ISSN: 0067-2904

Security of Wireless Sensor Nodes

Alya'a Abdulrazzak Msekh*, Jamal Mohamed Kadhim
Computer Department, College of Science, Al-Nahrain University, Baghdad, Iraq

Received: 15/9/2019 Accepted: 31/10/2019

Abstract

Due to the large-scale development in satellite and network communication technologies, there is a significant demand for preserving the secure storage and transmission of the data over the internet and shared network environments. New challenges appeared that are related to the protection of critical and sensitive data from illegal usage and unauthorized access. In this paper, we address the issues described above and develop new techniques to eliminate the associated problems. To achieve this, we propose a design of a new sensor node for tracking the location of cars and collecting all information and all visited locations by cars, followed by encryption in a sensor node and saving in the database. A microcontroller of Arduino esp8266 Node MCU board and a GPS module are used. The cryptography uses the chaos-based symmetric-key encryption technique for data. This scheme utilizes a chaotic map (Hénon map) for robustness and security of data. The key sensitivity can be performed by statistical experiments to determine the safety, reliability, and speed of the algorithm. The proposed algorithm presents several exciting features, such as a high level of security, sufficient saving of the energy of the sensor network, and an acceptable encryption speed compared to Advanced Encryption Standard (AES) and Data Encryption Standard (DES).

Keyword: IoT, WSN, Chaotic map, Hénon map, Encryption, esp8266.

حماية العقد الحساسة عبر الاتصال اللاسلكي

علياء عبد الرزاق مصيخ *، جمال محمد كاظ
قسم الحاسوب، كلية العلوم، جامعة النهرين، بغداد، العراق

الخلاصة

نظرًا للتطور الكبير في تقنيات الاتصالات عبر الأقمار الصناعية والشبكات اللاسلكية، هناك مطالب كبيرة للحفاظ على آمن البيانات عند تنقلها عبر الإنترنت وبيئة الشبكة المشتركة. ظهرت التحديات الجديدة لحماية البيانات الحرجة والحساسة من الاستخدام غير القانوني والوصول غير المصرح به. في هذا العمل، نعالج المشاكل الموضحة أعلاه باستخدام تقنيات مطورة جديدة للقضاء على المشاكل المرتبطة بها. لتحقيق ذلك، نقترح تصميم عقدة مستشعر جديدة لتحقيق ذلك، نقترح تصميم عقدة استشعار جديدة لتتبع موقع السيارات وجمع جميع المعلومات وجميع المواقع التي تمت زيارتها من قبل السيارات ثم تقوم عقدة الاستشعار بتشفيرها وحفظها في قاعدة البيانات. حيث – تم استخدام متحكم (Arduino esp8266 NodeMCU) ووحدة (GPS)في تصميم هذه العقدة.

يستخدم التشفير تقنية تشفير المفتاح المتماثل المستندة إلى فوضى البيانات. يستخدم هذا المخطط خريطة فوضوية(Hénon map) لقوة أمان البيانات. حساب الحساسية الرئيسية من خلال إجراء تجارب إحصائية لتحديد سلامة وموثوقية وسرعة عمل خوارزمية تشفير البيانات المستخدمة. تقدم الخوارزمية المقترحة العديد من

*Email: proalyaa@gmail.com

الميزات المثيرة، مثل مستوى عالٍ من الأمان، وتوفر ما يكفي من الطاقة لشبكة الاستشعار، وسرعة تشفير مقبولة بالمقارنة مع معيار التشفير المتقدم (AES) ومعيار تشفير البيانات(DES) .

1. INTRODUCTION

The Internet of Things (IoT) in computers and wireless networks became more important. IoT consists of a continuum of uniquely addressable things communicating together to form worldwide dynamic networks. The concept of IoT has been introduced to enable full access and security to data in Sensor Node (SN) or things [1].

Wireless Sensor Networks (WSNs) and wired networks are exposed to risks such as the eavesdrop on data by an attacker [2]. The SNs placed in unprotected areas may lead to easy susceptibility to attacks; therefore, it must be safe by providing secure algorithm encryption in WSNs [3]. One of the most secure algorithms is a chaotic algorithm, which has gained a great interest by information security researchers. For the sake of suitability, the properties of the chaotic algorithm, such as mixing, complexity, sensitivity to initial conditions, diffusion, and lightweight processing space, have assisted the use of chaos in cryptography.

The chaotic systems for secure communication are generating stream cipher or block cipher [4]. In 2012, Chandra and his group proposed a protocol that depends on public-key cryptography for agent authentication and session key establishment. The SNs were executed in Rivest–Shamir–Adleman (RSA) algorithm by connecting the external agent and the base station through Public. Key Cryptography. (PKC), while the base station is communicating with the sensor by sharing a private key technique [5]. In 2015, Panda introduced an encryption algorithm which is implemented using AES. The AES-based symmetric key approach is implemented for the confidentiality of data in the WSN by sharing the same key for encryption and decryption between both sides of the communication. This algorithm results in plaintext by calculating ten rounds mathematically to produce the cipher-text in a short time [6]. In 2016, Mahdi and Hreshee designed a model of a security that depends on a chaotic system by encrypting voice signals. They used Henon map that deals with discrete-time system differential equations. The encryption in this system depends on generating a stream of bits (ones and zeroes) from the Henon map. Henon map gives a very strong ability for encryption in comparison with the traditional methods used for encryption [7].

In this paper, a WSN security was designed and implemented. The design contains SNs to perform desired measurements, process the measured data, and transmit it after encryption to the client over a wireless channel. The client makes TCP/IP connection with the SN to collect the required data and then encrypt and analyze these data. This method minimizes the implementation gaps between different security mechanisms by establishing a new key procedure. In each new procedure, Henon map's equations are computed, and a new key is produced. Therefore, a new key will be generated in each cycle.

2. THE SENSOR NODES

The SNs lie at the core of the WSNs, which work as a device that possesses sensing, computation, and communication capabilities. Based on their sensing components and the application requirements, the SNs would be used to monitor many properties such as temperature, light, motion, pressure, and humidity. The processing module of the SN can do computation on the sensed data and the data received from other sensors. The communication module in the SNs is used to send and receive the data packets to and from the neighboring nodes [8]. The sensors (sensor nodes) realize the presence of a physical entity using device-specific embedded software in the surrounding and gather the information required for the interaction. Each physical device has a unique Internet Protocol (IP). The information collected will be processed in these physical devices via a connection between IP with storage servers on the web and will be delivered at the right place and time to be utilized by different applications [9].

3. THE ARCHITECTURE OF SENSOR NETWORKS COMMUNICATION

WSNs are small and light weight sensing devices that contain a constrained processing unit, EEPROM or Flash memory, little memory for tiny operating-systems, one or more sensors, limited range transceiver, Analog to Digital Converter (ADC), and other desired programs depending on type of node, as shown in Figure-1 [10].

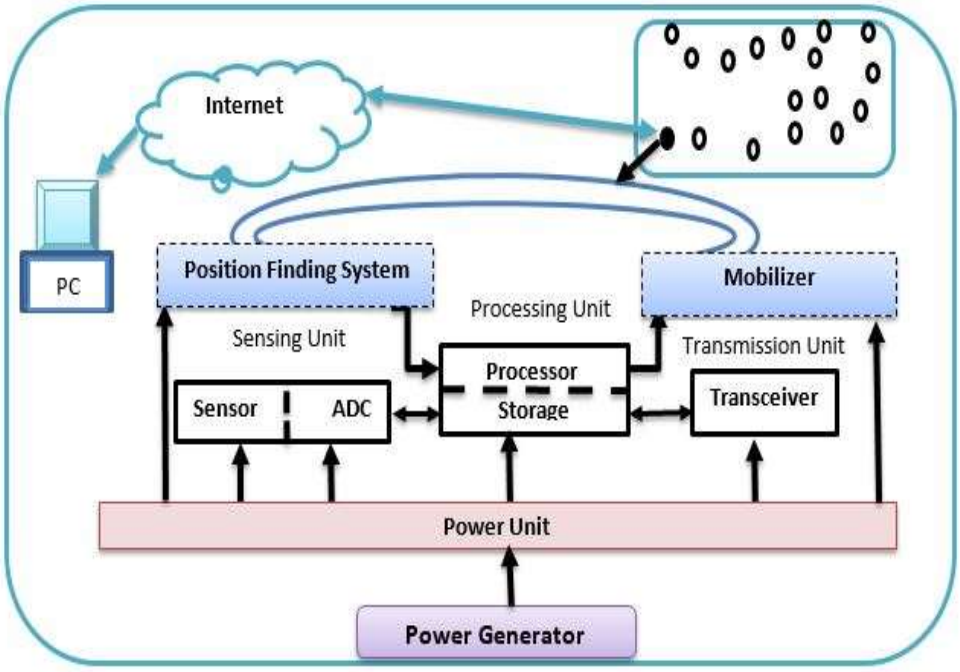

Figure 1-Architecture of the sensor node [11].

4. WIRELESS SENSOR NETWORK

WSNs are a collection of specialized autonomous sensors and actuators with a wireless communications infrastructure. These sensors are intended to control physical or environmental conditions at different locations and pass their data and their control command to the central area and the desired actuator through the network, respectively [12]. Every SN provides a transducer, a radio transceiver, a microcontroller, a power supply, and usually a battery. Through the satellite network and the internet, the collected data is received by an application at the end. It is not necessary that the SNs have a fixed area; most of SNs are randomly deployed to monitor the sensor area, and usually communicate with each other and the radio transceiver [13].

5. CONNECTING WSNs WITH THE INTERNET

Direct or indirect communication with things in a smart way is basic for the Internet of things, where things can communicate with each other at any place and time. The difference between the Internet and the IoT is the use of computers on the Internet, while the terminal devices of the IoT are intelligent things. WSNs are a network of intelligent things. Connecting WSNs with the Internet will form an IoT information infrastructure. There are many ways of connecting WSNs to the Internet. The approach of Transmission Control Protocol (TCP) //IP overlay solution is performed by an overlay network constructed on either WSNs or the Internet [14].

5.1 TCP/ IP OVERLAY SOLUTION

TCP/IP protocols suite consists of many protocols, but its name came especially from two main protocols, TCP and Internet Protocol (IP). IP is responsible for providing addressing and routing globally [14]. TCP/IP overlay sensor networks are to implement TCP/IP protocol above a microcomputer system with minimal resources, as shown in Figure-2. Many problems may accompany the implementation of TCP/IP in WSNs. For example, the problems of how the IP address is assigned to the SN and how to mix the address-based and data-.based routing efficiently according to network traffic. The IPv16 over Low Power Wireless Personal Area Networks (61LowPAN) is a typical TCP/IP overlay solution. Internet users can access individual SNs directly by using the IPv.6 address [13].

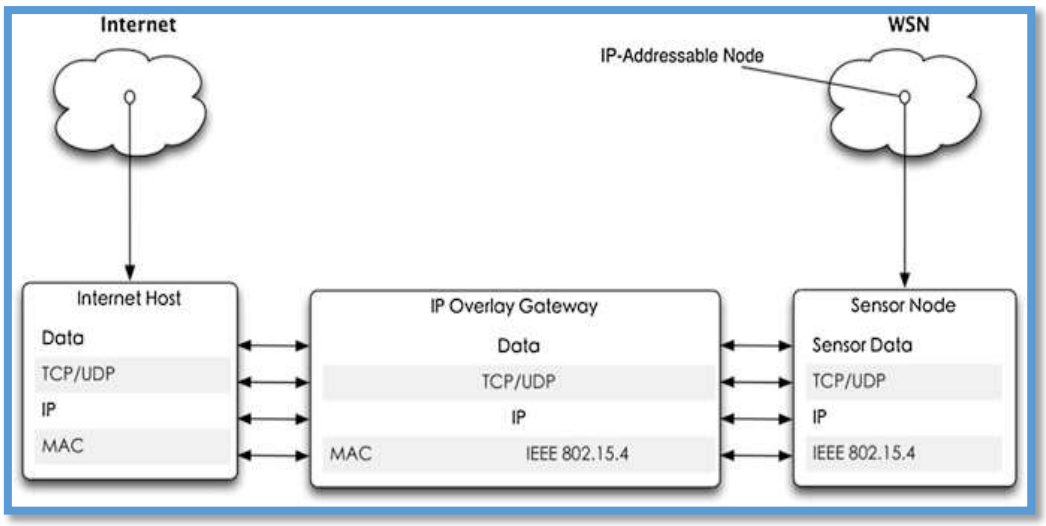

Figure 2- TCP/IP overlay solution [13].

6. SECURITY SCHEMES FOR WIRELESS SENSOR NETWORKS

Security is the most important factor to be considered in the design of information and networking systems that might be subjected to security attacks on WSNs, which are similar to wired networks [15]. WSNs are more susceptible to attacks due to the deployment of SNs in unprotected areas [2].

7. CHAOTIC SYSTEMS

Chaos had become the base of many encryptions techniques, because it has many advantages that help to use it as an encryption algorithm [16]. Chaotic systems used in cryptography for secure communication are generating stream cipher or block cipher [17]. There are two types of Chaotic systems; the first one is the chaotic flow, such as Lorenz, Rössler, Chua, etc., which deals with the Continuous-Time Systems. The second is the chaotic maps such as Henon, logistic, cat map, etc., that describe the Discrete-Time Systems (DTS)[18].

The chaotic systems have many characteristics compared to the other linear and nonlinear systems. These characteristics involve that the movement in a chaotic system is always bound to a particular region; cyclicity is the motion of a chaotic system is ergodic theory in its attractor. The chaotic trajectory does not stay at a point if it passes through every point state in the region of the system, and randomness is a fully deterministic system. Thus, if the initial condition is known in perfect detail, any small inaccuracy in the initial state will grow exponentially with time. Therefore, the predictably of the system behavior for a long term future is impossible[4].

7.1 Hénon Map

The chaotic map used in this paper is the Hénon map. It has a discrete dynamical behavior with a very simple nonlinear difference equation. It is one of the most studied examples of dynamical systems that exhibit chaotic behavior [19]. As explained below in equations (1) and (2), the Henon map takes a point (X_n, Y_n) in the plane and maps it to a new position. The difference equations for the Henon map [7] are:

$$x_{n+1} = 1 - p{x_n}^2 + y_n \quad (1)$$

$$y_{n+1} = qx_n \quad (2)$$

This map depends on two parameters (p and q). The classical Henon map has values of p = 1.44 and q = 0.33 [20].

7.2 GENERATING A SEQUENCE OF BITS FROM CHAOTIC MAP

The encryption in this system depends on generating a stream of bits of ones and zeroes from the Henon-map. This code will be exclusive OR with the input data. The technique is used to convert each data that result from the SN to a number of bits that will be equal to the number of bits that are converted from the input data [7]. The strength of security in Henon map was previously studied [21]. In many researches, it was proved that Henon method is strong against brute force attack as compared with the classical methods because of having high key space [22]. The size of the key space should be greater than 2^{100} to prepare a high-security system [23]. A previous study [24] proved that if the limited of space key less than 2^{100} it easy to broken the key space reaches to $.8426\times10^{128}$ [7].

8. THE MODEL OF THE PROPOSED SYSTEM

Advances in microelectronic systems and wireless communication technologies have led to the proliferation of WSNs. The SNs can work in harsh operating environments and the nodes make a collaborative effort to sense specific data around its periphery. The typical sensor network consists of many low-powered and low-cost SNs. WSN protocols should be designed to prolong the lifetime of the network and minimize the energy consumption. Information collecting in WSN is performed by requesting the statistics about the area in the sensor field; this requires a protocol that can deal with the requests in WSN. The last important characteristic of WSNs is the position of the nodes which may not be engineered or predetermined, therefore, data routes that are self-organizing must be provided. The TCP/IP connection is used to ensure a safe connection. Each SN (Transmitter) contains an IP Address that allows dealing with the SN and operating the data in it. Figure-3 explains a general block diagram for data and how it operates inside the Henon map. Finally, encrypted data are represented as a result of security for this chaotic system and transmitted via a wireless connection to the client.

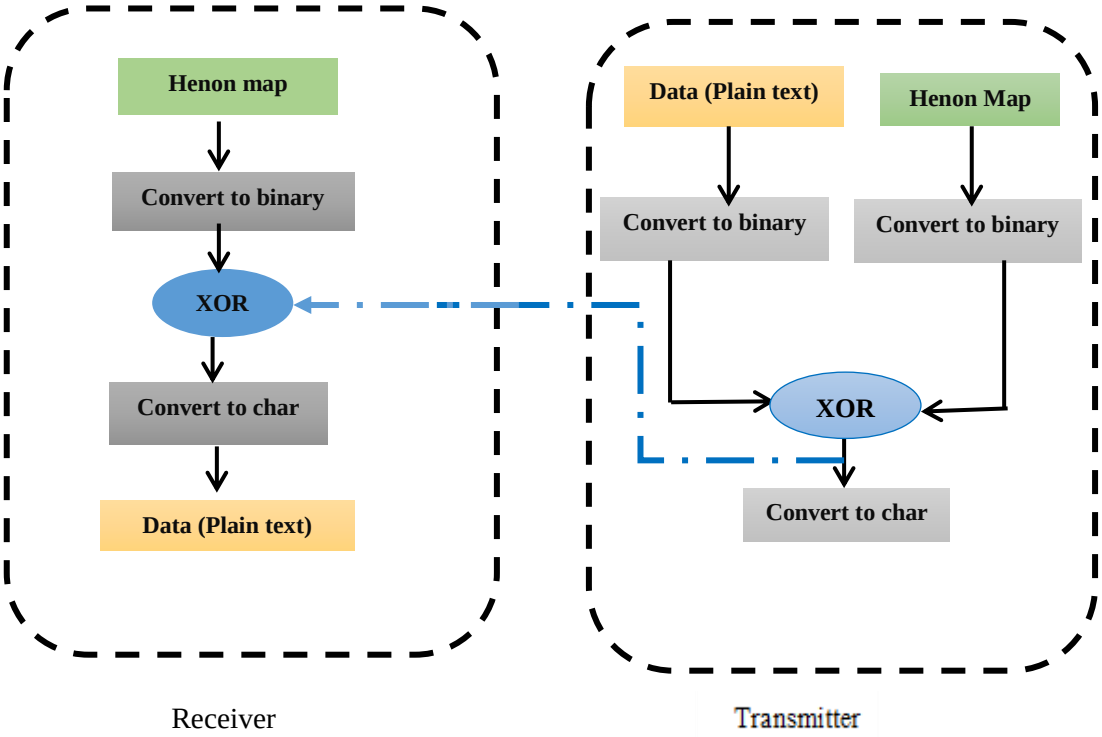

Figure 3- General block diagram for data inside the Henon map.

Transmitter: A WSN consists of Arduino hardware ESP8266 board, GPS, and battery to support the SN energy. This connection will emulate the satellites and retrieve the required information. Each node will collect the car information in addition to the location details such as IP, name, color and model of the car, longitude, latitude, time, and date for the SN. This information is considered as input data to the encryption system of Henon map to protect it from any malicious attacks by using a secure algorithm for encrypting.

Receiver: A client makes TCP/IP connection with a SN to collect and decrypt the required data. The encrypted data is transmitted in communications over a wireless channel.

9. RESULTS

The basic location details are displayed when a client makes a connection with the SN. Accessibility for a node is achieved by knowing the IP address to each SN by wireless communication, as shown in Figure-4.

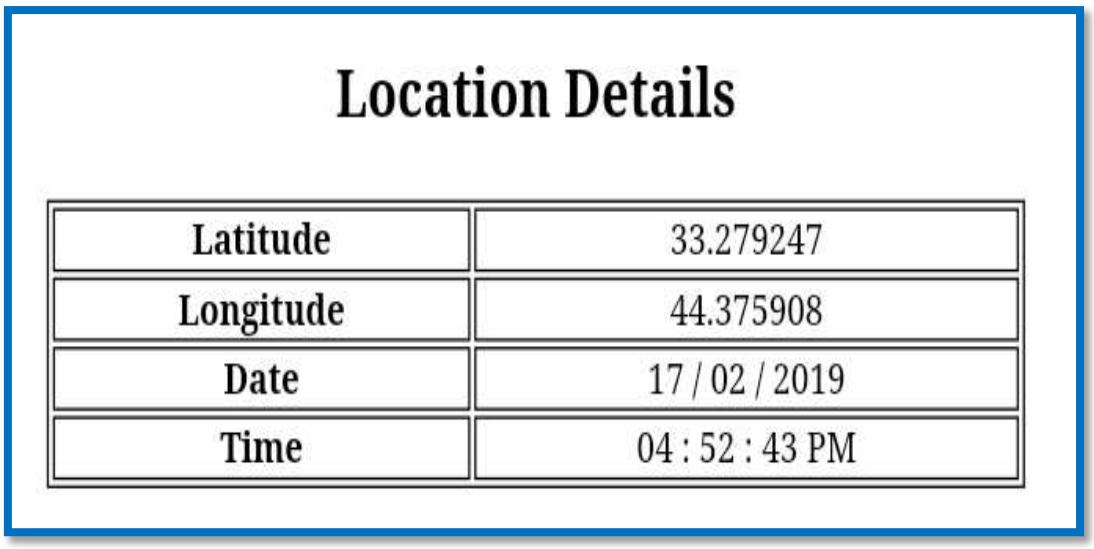

Figure 4-The location details captured by a sensor node.

In the SN, the data is encrypted as shown in Figure-5 and sent as ciphertext to the database.

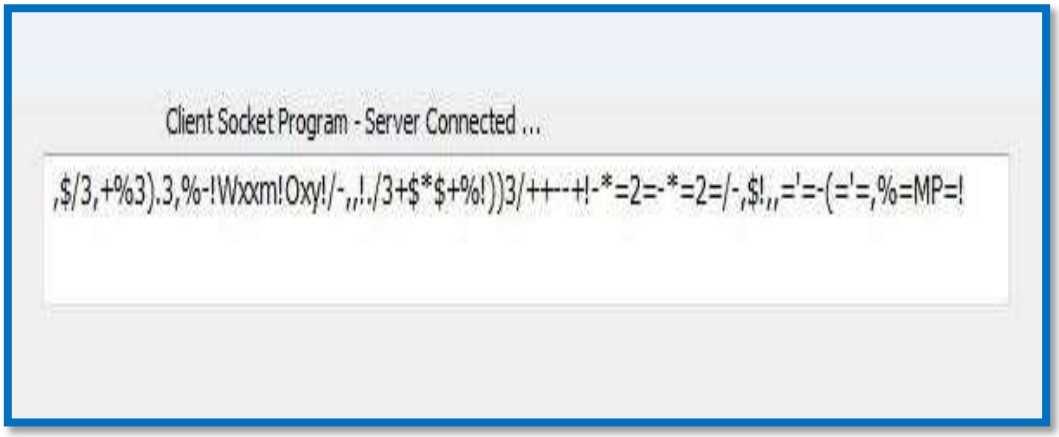

Figure 5-Encrypted data that result from a sensor node.

A client collects the data from the SNs and decrypts it as shown in Figure-6. Hence, no other user can read or access these data except the authorized users. This data is saved in a database in a specific application that is designed for this purpose.

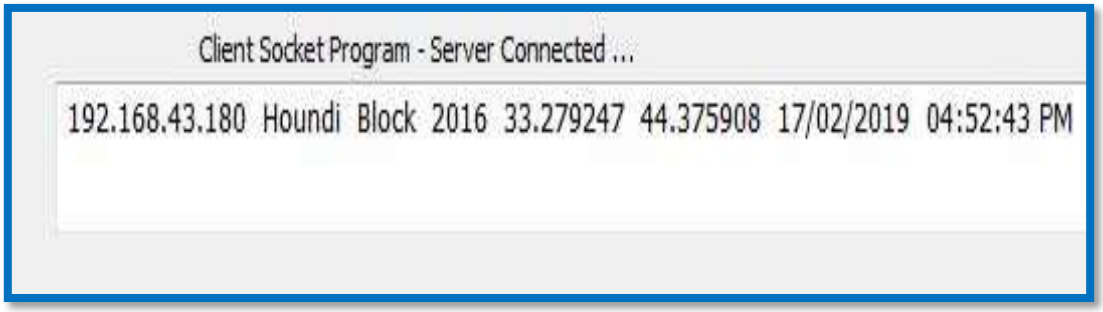

Figure 6-Plaintext after decryption of data in the database.

The implemented system was designed with a simple encryption process. It is clear that there is no expansion found in the size of the encrypted text which is equal to the size of the original text. The recipient text is 100% correct and has no error.

The time needed to make the sensor node capture the information, such as longitude, latitude, time, and date, and execute the chaotic map to encrypt data was 41.88 ms, as given in Figure-7. This short time will help the network to keep working for the longest time possible without stop, since the mathematical operation in the algorithm used is simple and does not need more computation and, thus, does not consume energy.

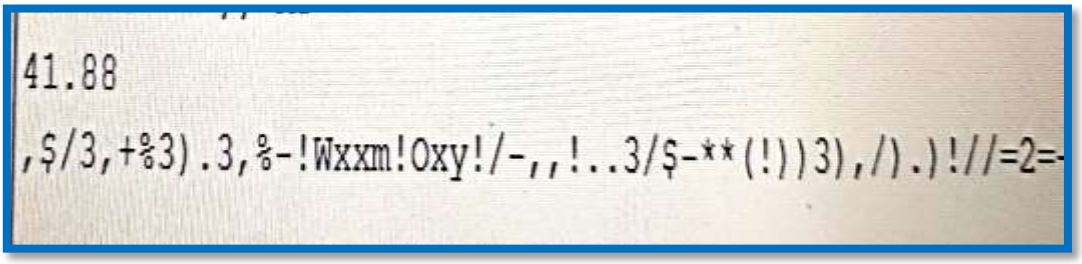

Figure 5-Execution time for encrypting the sensor node information.

10. CONCLUSIONS

The important conclusions of this work can be summarized as follows:

1. A novel cryptographic scheme that integrates the discrete chaotic map and genetic cryptography as 2DES, 3DES for WSN applications was applied. This integration ensures a sufficient level of security with limited resources.
2. Henon map encryption can be used for both text and image data encryption because it is a robust block cipher. It enables the use of the same encryption mechanism in different-mode sensors; for example, sensing images with different environmental phenomena.
3. The system was used based on the Arduino microcontroller; the speed of the operations in the implemented system was perfect and it was very accurate.
4. Time effect: The attacker takes a very long time to get and recover the plain text. It may take several days, months, or years in some times, depending on the attacker PC speed. This advantage puts the proposed system as one of the best ways to achieve very secure communication systems and make it stronger to prevent any attack. Since this system works on random numbers, the attacker cannot know the key used to encrypt data.

11. REFERENCES

1. Dogo, E.M., Salami, A.F., Nwulu, N.L. and Aigbavboa, C.O. **2019**. "Blockchain and Internet of Things-Based Technologies for Intelligent Water Management System," pp. 129–150.

2. WONG, V.W.S., Schober, R., NG, D.W.K. and Wang, L. **2017**. "Key technologies for 5G wireless communications," *Science China Information Sciences*.

3. Azzabi, T., Farhat, H. and Sahli, N. **2017**. "A survey on wireless sensor networks security issues and military specificities," in Proceedings of International Conference on Advanced Systems and Electric Technologies, IC_ASET 2017, pp. 66–72.

4. Kuzmin, L. and Andreyev, Y.V. **2017**. "Chaotic synchronous response in multipath channel," *Prog. Electromagn. Res. Symp.*, **2648**(1): 2648–2653.

5. Sekhar, V.C. and Sarvabhatla, M. **2012**. "Security in wireless sensor networks with public key techniques," 2012 Int. Conf. Comput. Commun. Informatics, ICCCI 2012.

6. Panda, M. **2015**. "Data security in wireless sensor networks via AES algorithm," Proc. 2015 IEEE 9th Int. Conf. Intell. Syst. Control. ISCO 2015.

7. Mahdi, A. and Hreshee, S.S. **2016**. "Design and implementation of voice encryption system using XOR based on Hénon map," *Al-Sadiq Int. Conf. Multidiscip. IT Commun. Tech. Sci. Appl. AIC-MITCSA 2016*, **4**(1): 82–86, 2016.

8. Dâmaso, A., Rosa, N. and Maciel, P. **2014**. "Reliability of wireless sensor networks," *Sensors (Switzerland)*, **14**(9): 15760–15785.

9. Praveena, A. and Smys, S. **2016**. "Efficient cryptographic approach for data security in wireless sensor networks using MES V-U," Proc. 10th Int. Conf. Intell. Syst. Control. ISCO 2016, 2016.

10. Zeng, Y., Cao, J., Zhang, S., Guo, S. and Xie, L. **2010**. "Random-walk based approach to detect clone attacks in wireless sensor networks," *IEEE J. Sel. Areas Commun.*, **28**(5): 677–691.

11. Dong, Q., Yu, L., Lu, H., Hong, Z. and Chen, Y. **2010**. "Design of Building Monitoring Systems Based on Wireless Sensor Networks," *Wirel. Sens. Netw.*, **2**(9): 703–709.
12. Chakchouk, N. **2015**. "A Survey on Opportunistic Routing in Wireless Communication Networks," *IEEE Commun. Surv. Tutorials*, **17**(4): 2214–2241.
13. Shen, F., Liu, C., Qi, B., Ji, Y. and Caban, D. **2014**. "Building effective scheduling algorithms for sensor networks," in ITNG 2014 - Proceedings of the 11th International Conference on Information Technology: New Generations, 2014, pp. 403–406.
14. Kosanovic, M.R. and Stojcev, M.K. **2011**. "Delay compensation method for time synchronization in wireless sensor networks," in *2011 10th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services, TELSIKS 2011 - Proceedings of Papers*, **2**: pp. 623–629.
15. Kadhim, J.M. and Abed, A.E. **2017**."Steganography Using TCP / IP's Sequence Number," *J. Al-Nahrain Univ. Sci.*, **20**(4): 102–108.
16. Osanaiye, O.A., Alfa, A.S. and Hancke, G.P. **2018**. "Denial of Service Defence for Resource Availability in Wireless Sensor Networks," *IEEE Access*, **6**(c): 6975–7004, 2018.
17. Vaidyanathan, S. and Volos, C. **2016**. "Advances and applications in chaotic systems," *Stud. Comput. Intell.*, **636**.
18. Shukla, P.K., Khare, A., Rizvi, M.A., Stalin, S. and Kumar, S. **2015**."Applied cryptography using chaos function for fast digital logic-based systems in ubiquitous computing," *Entropy*, **17**(3): 1387–1410, 2015.
19. Jovic, B., Unsworth, C.P., Sandhu, G.S., and Berber, S.M. **2007**. "A robust sequence synchronization unit for multi-user DS-CDMA chaos-based communication systems," *Signal Processing*, **87**(7): 1692–1708.
20. Raja Kumar, R., Revathi, M., Sampath, A. and Indumathi, P. **2010**. "Secure communication using chaos in multiple access environment," in Proceedings of the 8th WSEAS International Conference on Applied Electromagnetics, Wireless and Optical Communications, ELECTRO '10, pp. 15–19.
21. Mursi, M.F.M., Ahmed, H.E.H., El-Samie, F.E.A. and El-Aziem, A.H.A. **2015**. "Image Encryption Based on Development of Hénon Chaotic Maps using Fractional Fourier Transform," *Int. J. Strateg. Inf. Technol. Appl.*, **5**(3): 62–77.
22. Mishra, M. **2012**. "Hybrid Message-Embedded Cipher using Logistic Map," *Int. J. Secur. Priv. Trust Manag.*, **1**(3): 81–91.
23. Al-Shameri, W.F.H. **2012**. "Dynamical properties of the hénon mapping," *Int. J. Math. Anal.*, **6**(49–52): 2419–2430.
24. Qu, H. and Liu, W. **2011**. "A robust key predistribution scheme for wireless sensor networks," in 2011 IEEE 3rd International Conference on Communication Software and Networks, ICCSN 2011, pp. 634–637.