process

Chaos value	After Multiplication	After Rounding	Binary
0.600	2576980377	2576980377	10011001100110011001100110011001
0.958	4114578668.61	4114578668	11110101001111101111011101101100
0.162	695784701.79	695784701	00101001011100011010100111111101
0.543	2332167241.18	2332167241	10001011000000100000110001001001
0.990	4252017622.05	4252017622	11111101011000010100011110101110
0.038	163208757.21	163208757	00001001101110100101111000110101
0.145	622770257.775	622770257	00100101000111101011100001010001
0.496	2130303778.32	2130303778	01111110111100111011011001000010

4. RESULTS AND DISCUSSION

The performance of the proposed scheme in terms of its applicability in smart grids electronic devices has been evaluated. The performance is mathematically analyzed in terms of computational energy consumption, processing time and throughput. For mathematical analysis purpose, the hardware is Intel Core Duo CPU 2.13 GHz processor whose operating voltage range is 0.8500V-1.5V, clock cycle or base frequency is 2.13 GHz.

For the aspect of computational energy: this performance metric defines the average amount of energy consumed by a cryptography algorithm when it operates encryption or decryption operation, It is important to analyze energy efficiency as most of the wireless devices are battery powered and suffers from battery power limitation. Thus designing energy efficient security protocols will prolong the lifetime of the devices. To evaluate energy consumption of the proposed scheme and AES, the following equation have been utilised [22]:

$$E = \frac{CC/B}{CC/S} IV \quad (6)$$

where, *CC/B* denotes clock cycles per byte during encryption and decryption. *CS* denotes processors clock cycle. *I* defines current required in total encryption and decryption cycles and finally *V* is the processors operating voltage.

Figure 5 shows the comparison of computational energy consumption of AES and ChaCha20. From the figure, it can be seen that to process 128 Byte data ChaCha20 requires 8 times lower energy than AES that is to process 128 Byte data AES consumes 8 Joules on the otherhand ChaCha20 consumes only 1 Joule of energy.

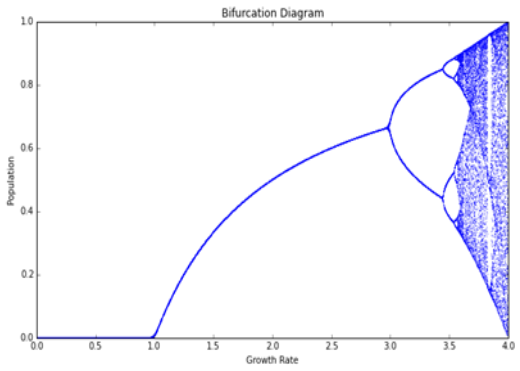


Figure 4. Bifurcation diagram

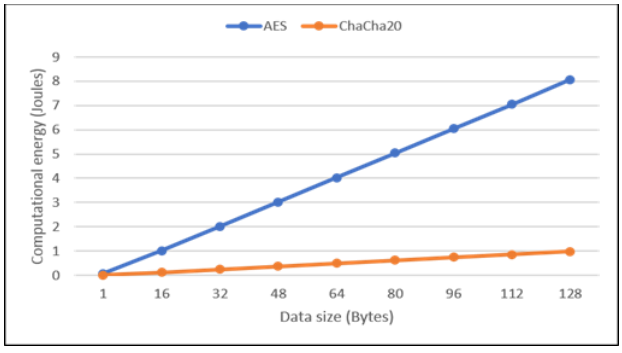


Figure 5. Comparison of energy consumption of AES and ChaCha20

In terms of Processing Time: Processing time defines the time required for the processor to perform encryption or decryption of a particular size of data. Less processing time ensures faster cryptographic schemes. The required time can be calculated as:

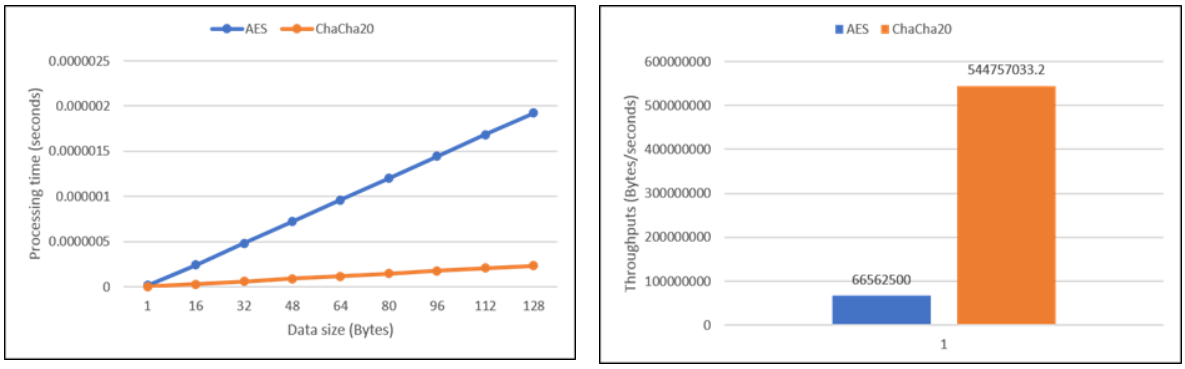
$$t = \frac{Data\ Size}{Speed} \quad (7)$$

$$Speed = \frac{CC/S}{CC/B} \quad (8)$$

where, speed defines bytes per second or throughput. Figure 6(a) demonstrates processing time comparison of the two schemes. It is clear that the processing time has been drastically reduces for ChaCha20 than AES. Throughput refers to the amount of data that a system can process per unit of time. The higher the throughput the better the system performance. Throughput can be modeled through the following equation [23, 24]:

$$Throughput = \frac{Size\ of\ Data}{Encryption\ time} \quad (9)$$

From Figure 6(b) it can be seen that the throughput of ChaCha20 is much higher than AES. The proposed scheme has been compared with AES [25]. In future, the effects of various attacks like wormhole attack, black hole attack, phishing attack [26] on smart grid and their mitigation techniques could be investigated.



(a) (b)

Figure 6. (a) Comparison of processing time of AES and ChaCha20, (b) Throughput comparison of AES and ChaCha20

5. CONCLUSION

In this paper, it has been shown from recent work that the electronic devices along with SM used in SG network are low powered and resource constrained which asserts faster, low processing time, low powered cryptography scheme to secure the network. To meet this demand, a ChaCha20 based lightweight data encryption and decryption scheme to be used in SG network has been proposed. To validate a device as a legitimate device, public key and private key based authentication scheme has also been proposed. Also, to make the existing ChaCha20 encryption method stronger, chaos based random number generation method has been uilized. Based on these random numbers, the ChaCha20 will generate keys and perform cryptography operations. Through mathematical analysis, the proposed method has been proven applicable to be used in SG network which suffices the demands of electronic devices in SG. The proposed protocol is also able to eliminate any kind of timing attacks such as replay attacks as preventing timing attack is an inherent feature of ChaCha20.

ACKNOWLEDGEMENTS

This research has been made possible by the funding from the Ministry of Education Malaysia grant number LRGS/2018/UNITEN-UKM/EWS/04.

REFERENCES

[1] C. Atheeq, Asma Siddiqua, Saba Begum, Muirza Younus A. B., "A review and techniques in smart grid for authentication of messages," *International Journal of Latest Engineering and Management Research (IJLEMR)*, vol. 3, no 3, pp. 91-96, March 2018.

[2] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," in *IEEE Communications Surveys and Tutorials*, vol. 16, no. 4, pp. 1933-1954, Fourthquarter 2014.
[3] X. Fan and G. Gong, "Security challenges in smart-grid metering and control systems," *Technology Innovation Management Review*, vol. 3, no. 7, July 2013.
[4] E. Bou-Harb, C. Fachkha, M. Pourzandi, M. Debbabi, and C. Assi, "Communication security for smart grid distribution networks," *IEEE Communications Magazine*, vol. 51, no. 1, pp. 42-49, January 2013.
[5] L. Wu, J. Wang, S. Zeadally, and D. He, "Anonymous and e cient message authentication scheme for smart grid," *Security and Communication Networks*, vol. 2019, no. 4, pp. 1-12, May 2019.
[6] D. J. Bernstein, "Chacha, a variant of salsa20," in *Workshop Record of SASC*, vol. 8, pp. 3-5, January 2008.
[7] M. Hamdi, R. Rhouma, and S. Belghith, "A very e cient pseudo-random number generator based on chaotic maps and s-box tables," *International Journal of Electronics and Engineering*, vol. 9, no. 2, pp. 481-485, 2015.
[8] A. Alam, "A novel non-cryptographic security services for advanced metering infrastructure in smart grid," *Communications on Applied Electronics (CAE)*, vol. 3, no. 7, pp. 35-39, November 2015.
[9] A. Abdallah and X. Shen, "Lightweight security and privacy preserving scheme for smart grid customer-side networks," *IEEE Transactions on Smart Grid*, vol. 8, no. 3, pp. 1064-1074, May 2017.
[10] I. Doh, J. Lim, and K. Chae, "Secure authentication for structured smart grid system," in *2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, Blumenau, pp. 200-204, 2015.
[11] S. Afrin and S. Mishra, "An anonymized authentication framework for smart metering data privacy," *2016 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, Minneapolis, MN, pp. 1-5, 2016.
[12] D. Ghosh, C. Li, and C. Yang, "A lightweight authentication protocol in smart grid," *International Journal of Network Security*, vol. 20, no. 3, pp. 414-422, May 2018.
[13] Q. Wu and M. Li, "A lightweight authentication protocol for smart grid," in *IOP Conference Series: Earth and Environmental Science*, vol. 234, no. 1, March 2019.
[14] P. Gope and B. Sikdar, "Privacy-aware authenticated key agreement scheme for secure smart grid communication," *IEEE Transactions on Smart Grid*, vol. 10, no. 4, pp. 3953-3962, July 2019.
[15] Y. Chen, J. Mart nez, P. Castillejo, and L. Lopez, "A bilinear map pairing based authentication scheme for smart grid communications: Pauth," *IEEE Access*, vol. 7, pp. 22633-22643, 2019.
[16] K. Mahmood, S. A. Chaudhry, H. Naqvi, S. Kumari, X. Li, and A. K. Sangaiah, "An elliptic curve cryp-tography based lightweight authentication scheme for smart grid communication," *Future Generation Computer Systems*, vol. 81, pp. 557-565, April 2018.
[17] L. F. Roman, P. R. Gondim, and J. Lloret, "Pairing-based authentication protocol for v2g networks in smart grid," *Ad Hoc Networks*, vol. 90, p. 101745, July 2019.
[18] X. Li, F. Wu, S. Kumari, L. Xu, A. K. Sangaiah, and K.-K. R. Choo, "A provably secure and anonymous message authentication scheme for smart grids," *Journal of Parallel and Distributed Computing*, vol. 132, pp. 242-249, October 2019.
[19] Gao, Jingcheng and Xiao, Yang and Liu, Jing and Liang, Wei and Chen, CL Philip, "A survey of communication/networking in Smart Grids," *Future generation computer systems*, vol. 28, no. 2, pp. 391-404, February 2012.
[20] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Computer networks*, vol. 57, no. 5, pp. 1344-1371, April 2013.
[21] H. Al-Mashhadi, H. Abdul wahab, and R. Hassan, "Chaotic encryption scheme for wireless sensor network's message," 06 2014.
[22] A. Ahmad, A. Swidan, and R. Saifan, "Comparative analysis of di erent encryption techniques in mobile ad hoc networks (manets)," *International journal of Computer Networks and Communications (IJCNC)*, vol. 8, no. 2, pp. 89-101, April 2016.
[23] D. Salama, H. A. Kader, and M. Hadhoud, "Studying the e ects of most common encryption algo-rithms," *International Arab Journal of e-Technology*, vol. 2, no. 1, pp. 1-10, January 2011.
[24] N. Kumar and P. Chaudhary, "Performance evaluation of encryptiondecryption mechanisms to enhance data security," *Indian Journal of Science and Technology*, vol. 9, no. 20, pp. 1-10, May 2016.
[25] Gamido, Heidilyn V. and Gamido, Marlon V. and Sison, Ariel M., "Developing a secured image file management system using modified AES," *Bulletin of Electrical Engineering and Informatics*, vol. 8, no.4, pp.1461-1467, December 2019.
[26] Jupin, John Arthur and Sutikno, Tole and Ismail, Mohd Arfian and Mohamad, Mohd Saberi and Kasim, Shahreen and Stiawan, Deris, "Review of the machine learning methods in the classification of phishing attack," *Bulletin of Electrical Engineering and Informatics*, vol. 8, no.4, pp. 1545-1555, December 2019.