The Best Performance Evaluation of Encryption Algorithms to Reduce Power Consumption in WSN

Mustafa A. Al Sibahee[1], Songfeng Lu[1], Mohammed Abdulridha Hussain [3], Keyan Abdul-Aziz Mutlaq[3], Zaid Alaa Hussien [2], Zaid Ameen Abduljabbar [3]
[1]School of Computer Science and Technology
Huazhong University of Science and Technology, Wuhan, 430074, China
[2]Southern Technical University, Basrah, Iraq.
[3]University of Basrah, Basrah, Iraq
MUSTAFA.A@hust.edu.cn , lusongfeng@hust.edu.cn

***Abstract*— Wireless Sensor Networks (WSNs), applications are growing rapidly, so the needs to protect such applications are increased. Cryptography plays a main role in information system security where encryption algorithm is the essential component of the security. On the other side, those algorithms consume a significant amount of computing resources such as CPU time, memory, and battery power. This paper provides evaluation of four of the most common encryption algorithms namely: RC4, DES, and AES as a symmetric cipher and RSA for asymmetric cipher. A comparison has been conducted for those encryption algorithms at different settings such as different sizes of data blocks, different key size and finally encryption/decryption speed. Simulation results are given to demonstrate the effectiveness of each algorithm on power consuming.**

Keywords- Encryption techniques, power consumption, WSN security.

I. INTRODUCTION

Wireless sensor networks (WSN) are used to monitor environmental and physical changes by means of sensor nodes[1]. Which are becoming a popular ubiquitous computing. They are used in different applications such as health care monitoring, environmental/earth sensing, air pollution monitoring, forest fire detection, industrial monitoring and many more. Since there are only limited resources, WSNs are exposed to many vulnerable attacks such as false message injection, eavesdropping etc., hence more security measures are needed. In recent times many techniques such as random key pre-distribution and random pairwise key distribution has been used. The security in WSN has been enhanced by using a symmetric key encryption technique. The pros and cons of the issues related to WSN have been put forth discussed, compared and evaluated in this research. Cryptographic is a set of algorithms operate in a way to encrypt and decrypt data. Encryption is transform plaintext to cipher text to serve security purposes. Whereas decryption is transform cipher text to plaintext that is the reverse operation of the encryption. Cryptography is divided in to two main category symmetric and asymmetric algorithms. Symmetric is using a same key for encryption and decryption by both sender and receiver .The challenge is how to security shared the key between the pairing nodes. WSN method for key distribution is by saving the key using offline phase , in other words , storing the key before the node operate . The drawback of this method is the static key value .while symmetric is preferred because low cost and high speed computation [5].

In order to optimize the conventional security algorithms for WSNs, it is necessary to be aware about the constraints of sensor nodes [2]. The major constraints of a WSN are Energy constraints. Energy is the biggest constraint for a WSN. In general, energy consumption in sensor nodes can be categorized in three parts: (i) energy for the sensor transducer, (ii) energy for communication among sensor nodes, and (iii) energy for microprocessor computation. According to the study in [3].one bit transmit with in WSN media will consumes power more than execution about 800 to 1000 instruction in WSN node. The consolation from such study is lead to reduce the communication messages size to save energy.

Security message data may results increasing data size spirally when using complex cryptography algorithms such as PKI. As mentioned above complicated mechanisms will directly effects the system power consuming.

The objective in this Paper is presenting varies security methods from power consuming point of view and the main contribution in WSN field as follow:

- We demonstrate the relationship between different security algorithm and power consumption.
- We measured the execution times for nods communication when using different security algorithms to recognize the best security algorithms to prolong power consumption.
- The affrication of distance between nods on power is presented in our work.
- To explain is there any impact on power by using different plaintext size.

The rest of this paper is organized as follows. Section II presents the related works conducted in the area of power consumption in WSN Security. Section III demonstrates the simulation scheme. Section IV introduces the experimental and evaluation results. Section V concludes the paper.

II. RELATED WORK

The cost of encryption on wireless sensor node has attention of many researchers as explained in the following paragraphs. Lee, Kapitanova, and Son [8] analyze several symmetric algorithms and message authentication code algorithms in the context of WSNs. MicaZ and TelosB sensor nodes has been used and measure the execution time and energy consumption for number of algorithms. The AES measured in hardware level implementation using a single block which shows the best results in either time or energy. While Zhang, Dojen, Coffey [10] tries different AES block length on MicaZ node without account the distance measuring. They conclude that hardware assisted encryption is faster, but also consumes more energy due to the external chip which handles the computation in hardware.

In [7] Law, Doumen, and Hartel, conduct a thorough survey of the costs of different block ciphers, by hardware implemented on sensor node. They conclude that Rijndael (AES) is the second most efficient cipher, being surpassed only by Skipjack. However, their analysis is based on older hardware and does not consider any hardware accelerated implementations.

Meulenaer, Gosset, Standaert, and Bereira [6] study the problem of key exchange and measure the cost of two key agreement protocols: Kerberos and Elliptic Curve Diffie-Hellman. The energy consumption of the two protocols is measured on MicaZ and TelosB sensor nodes. The conclusion is the listening mode is the principal factor in the energy efficiency of key exchange protocols, with Kerberos being the more efficient protocol. While our concentration on the securing message transformation in the WSN media and such objective is tested on a number of cryptographic algorithms.

Panait and Dragomir [9] compare the performance and energy consumption to four block cipher operation mode using AES algorithm. The modes are ECB, CBC, CFB and CTR. The same authors in [11] add the fifth block cipher operation mode to compare with. While our work compare among different algorithms to find the best power conception.

III. SIMULATION SCHEME

Cryptography Support a huge number of cipher algorithms to secure node communication. Our scheme is to select the suitable security algorithm in WSN, according to power conception perspective.

Power consumption in WSN based on three factors .As shown in Fig.1. The first factor is the transmission power which is depending on data size to be transmitted and the distance to carry this data according in (1).

The second factor is the receiving power; however the receiving power is depending on the packet size only. As demonstrated in (2).

The final factor is the power consumes by the WSN processor, in other words, the computation power consuming which is based on number of instructions excited in the CPU, as explain in (3).

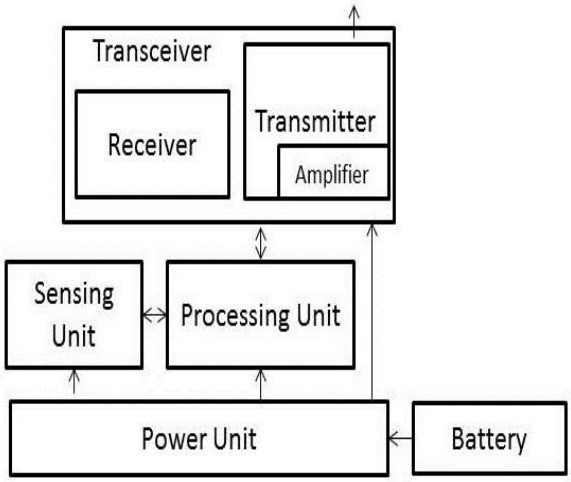


Figure 1. Senosr Node Structure

$$E_t(k,d) = E_{elec}K + G_{amp}kd^2 \quad (1)$$

$$E_r(k) = E_{elec}K \quad (2)$$

$$E_c = E_{inst} \times I \quad (3)$$

A case study used ARM9TDMI, processor in our simulation scheme where the processor consume 1.125Nj/instructions and the other quotations constant value shown in table 1. [12, 13].

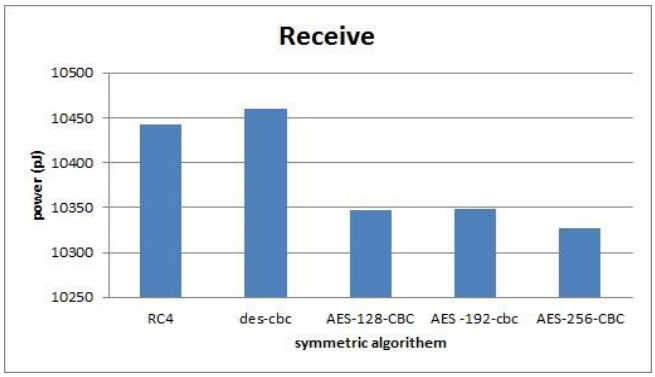
TABLE I. CONSTANT VALUES

Constant	Value
E_{elec}	50 nJ / bit
G_{amp}	100 pJ/bit/m^2
E_{inst}	1.125 nJ/instruction

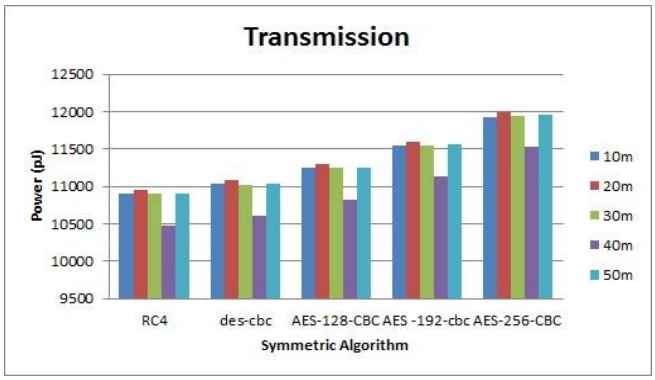
IV. EXPERIMENTAL AND EVALUATION RESULTS

The will-known Cryptography algorithms are measured in this experiment for both symmetric and asymmetric cipher technology for code optimization and faire judgment. We utilized from OpenSSL packet [14], RC4, DES, AES and RSA. Demonstrate an approximately computation cost the experiment use the mentioned algorithms for different key size and under Cipher Block Chaining (CBC) mode for block cipher algorithms. The number of tractions counted for encryption and decryption to all the mentioned algorithms taking in to account plaintext size.

The distance between two nodes has been veering to evaluate the effect on the source node transmission power. While different plaintext size to measure the effect on transmission and power for the source and the receiving power for distribution nods .Moreover, we assumed WSN pirate using IEEE802.11, which has coverage range up to 50m.Inour experiment we execute for (10, 20, 30, 40 and 50m).



(a)



(b)

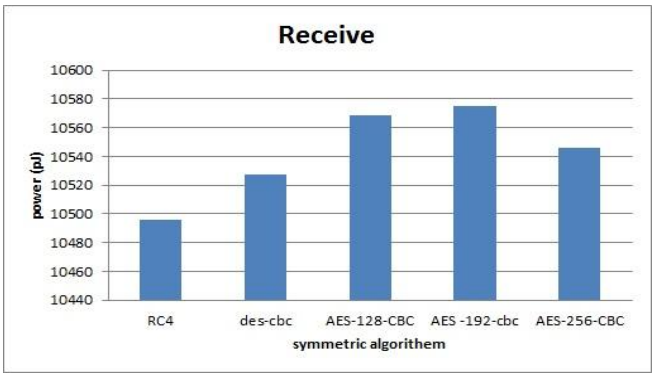
Figure 2. Average power consumption using plaintext 512 Byte

Fig. 2, shows the power average rate of sent and received packets of five protocols in wsn security using 512 byte plaintext .The power counsumption of every protocols affected by the presence of encryption and decryption packet.we can observe from the figure (a)that DES-CBC and RC4 protocols has highest power rate(PJ). We also observed that the power rate was lesser than in the other three protocols of the decryption power.

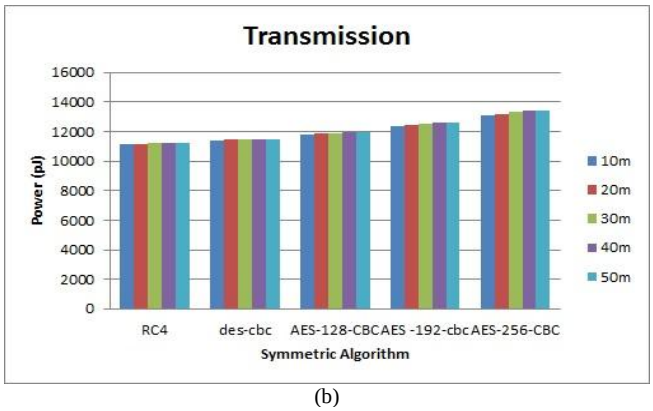
Fig. 2, the received power computed by combining the result of (2) and (3), however plaintext size is fixed for all algorithems that make the reason of such diffrens behind the number of instraction for the decraption proceger. We can observe from Fig. 2(b), RC4 is the lowest power consumes and AES-256 is the highest one.

Fig. 3(b), shows a small different in power consume between algorithms. When we are change the plaintext from 512 to 1k .even the distance has been changed, because the plaintext size is constant this lead the different courses by number of instructions. We also can observe from the receive Fig. 3(a) that AES-128and AES -192 protocols has height power consume .The reason behind this result is 1k plaintext will increase number of instruction performed in the CPU.

The result behind changing the plaintext size to 2k byte demonstrates in Fig.4 (a) where RC4 and AES-192 is highest power conception. While in fig. 4(b), seems the distance has no effects on the transmission power consuming.

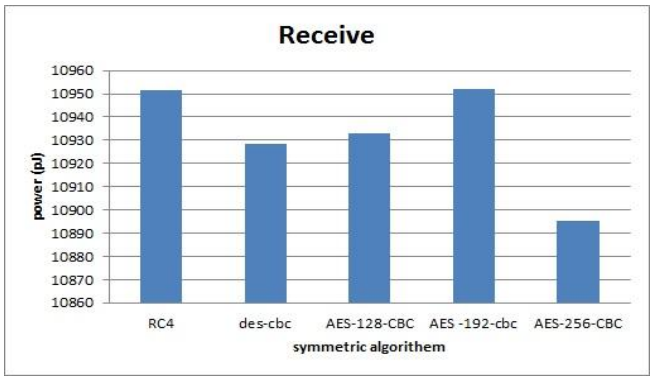


(a)

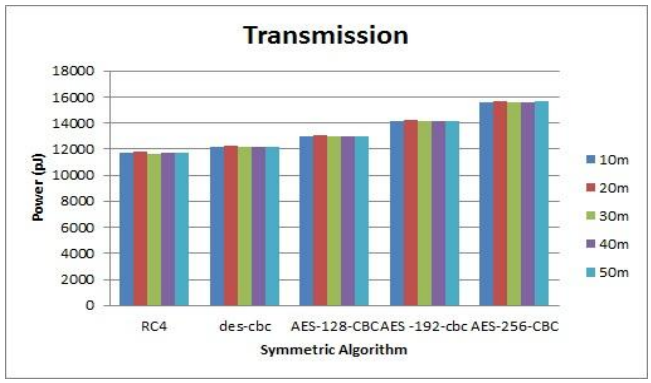


(b)

Figure 3. Average power consumption using plaintext 1K Byte

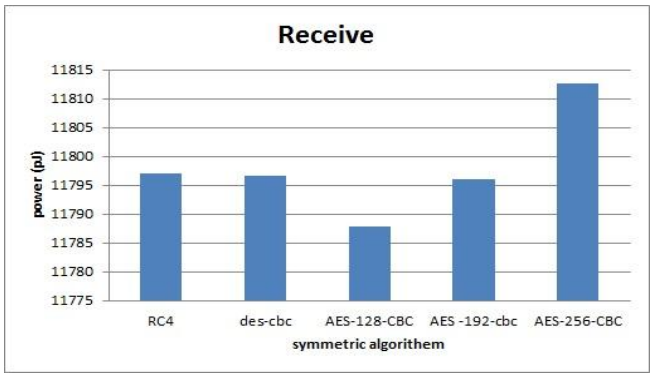


(a)

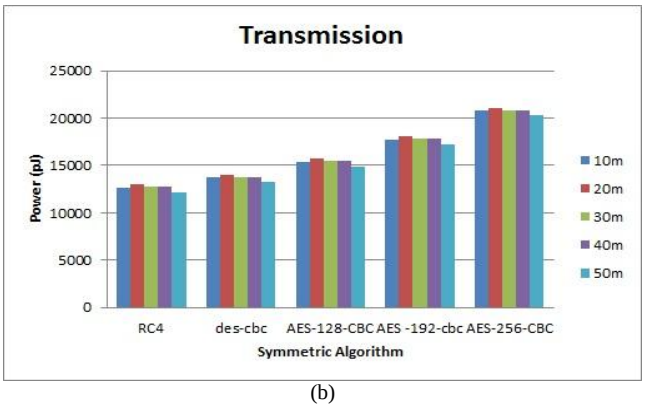


(b)

Figure 4. Average power consumption using plaintext 2K Byte

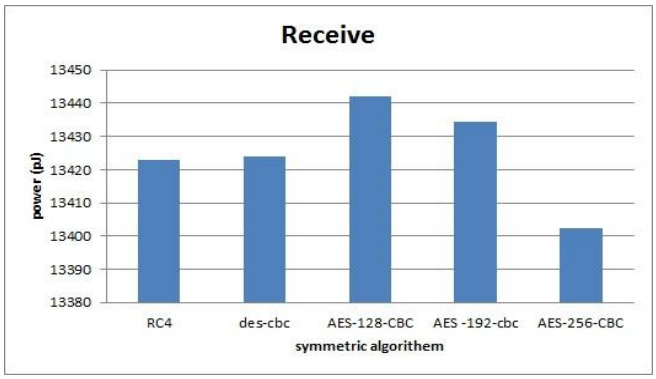


(a)

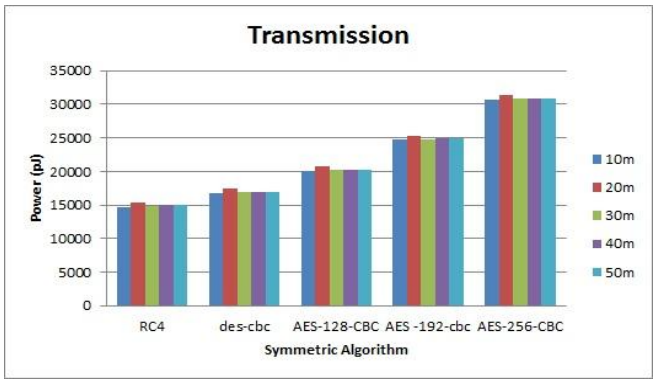


(b)

Figure 5. Average power consumption using plaintext 4K Byte



(a)



(b)

Figure 6. Average power consumption using plaintext 8K Byte

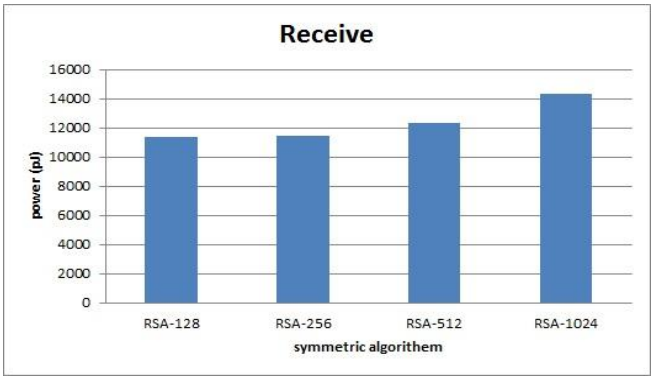
Fig. 5 (b), continue showing RC4 is the lowest power consuming .even the plaintext size change to 4k. However Fig. 5 (a), observes AES-256, is highest in power consuming.

Fig. 6(a) shows similar pattern with Fig. 2 but the power consume vale it's different, which means more instruction in the decryption producer by using 8k byte by plaintext. However Fig. 6(b) proved that RC4 its keep the average lost power consuming.

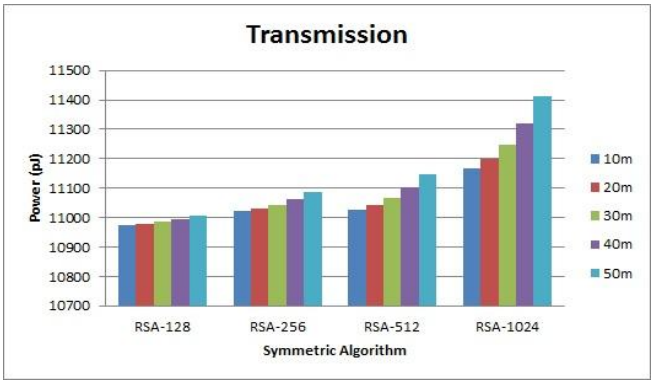
Finally, Fig. 6 shows the RSA Algorithm about four key (128,256,512 and 1024) while the plaintext size used 5 byte. Obviously RSA 128 has lowest power consume value and RSA-1024 has the highest consume power.

In general after the evaluation the result RC4 is the lowest power consuming in all cases. While AES is the highest power consuming value and obviously AES-128 has the lowest value comparing with AES-256.

The increasing power consuming among encryption algorithm is depending on the plaintext size, which will directly affects transmitting power and the number of instructions to be encryption. The distance sprite between two nodes has a small effect on the transmission power by comparing the power consume using RSA with symmetric cipher. We discover the asymmetric cipher techniques will drain WSN battery life.



(a)



(b)

Figure 7. The effect of changing key size of RSA on power consumption.

V. CONCLUSION

Wireless sensor networks power conception based on transmission message security. This paper presents new simulation for four cryptography algorithms are simulated to eliminate the encryption and distance issue. We conclude from our result that power consuming is depending on the nature of the cipher algorithm because the algorithm defined the number of instructions executed. The size of data have a direct effect on power consuming because increasing data will increase the instructions executed and size of the message to be transfer. While the distance has a small impact on power consuming in WSN.

Encryption power usage increases in a massive way by using asymmetric ciphers which is because rising computational power. Our simulation experiments show that RC4 performs better than other encryption algorithm in power consumption point of view by prolonging network lifetime. In another hand we can observe that RSA-128 its better than other RSA protocols for both of Receive and Transmission from power consuming perspective. The preferable cipher technique is the simplest algorithm in symmetric cipher and to achieve security in WSN we suggest updating the key periodically.

ACKNOWLEDGMENT

The Natural Science Foundation of Hubei Province under (Grant No. 2016CFB541) and the Applied Basic Research Program of Wuhan Science and Technology Bureau under (Grant No. 2016010101010003)

REFERENCES

[1] F. Gandino, R. Ferrero, and M. Rebaudengo, "A Key Distribution Scheme for Mobile Wireless Sensor Networks: q-s composite," Information Forensics and Security, vol. 12, Jan. 2017, pp. 34-47, doi: 10.1109/TIFS.2016.2601061.

[2] S. Slijepcevic, M. Potkonjak, V. Tsiatsis, S. Zimbeck, and M.B. Srivastava, "On communication security in wireless ad-hoc sensor networks," Proc. of the 11th IEEE International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE 02), IEEE Press, June 2002, pp. 139-144, doi: 10.1109/ENABL.2002.1030000.

[3] L. Yuan and G. Qu, "Design space exploration for energy-efficient secure sensor networks," Proc. IEEE International Conference on Application-Specific Systems, Architectures, and Processors (ICASSAP 02), IEEE Press, July 2002, pp. 88-100. doi: 10.1109/ASAP.2002.1030707.

[4] S. Seo, J. Won, S. Sultana, and E. Bertino, "Effective key management in dynamic wireless sensor networks," Information Forensics Security, vol. 10, Feb. 2015, pp. 371-383, doi: 10.1109/TIFS.2014.2375555.

[5] D. Yum and P. Lee, "Exact formulae for resilience in random key pre-distribution schemes," Wireless Communication, vol. 11, May 2012, pp. 1638-1642, doi: 10.1109/TWC.2012.031212.110887.

[6] G. Meulenaer, F. Gosset, O. Standaert, and O. Pereira, "On the energy cost of communication and cryptography in wireless sensor networks," Proc. IEEE International Conference on Wireless and Mobile Computing Networking and Communications (WIMOB 08), IEEE Press, Oct. 2008, pp. 580–585, doi: 10.1109/WiMob.2008.16.

[7] Y. Law, J. Doumen, and P. Hartel, "Survey and benchmark of block ciphers for wireless sensor networks," Sensor Network. vol. 2, Feb. 2006, pp. 65-93, doi: 10.1145/1138127.1138130.

[8] J. Lee, K. Kapitanova, and S. Son, "The price of security in wireless sensor networks," Computer Network, vol. 54, May 2010, pp. 2967–2978, doi:10.1016/j.comnet.2010.05.011.

[9] C. Panait and D. Dragomir, "Measuring the performance and energy consumption of AES in wireless sensor networks," Proc. Federated Conference on Computer Science and Information Systems (CSIS 15), IEEE Press,, Sept. 2015, pp. 1261–1226, doi: 10.15439/2015F322.

[10] F. Zhang, R. Dojen, and T. Coffey, "Comparative performance and energy consumption analysis of different AES implementations on a wireless sensor network node," Sensor Network, vol. 10, 2011, pp. 192–201, doi:10.1504/IJSNET.2011.042767.

[11] D. Dragomir and C. Panait, "Performance and Energy Consumption Analysis of AES in Wireless Sensor Networks," Proc. Advances in Intelligent Systems and Computing (AISC 16), Springer, Dec. 2016, pp. 181-196, doi: 10.1007/978-3-319-44354-6_11.

[12] A. Moschitta and I. Neri, "Power consumption Assessment in Wireless Sensor Networks," ICT - Energy - Concepts Towards Zero - Power Information and Communication Technology, vol. 9, Feb. 2014, doi: *10.5772/57201.*

[13] J. Castillo, H. Posadas, E. Villar, and M. Martinez, "Energy Consumption Estimation Technique in Embedded Processors with Stable Power Consumption based on Source-Code Operator Energy Figures," Proc. Conference on Design of Circuits and Integrated Systems (DCIS 07), IMSE-CNM, 2007, pp. 1–7.

[14] OpenSSL. https://www.openssl.org/.