International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org, editorijettcs@gmail.com
Volume 11, Issue 6, November –December 2022 ISSN 2278-6856

CRYPTOGRAPHIC ALGORITHM GRAFTED ONTO THE ESP NOW PROTOCOL FOR SECURITY OPTIMIZATION IN WIRELESS SENSOR NETWORK CHAINS

MOTSO CHATUE Laura[1], GAMOM NGOUNOU EWO Roland[2] and NNEME NNEME Leandre[3]

[1]Research laboratory in Computer science and Automation Engineering at ENSET University of Douala, Cameroon

[2] Research laboratory in Computer science and Automation Engineering at ENSET University of Douala, Cameroon

[3] Research laboratory in Computer science and Automation Engineering at ENSET University of Douala, Cameroon

Abstract: ***This article presents a secure routing scheme based on the ESP NOW protocol of ESP32 microcontrollers. In addition to security specific to this protocol, the data transmitted is encapsulated in a symmetric cryptography algorithm based on binary and hash cryptographic functions. A unique encryption and decryption key is used when sending and receiving data. The algorithm is written in C++ program in the form of a library and included in an Arduino sketch. The sensor node calls the library for encryption and the central node uses this same library to decrypt the message received and restore the encrypted information. The tests are carried out on a network made up of two ESP 32, each coupled with a DHT11 sensor which sends the information to a central node for control and monitoring. The results obtained optimize data security in networks based on ESP NOW communication protocols. The goal is to contribute to the reinforcement of data transmission security for a sensor network within a logistics transport chain equipped with temperature and humidity sensors.***

Keywords: wireless sensor network, symmetric cryptography, ESP - NOW, hashing, encryption, decryption.

1. INTRODUCTION

Electronic data interchange is increasing rapidly, thus making it easier to access data [1]. Wireless sensor networks (WSNs) have attracted a lot of interest in recent years. It is expected that WSNs will be applied in our daily life, in healthcare [2], video surveillance, real-time target tracking, and home surveillance [3]. These applications require the deployment of multiple sensors to cover a given region of networking interest, while establishing ubiquitous wireless sensor networks that will pervade society redefining the way we live and work [4]. The proliferation of wireless sensor networks has paved the way for a multitude of research fields which constitute the privileged sites for their deployment. The interest raised by this multitude of investigations creates ideal conditions for large fields of deployment in the near future. Nevertheless, many obstacles inherent in their specificities must be overcome before they can reach maturity. Among these obstacles, the problem of security is acute and must be solved appropriately and in accordance with the particular characteristics of WSNs. These constraining characteristics are observed in the limitation of resources such as: energy, computing power, bandwidth and memory space. Due to these constraints and their deployment in unattended and hostile environments, the various sensor nodes of an WSN are vulnerable to compromise and susceptible to physical breach. Moreover, the use of wireless transmissions makes the WSNs permeable to malevolence of all kinds, and constitutes a real security challenge to be taken up. Having sensors and their applications in the military and business increases the demand to look for ways to secure the flow of data using cryptography which is the technique used to establish secure communication between two parties in the public environment where unauthorized users and malicious attackers are present [5]. Cryptography is a well-known mechanism in which asymmetric or symmetric algorithms using public or private keys provide secure data communication [6]. The purpose of cryptography is to provide confidentiality, authenticity and integrity of data. There are two types of cryptographic techniques, namely symmetric key and asymmetric key [7]. In the first case, two communicating entities share a secret key and messages are encrypted and decrypted at either end using the same key while in the second, each entity has its own private key (secret key) and its public key [7]. Binary encryption [8] much more used in the encryption of images, can help in other areas through its techniques and its operation. Thus, there are many works highlighting cryptography in the WSNs [9],[10],[11],[12],[13]. Although several works have been done in this area, they are less successful in providing both high security and low computational complexity. The cryptography technique chosen for the WSNs must be appropriate to meet the limitations or constraints of the WSNs such as power consumption, memory, as well as the encryption/decryption

times and the lifetime of the WSNs. Some public key cryptographies used in WSNs are the Diffe-Hellman Key Agreement Protocol or RSA [14] signatures. Asymmetric key encryption algorithms help preserve the authenticity and confidentiality of data. However, they are computationally intensive as they consume more energy and power; therefore, symmetric key algorithms are used to encrypt data in WSNs in accordance with the limited power source in the sensor device [15], hence private key cryptography is preferred over public key cryptography [16]. We thus notice an overwhelming use of symmetric cryptography algorithms for WSNs like the AES algorithm. The latter is used in many WSN works. I. Sultan, B. J. Mir, and M. T. Banday in [17] performed a simulation analysis on the effect of changing key size and mode types of AES encryption. The results obtained do not take into account the nature of the transmission media which can considerably affect this result, but also the simulation results obtained, which are far from realistic and practical results. Another article that focuses on the comparison between hardware and software implementation of AES encryption is presented in [18]. In this article, the authors studied the power consumption of the AES algorithm for different modes. However, neither the effect of changing the key size, nor the effect of the communication media or the encryption done by the wireless module on the energy consumption has been studied. Other works like those of [19] make AES software optimization modifications where the main objective was to propose an optimized code capable of encrypting/decrypting information at a speed comparable to the speed of the communication module. ZigBee (close to 250 Kbps). The interest of this article is to contribute to the literature by implementing a lightweight symmetric cryptography algorithm comparable to AES, consuming less resource and memory, for data security and optimization of data transmission and reception times. In our particular case, we will focus on the ESP- NOW transmission protocol on which our algorithm will be grafted in order to optimize the level of security. We therefore propose a custom algorithm for WSN that will ensure data confidentiality by protecting the network against various attacks thanks to a double security algorithm. Obviously, this research will enrich the literature on data security. The rest of the article is organized as follows: the second section presents the architecture of the proposed system; the third section presents the results and the analysis of the security performances and then a conclusion.

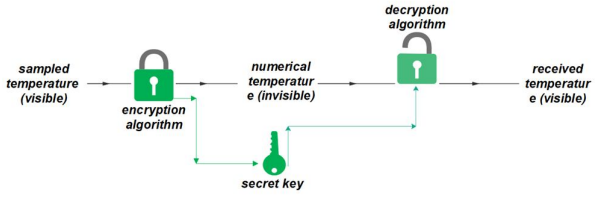

Figure 1 Symmetric Cryptography.

2. ARCHITECTURE OF THE PROPOSED SYSTEM

2.1 The proposed Solution

To overcome the problem of securing communications within wireless sensor networks, we propose in this article an encryption/decryption algorithm based on symmetric cryptography with a unique encryption/decryption key, which constitutes one of its fundamental concepts. We apply this security within a network of wireless sensors based on the ESP_NOW protocol of ESP32 microcontrollers by *Espressif* for real-time monitoring of the temperature and humidity parameters of a supply chain.

2.2 Hardware

2.2.1 ESP32

ESP32 is a low-cost microcontroller which succeeded to the famous ESP8266 designed in 2016 by Espressif System. This microcontroller has proven its capability for Wi-Fi-automation as a working solution. This controller features a variety of its company's features and supports to be adopted for a wide range of applications ranging from IoT to audio streaming. Thus, its specifications offer an extreme arsenal for programmers with a 240 MHz dual core, 520 KB of RAM and peripherals including ADC, DAC, I2C, UART, SPI, GPIO and costing only $10. Additionally, the power management unit and ultra-low-power coprocessor enable ESP32 to operate at 1mA in hibernate mode. These features make ESP 32 an excellent choice for low power applications. In terms of usability, ESP32 can be programmed on several development tools such as Arduino-IDE, AT command or by using Espressif's officially open development framework based on FreeRTOS [20].

2.2.2 DHT11

The microcontroller measures temperature from the digital integrated circuit (DIC) sensor DHT11 which detects the humidity and temperature of the environment. This sensor can measure a temperature range of 0°C to 50°C and a humidity range of 20% to 90% with an accuracy of ±1°C and ±1% [21]. It works with operating voltages from 3.5 V to 5.5 V and operating currents up to 0.3 mA. The DHT11 sensor module gives the measured temperature value in Celsius degrees. When an ambient temperature increases by one degree Celsius, the sensor generates a voltage of 10 mV. Figure 3 shows the schematic diagram of the proposed system on the sensor node side.

2.3 The ESP-NOW protocol

ESP-NOW [22] is a kind of connectionless communication protocol defined by Espressif. Compared to normal Wi-Fi, this method is more energy efficient and faster to deploy with a range of 200 to 220 meters outdoors. Inside the ESP-NOW network, all devices can

communicate by 3 main methods: broadcast, unicast and multicast with a data rate of 1 Mbps and above. While unicast and multicast require initial pairing, acknowledgment response and a limited number of receivers up to 20[20], in this protocol application data is encapsulated in a vendor-specific action frame and then transmitted from one Wi-Fi device to another without a connection. The CTR with the CBC-MAC protocol (CCMP) is used to protect the action framework for security. The format of the vendor-specific action framework is shown in Figure 2.

Figure 2: ESP-NOW Protocol Frame Format.

This frame is transmitted by ESP-NOW using the CCMP security method, which is described in IEEE Std. 802.11-2012, to protect the vendor-specific action framework. The Wi-Fi device maintains a master key (PMK) and several local master keys (LMK). The lengths of PMK and LMK are 16 bytes.

- PMK is used to encrypt LMK with AES 128 algorithm.

Call `esp_now_set_pmk ()` to set PMK. If PMK is not defined, a default PMK will be used.

- LMK of paired device is used to encrypt vendor-specific action frame with CCMP method.

The maximum number of different LMKs is six. If the paired device's LMK is not set, the vendor-specific action frame will not be encrypted.
Multicast provider-specific action frame encryption is not supported.

2.4 Description of the proposed algorithm

The algorithm we propose is based on the principles of binary cryptography and cryptographic hash leading to a condensed message which corresponds to a fixed size on 10 bits. Like any symmetric algorithm, it consists of a unique 8-bit secret key present in the encryption and decryption programs. The encryption process is as follows:

- Sampling of encrypted value. It is a real variable with two decimal places. Example ***n.m*** degrees Celsius for a temperature value. **n** being the whole part and **m** the decimal part. They are numbered identically. $n.m = n + m*10^{-2}$
- We define an 8-bit binary key. Key = 173 or $(10101101)_2$ in binary
- We define $(k)_2$ as the result of the operation $(k)_2 = \overline{(n)_2 \; \boldsymbol{XOR} \; (key)_2}$ coded on 8 bits.
- So we have $(k)_2 = (a_7a_6a_5a_4a_3a_2a_1a_0)$ $avec$ $a \in \{0,1\}$
- k being on 8 bits, we decide to dissect it into sections of two-two bits going from LSB to MSB, knowing that on two bits the maximum value is $(2^2 - 1) = 11$. We obtain numbers belonging to $\{00, 01, 10, 11\}$ and decide to set up the following correspondences:

$$\begin{cases} \mathbf{00} = \text{"\$"} \\ \mathbf{01} = \text{"@"} \\ \mathbf{10} = \text{" \#"} \\ \mathbf{11} = \text{"\%"} \end{cases}$$

- Depending on the correspondences with k, these values enable us to obtain a new 4-bit character string type variable defined as follows:

$$\boldsymbol{m} = \sum_{i=0}^{3} \boldsymbol{a_i} \quad (1)$$

. We define a 15-element string array as follows:
Tab = {**"1"**, **"^"**, **"+"**, **"*"**, **"4"**, **"/"**, **"-"**, **"&"**, **"_"**, **"="**, **"]"**, **"{"**, **">"**, **"."**, **":"**}.

- The final value will include a combination of the values of **m** with those of the preceding array according to an algorithmically defined hash function.
- The decryption process works according to a decomposition of the string received during the encryption of the data which will lead to integer values which will be combined by identification of the whole and decimal parts as shown in Figure 7.

2.5 System Implementation

Our task consists in networking several communicating sensor nodes with a master node which is the point of reception and monitoring of the various data that can be stored in a database or routed on a website for example. The sensor is responsible for acquiring data which is then transmitted to the microcontroller, and then to the central node via the ESP_NOW protocol. We therefore have the diagrams of the figures which present the synoptic architecture of the points of our network.

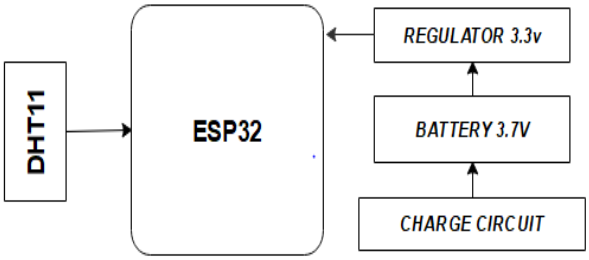

Figure 3 Sensor node diagram.

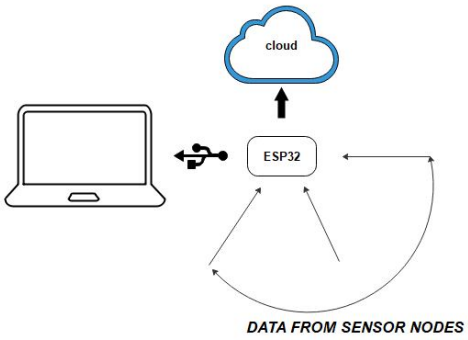

Figure 4 Central node with monitoring possibilities.

Communication from one node to another is done through the protocol. Establishing this communication requires to set the code to be transmitted in the ESP32 microcontroller and this by including the esp_now.h library. The sensor nodes couple to the central node by adding its mac address to their code. A node that does not have the mac address of the central node cannot therefore communicate with it.

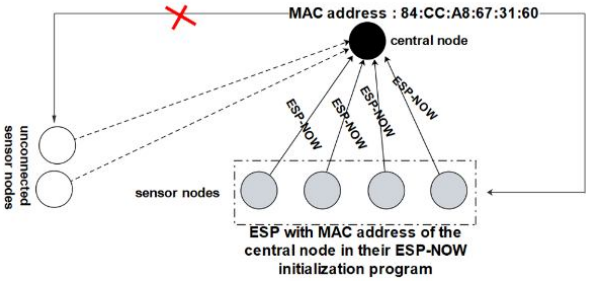

Figure 5: Process of connecting nodes in the network.

Since a level of security is already included in the protocol, we add an algorithm to it. This algorithm is responsible for strengthening it in order to make our system more robust against external attacks. The data being encapsulated in the frame format, the diagram of the level of security is illustrated in Figure 3.

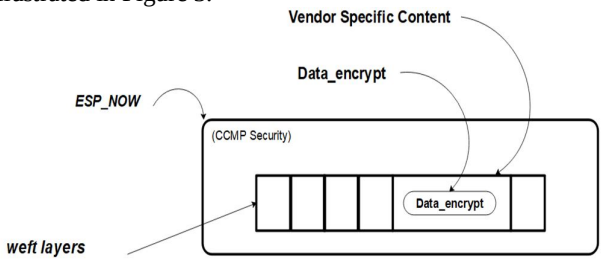

Figure 6 Level of communication security in the designed network.

In this illustration Data_encrypt represents the outgoing data of the encryption algorithm. It will be decrypted upon receipt thanks to a secret key in the receiving node (or central node) decryption program which is responsible for monitoring all the nodes.

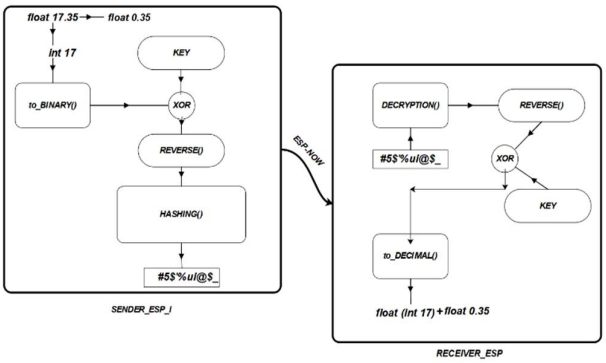

Figure 7 Algorithmic description of encryption and decryption processes in the transmission network from a sensor node to the central node.

The general architecture of the communication flow is presented in the figure below. As shown in figure 5, it is possible to add nodes in the circuit, the communication process will remain the same as well as the established security.

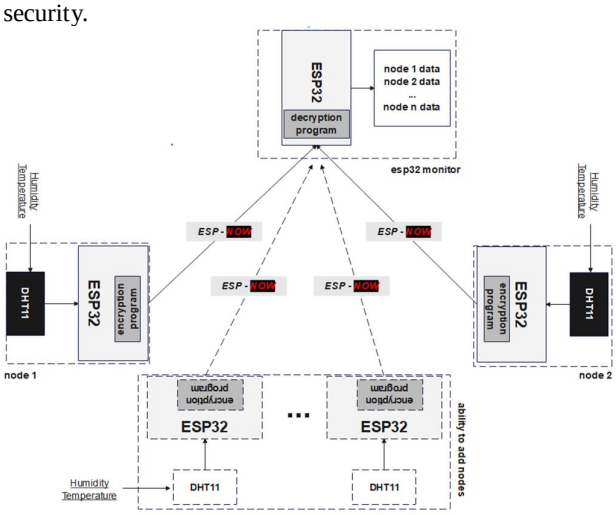

Figure 8 functional scheme.

3. Results And Analysis Of Safety Performances

The algorithm is developed in C++ language and individually tested in console in a GCC compiler. Random values are included in the code, then they are encrypted and decrypted through the functions of a category described beforehand. The figure describes the process in a console window correctly because the input data is the same as that found at the end.

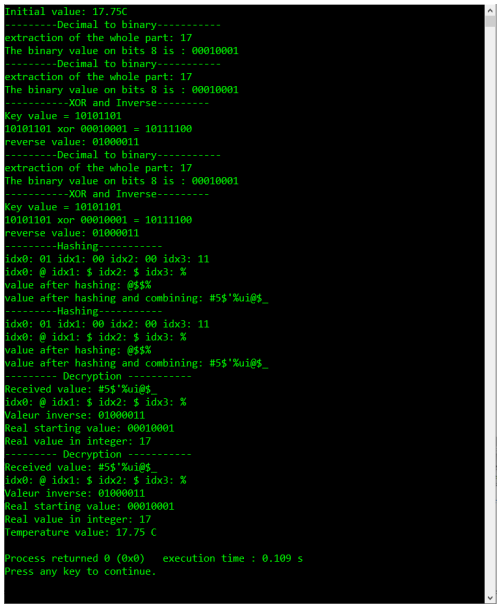

Figure 9 encryption/decryption in programming language C++.

This algorithm is then adapted in the form of an Arduino library and then included locally (#include "Crypto.h") in the sketch. We thus have three programs which are: a **Crypto.h** header file, **cryptoCPP.cpp** and a **cryptoSender.ino** file.

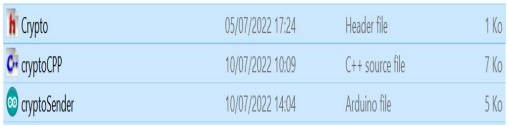

Figure 10 Programming Files.

The network consists of two sender nodes which send data to the central node. We can see according to figures 10, 11 and 12 that we have 3 levels of encryption. First of all the data is taken from the DHT11 sensor, then it is sent to the first level of encryption which constitutes the basis of our algorithm. In fact, our algorithm is based on binary encryption and makes it possible to implement symmetric cryptography by an XOR operation with the secret key defined. This key is initialized in the program and cannot be modified by an external user. Levels 2 and 3 are based on cryptographic hash functions. They result from a message with a size of 4 bytes which is combined with a set of characters. A random function is executed 6 times randomly in the character set defined in section II.3 to form the final digest. The latter will be made up of 10 characters also having a size of 4 bytes, thus very far from the threshold of the transport payload supported by protocol (250 bytes [14]).

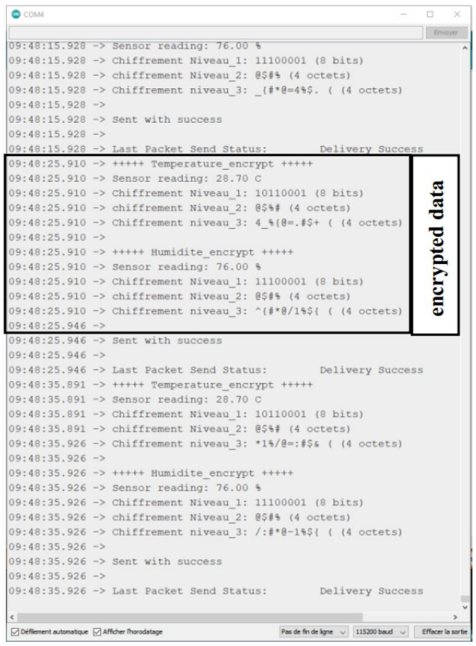

Figure 11: Node 1 data.

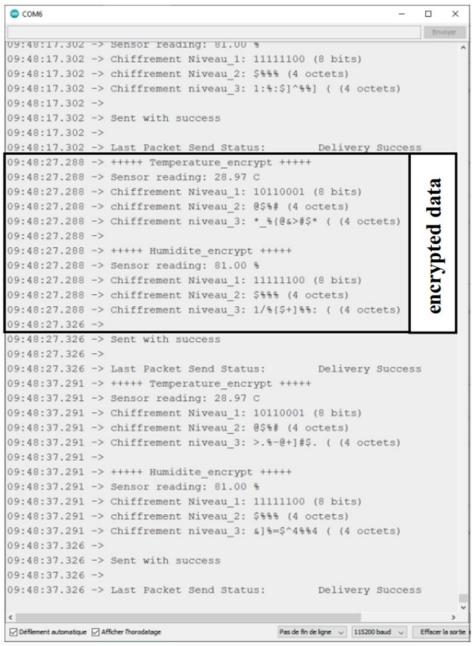

Figure 12: Node 2 data.

Figures 6 and 7 clearly show the process described with the sending times, then the same data is found in Figure 8. This figure shows the central monitoring node which deciphers the data coming from the network through the protocols established on the different nodes and restores the starting information. At this stage, the data is securely transmitted through the network and can be returned for different uses such as monitoring some remote parameters such as temperature, humidity, CO2 rate, etc. in farms or in supply chains (the subject matter of this research) or even in e-

textiles and many other fields requiring remote monitoring and above all, total safety.

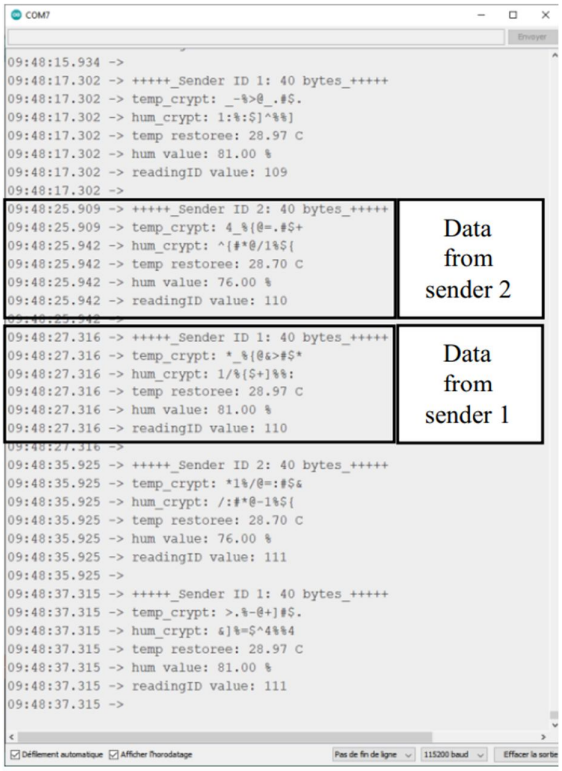

Figure 13: Central node data (monitor node).

As mentioned earlier in this article and demonstrated in section II. 3, the first level of security remains that of the ESP_NOW protocol in which we graft our algorithm. The inclusion of the library increases the size of the binary program in memory which takes up more space. Nevertheless, as shown in Figure 9, we are still very far from the maximum size of the program in the memory of ESP 32.

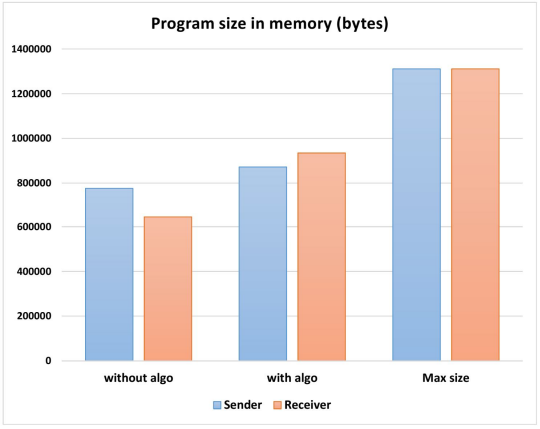

Figure 14: Program size in memory.

Before being sent, the data is encrypted using a hash function combined with a Radom-type function which is responsible of choosing special characters from the defined table. The same data sampled at different time intervals does not have the same final encryption signature (C3 in the table), which is a robustness criterion likely to make the system more reliable against external attacks.

Table 1: Encryption of temperature values taken from node 1 at different time intervals

NODE 1			
Temp	**C1**	**C2**	**C3**
28.50	10110001	@$%#	=/%*@::#$:
29.00	10110000	$$%#	&=% :$1]#$&
29.00	10110000	$$%#	*_%+$_=#${
29.00	10110000	$$%#	++%1$>{#$=
30.20	10110011	%$%#	=>%_% ^^#$

The encryption of our algorithm is comparable to that of [24], we notice a similarity in the final message obtained. A second remark is about the data transmission time which is in milliseconds with a maximum time not exceeding 3500 microseconds as shown in the figure (where N1 represents node 1 and N2 is node 2). The deviations in the transmission times also show how instruction processing is very fast, which makes it possible to perform transmissions in very short times. For example data 2 and 3 of N1 are transmitted respectively in 2936 microseconds and 2935 microseconds. We thus end up with a robust and light algorithm consuming little resource.

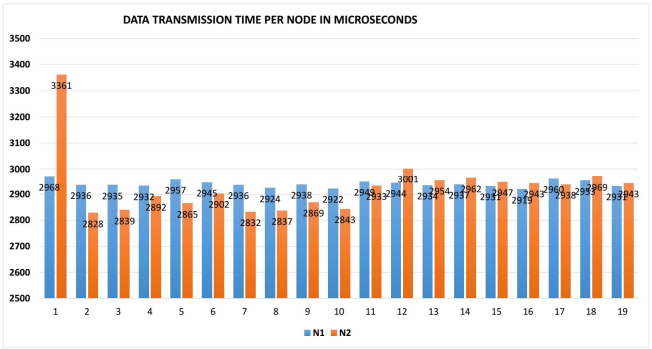

Figure 15: Data transmission time per node (N1 for node 1 and N2 for node 2).

The data is well transmitted and secure thanks to a light algorithm, consuming very little resource.

4. CONCLUSION

In this article, we mainly present the design of a security algorithm based on symmetric cryptography. Starting from the ESP_NOW protocol secure routing process, we graft our algorithm into this chain, which makes the system more complex, with two levels of encryption/decryption. The goal was to set up an algorithm less complex than those of asymmetric cryptography, consuming few resources while keeping its efficiency on the security side. The major novelty of this work lies on the double security of information transmission in the network. We start first with the AES 128 security specific to the

ESP-NOW protocol, from there we add our own algorithm and the results are quite satisfactory. The algorithm being written in the form of an Arduino library, it can be used with any kind of microcontroller compatible with Arduino software. Adding the algorithm to the original transmission system does not negatively impact data transmission; and the processor's processing time remains maximum. So the network remains very stable and doubly secure. It should also be noted that the algorithm written in the form of a library is portable and can be used in fields such as health (monitoring of health constants, connected devices), agriculture or surveillance.

References

[1] A. Nag *et al.*, « Image encryption using affine transform and XOR operation », in *2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies*, Thuckalay, Tamil Nadu, India, juill. 2011, p. 309-312. doi: 10.1109/ICSCCN.2011.6024565.

[2] D. He, N. Kumar, J. Chen, C.-C. Lee, N. Chilamkurti, et S.-S. Yeo, « Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks », *Multimed. Syst.*, vol. 21, nº 1, p. 49-60, févr. 2015, doi: 10.1007/s00530-013-0346-9.

[3] N. Abbas et F. Yu, « Design and Implementation of a Video Surveillance System for Linear Wireless Multimedia Sensor Networks », in *2018 IEEE 3rd International Conference on Image, Vision and Computing (ICIVC)*, Chongqing, juin 2018, p. 524-527. doi: 10.1109/ICIVC.2018.8492776.

[4] M. F. Munir, « Wireless Sensor and Sensor-Actuator Networks: Research Trends, Protocols, and Applications », in *2008 IEEE International Networking and Communications Conference*, mai 2008, p. 6-6. doi: 10.1109/INCC.2008.4562673.

[5] H. R. Pawar et D. G. Harkut, « Classical and Quantum Cryptography for Image Encryption & Decryption », in *2018 International Conference on Research in Intelligent and Computing in Engineering (RICE)*, San Salvador, août 2018, p. 1-4. doi: 10.1109/RICE.2018.8509035.

[6] B. OzCakmak, A. OzbIlen, U. YavanoGlu, et K. CIn, « Neural and Quantum Cryptography in Big Data: A Review », in *2019 IEEE International Conference on Big Data (Big Data)*, Los Angeles, CA, USA, déc. 2019, p. 2413-2417. doi: 10.1109/BigData47090.2019.9006238.

[7] S. Arora et M. Hussain, « Secure Session Key Sharing Using Symmetric Key Cryptography », in *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Bangalore, sept. 2018, p. 850-855. doi: 10.1109/ICACCI.2018.8554553.

[8] Xin Ge, Bin Lu, Hui Guan, et Kai Zhang, « Differential attack on image encryption algorithm using binary bitplane », in *2015 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)*, Zhangjiajie, China, août 2015, p. 2519-2522. doi: 10.1109/FSKD.2015.7382351.

[9] Ü. Çavuşoğlu et H. Al-Sanabani, « Hafif Sıklet Şifreleme Algoritmalarının Performans Karşılaştırması », *Sak. Univ. J. Comput. Inf. Sci.*, vol. 2, nº 3, Art. nº 3, déc. 2019, doi: 10.35377/saucis.02.03.648493.

[10] W. K. Koo, H. Lee, Y. H. Kim, et D. H. Lee, « Implementation and Analysis of New Lightweight Cryptographic Algorithm Suitable for Wireless Sensor Networks », in *2008 International Conference on Information Security and Assurance (isa 2008)*, Busan, Korea, avr. 2008, p. 73-76. doi: 10.1109/ISA.2008.53.

[11] M. Panda, « Data security in wireless sensor networks via AES algorithm », in *2015 IEEE 9th International Conference on Intelligent Systems and Control (ISCO)*, Coimbatore, India, janv. 2015, p. 1-5. doi: 10.1109/ISCO.2015.7282377.

[12] S. B. Kamble et V. V. Jog, « Efficient key management for dynamic wireless sensor network », in *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, Bangalore, mai 2017, p. 583-586. doi: 10.1109/RTEICT.2017.8256663.

[13] S. T. Patel et N. H. Mistry, « A survey: Lightweight cryptography in WSN », in *2015 International Conference on Communication Networks (ICCN)*, Gwalior, India, nov. 2015, p. 11-15. doi: 10.1109/ICCN.2015.3.

[14] G. Leelavathi, K. Shaila, et K. R. Venugopal, « RSA processor design with vedic multiplier for nodes in wireless sensor networks », in *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, Chennai, mars 2017, p. 1254-1257. doi: 10.1109/WiSPNET.2017.8299964.

[15] R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, et P. Kruus, « TinyPK: securing sensor networks with public key technology », in *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks - SASN '04*, Washington DC, USA, 2004, p. 59. doi: 10.1145/1029102.1029113.

[16] C. Mishra et B. Sahu, « Transmission of Encrypted data in WSN: An Implementation of Hybridized RSA-TDES Algorithm », in *2020 IEEE International Symposium on Sustainable Energy, Signal Processing and Cyber Security (iSSSC)*, Gunupur Odisha, India, déc. 2020, p. 1-6. doi: 10.1109/iSSSC50941.2020.9358833.

[17] I. Sultan, B. J. Mir, et M. T. Banday, « Analysis and Optimization of Advanced Encryption Standard for the Internet of Things », in *2020 7th International Conference on Signal Processing and Integrated Networks (SPIN)*, Noida, India, févr. 2020, p. 571-575. doi: 10.1109/SPIN48934.2020.9071380.

[18] C. Panait et D. Dragomir, « Measuring the performance and energy consumption of AES in wireless sensor networks », oct. 2015, p. 1261-1266. doi: 10.15439/2015F322.

[19] S. Didla, A. Ault, et S. Bagchi, « Optimizing AES for Embedded Devices and Wireless Sensor Networks », présenté à 4th International ICST Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities, Innsbruck, Austria, 2008. doi: 10.4108/tridentcom.2008.10409.

[20] T. N. Hoang, S.-T. Van, et B. D. Nguyen, « ESP-NOW Based Decentralized Low Cost Voice Communication Systems For Buildings », in *2019 International Symposium on Electrical and Electronics Engineering (ISEE)*, Ho Chi Minh, Vietnam, oct. 2019, p. 108-112. doi: 10.1109/ISEE2.2019.8921062.

[21] G. M. Debele et X. Qian, « Automatic Room Temperature Control System Using Arduino UNO R3 and DHT11 Sensor », in *2020 17th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP)*, Chengdu, China, déc. 2020, p. 428-432. doi: 10.1109/ICCWAMTIP51612.2020.9317307.

[22] « esp-now_user_guide_en.pdf ». Consulté le: 16 août 2022. [En ligne]. Disponible sur: https://www.espressif.com/sites/default/files/documentation/esp-now_user_guide_en.pdf

[23] K. Otal, « A Generalization of the Subfield Construction », *Int. J. Inf. Secur. Sci.*, vol. 11, nº 2, Art. nº 2, juin 2022.

[24] M. Panda, « Data security in wireless sensor networks via AES algorithm », in *2015 IEEE 9th International Conference on Intelligent Systems and Control (ISCO)*, Coimbatore, India, janv. 2015, p. 1-5. doi: 10.1109/ISCO.2015.7282377.

[25] T. Yue, C. Wang, et Z. Zhu, « Hybrid Encryption Algorithm Based on Wireless Sensor Networks », in *2019 IEEE International Conference on Mechatronics and Automation (ICMA)*, Tianjin, China, août 2019, p. 690-694. doi: 10.1109/ICMA.2019.8816451.

[26] Z. Zhi, « A Cryptography System for Wireless Sensor Networks Based on IBE and CPK Algorithms », in *2008 IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application*, Wuhan, déc. 2008, p. 857-861. doi: 10.1109/PACIIA.2008.305.

[27] M. H. Eldefrawy, M. K. Khan, et K. Alghathbar, « A key agreement algorithm with rekeying for wireless sensor networks using public key cryptography », in *2010 International Conference on Anti-Counterfeiting, Security and Identification*, Chengdu, China, juill. 2010, p. 1-6. doi: 10.1109/ICASID.2010.5551480.