

Data transmitted encryption for clustering protocol in heterogeneous wireless sensor networks

Basim Abood¹, Abeer Naser Faisal¹, Qasim Abduljabbar Hamed²

¹College of Computer Science and Information Technology, University of Sumer, Al-Rifai, Iraq

²Center of Computer, University of Sumer, Al-Rifai, Iraq

Article Info

Article history:

Received Jun 17, 2021

Revised Sep 2, 2021

Accepted Nov 1, 2021

Keywords:

Cheesboard clustering
Data encryption
Routing protocol
Secure clustering
Wireless sensor networks

ABSTRACT

In this paper, elliptic curves Diffie Hellman-Rivest Shamir Adleman algorithm (ECDH-RSA) is a novel encryption method was proposed, which based on ECDH and RSA algorithm to secure transmitted data in heterogeneous wireless sensor networks (HWSNs). The proposed encryption is built under cheesboard clustering routing method (CCRM). The CCRM used to regulate energy consumption of the nodes. To achieve good scalability and performance by using limited powerful max-end sensors besides a large powerful of min-end sensors. ECDH is used for the sharing of public and private keys because of its ability to provide small key size high protection. The proposed authentication key is generated by merging it with the reference number of the node, and distance to its cluster head (CH). Decreasing the energy intake of CHs, RSA encryption allows CH to compile the data which encrypted with no need to decrypt it. The results of the simulation show that the approach could maximize the life of the network by nearly (47%, and 35.7%) compare by secure low-energy adaptive clustering hierarchy (Sec-LEACH and SL-LEACH) approaches respectively.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Basim Abood

College of Computer Science and Information Technology, University of Sumer

Al-Rifai, Thi-Qar, Iraq

Email: b.abood@uos.edu.iq

1. INTRODUCTION

Information security (IS) is used to prevent unauthorized access to information and perform various operations on such information, such as the use, disclosure, disabling, destruction or modification of such information [1]-[3]. IS has many objectives in relation to the protection of information against any risks to which such information may be exposed. The type of risk to which the data is exposed varies by application [4]-[6]. However, The proposed security of low-energy adaptive clustering hierarchy (LEACH) protocol (SLEACH) to construct a secure wireless sensor networks (WSN) clustering model [7]-[9]. It purposes to avoid sinkholes, forwarding with care, and SLEACH in general, are limited by system memory, resulting in network efficiency reduction and a shorter lifespan. To overawed the complexity and difficulty of traditional encryption organizations in WSNs have a limited amount of storage space, the advanced encryption standard (AES) and elliptic curve cryptography (ECC) algorithms are used in [10] to reduce the complexity and exploit the advantages of these algorithms. In WSNs, ECC is used to create with sharing the key. To protect the aggregation with authentication scalable data management, analysis, and visualization (SDAV) is proposed [11], [12]. The researchers select the ECC over conventional asymmetric algorithms because of its low key and performance in terms of simulation and capacity. The aggregator gathers in SDAV for its members' encrypted data, decrypts it, averages it, and then returns the result to them. Secure enhanced data aggregation (SEDA) based on ECC was used by another secure in [13]. SEDA-ECC is based on the concepts

of privacy encryption algorithm for homomorphic technique. This system has great security outcomes, particularly when it comes to node exploitation attacks. But, The key challenges are the necessary memory capacity and energy consumption. For the energy cost of communication in WSNs [14], the authors suggested a cryptography to secure data transmission in WSNs routing architecture elliptic curves Diffie Hellman algorithm -elliptic curve digital signature algorithm (ECDH-ECDSA) key exchange and verify that it must be favored in cases where a trusted third party is accessible. Therefore, When it comes to calculating the cost of cryptographic protocols on sensor nodes, monitoring should be taken into account. In this paper, we proposed the ECDH-RSA an enhanced encryption algorithm plan based on ECDH and RSA in order to ensure data transfer security in WSN to overcome these limitations of various articles with dynamically clustered sensor nodes, The biggest drawbacks are a finite quantity of memory and the possibility of a single node failure. For compromise communication lines, the attacker can compromise many more nodes. Furthermore, the decryption algorithm is not suited for encrypting large amounts of data. The goal is to have the least amount of impact on the network's lifecycle, chessboard clustering routing method (CCRM) and ECDH is used to produce public and private keys for sensor nodes, and is used to find the most suitable sensor nodes as cluster heads to relay the message to the base station.

The suggested encryption method is based on CCRM, which employs the chessboard clustering algorithm (CC) to select the best network structure for lowering energy consumption after each round. CCRM is written at section 3. The following is how the rest of the paper is structured: The approach of this paper is clarified in section 2. The structure of the chessboard clustering routing protocol is showed in section 3. Our proposed solution for securing data clustered sensors in WSN is discussed in section 4. Simulation experimental findings and contribution are discussed in section 5. A summary finishes section 6 of this work.

2. METHODOLOGY

Figure 1 depicts the stages of our planned project. The first phase entails using CCRM to build a network topology that reduces energy fatigue. Then, to ensure secure data flow from sensor nodes to the BS, the proposed encryption schema is implemented. The next sections go over each of these phases in depth.

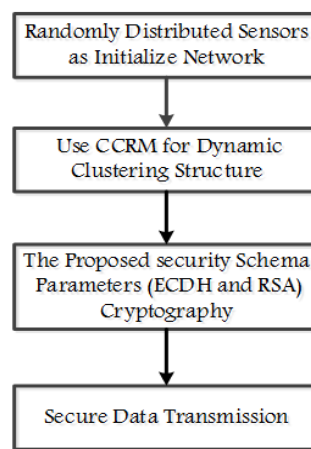


Figure 1. Developing the secure data transfer technique

3. THE CHESSBOARD CLUSTERING ROUTING PROTOCOL

In this part, the chessboard clustering algorithm is used to suggest heterogeneous sensor networks. We will employ the following two types of sensors:

- The usage of a restricted number of powerful high-end sensors is referred to as an H-sensor (cluster head).
- The term "L-sensor" refers to the employment of a variety of low-cost (basic) sensors.

3.1. Cluster deployment

We introduce our heterogeneous wireless sensor networks (HWSNs) checkerboard clustering approach in this part for heterogeneous sensor networks. In the sensor network, chessboard sensors are employed. The sensor network is divided into several small, equal-sized cells, as shown in Figure 2, with adjacent cells colored in various hues (white/black). H-sensors and L-sensors are expected to be distributed

evenly and randomly in this area. H-sensors, on the other hand, should be installed with greater care to ensure that all L-sensors are covered. That is, at least one cluster head can be heard by each sensor.

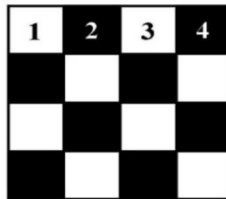


Figure 2. The chessboard clustering scheme

3.2. The partition method for clustering

Cluster partition is a technique for homogeneous networks that has been extensively researched [15]-[17], and for heterogeneous networks [18], [19]. First, Only the H-sensors in white cells are active during the initiation period, whereas the H-sensors in black cells are turned off. All of the L-sensors are working. In white cells, clusters form around H-sensors, and these H-sensors become cluster heads. Later, when H-sensors in white cells run out of energy, the clusters are formed around the H-sensors in black cells in the same way. The cluster partition concept will be described in terms of the H-sensors in the white cells. In turn, broadcast hello messages based on the H-sensors' IDs and their locations, starting with the H-sensor with the smallest ID. Each L-sensor will then build a list of the H-sensors it has heard from, or whose messages it has successfully received. The broadcast's transmission range is large enough, based on received signal strength, for most L-sensors to receive hello messages from multiple H-sensors. The cluster leader is then chosen by each L-sensor as the H-sensor whose hello message has the best signal strength. After this, each L-sensor will recognize which H-sensor it belongs to and will favor the H-sensor at the top of the list. The H-sensor then begins to determine which sensors should be included in its cluster. We just discuss it for cluster 1 because it is the same for all clusters. H-sensor 1, abbreviated H1, will send a message that says "All sensors within a reasonable distance of me should report to me as the preferred cluster head". Following that, each eligible L-sensor will deliver a packet to H_1 , this contains the ID as well as the location of the ID. After all, L-sensor has reported, H_1 will add them to a list L and broadcast an acknowledgment packet to them. The sensor in L with the least ID is then asked by H_1 , say S_1 , to send a message to sensors asking them to report to S_1 if they: *i*) H_1 is the best cluster head to use.; *ii*) S_1 has conveyed this message to H_1 ; and *iii*) H_1 has not acknowledged S_1 .

All of these L-sensors will pay attention to S_1 , and S_1 will inform H_1 about these L-sensors. H_1 will then ask another sensor in L to add these newly identified sensors to L , say S_2 , to follow in the footsteps of S_1 , and so forth, until there are no more sensors to discover. It is undeniable that, after this, H_1 will discover every sensor that has chosen H_1 as their preferred cluster head and has a path to H_1 .

After H_1 has finished, in the same way, H_2 can discover its sensors, then H_3 , H_4 until the last H-sensor. When the last H-sensor has completed his work, we may claim that the first round of discovery is finished. It's worth noting that after the first round, the majority of L-sensors have most likely previously been detected by the favored H-sensors. However, some L-sensors may have yet to be discovered because they lack a path to their preferred H-sensor. Such L-sensors are called the orphan sensors. To assist orphan sensors in locating the H-sensor, a second phase of discovery is required, in which each orphan sensor broadcasts a message stating that it saying that "Any non-orphan sensor who receives this message is welcome to add me to their cluster". The first non-orphan sensor to reply will inform its H-sensor of the new discovery. After this, we may claim that all L-sensors in the white cell have discovered the H-sensors.

As an example, Figure 3 depicts a very basic network, H_1 and H_2 are the cluster heads, and there are 10 sensors in all. The transmission distance of the cluster heads is DH that is only H_1 can be heard by sensors S_1 to S_5 , while H_2 can only be heard by sensors S_7 to S_{10} . Both H_1 and H_2 can be heard by S_6 , although it is considered that H_1 's signal is stronger. A sensor can send a packet to another node if it is capable of doing so, there is an edge between them. At first, Figure 4 shows how H_1 and H_2 will broadcast their signals in turn. Following that, H_1 will be the chosen cluster head for S_1 to S_6 , and H_2 will be the preferred cluster head for S_7 to S_{10} . Next, H_1 will look for sensors that can communicate with it directly. Because they are within D of H_1 , it will send a message, and S_1 and S_2 will respond, as shown in Figure 5(a). After this, as demonstrated in Figure 5(b), S_1 will discover S_3 , S_4 , and S_5 . Next, H_2 will discover sensors S_7 to S_{10} in a similar way, as shown in Figure 6(a). S_6 is an orphan since it chose H_1 as its cluster head of choice. However, it is unable to communicate with any sensor that has a connection to H_1 . Thus, S_6 will send a message to S_7 , who will add S_6 to the H_2 cluster, as shown in Figure 6(b).

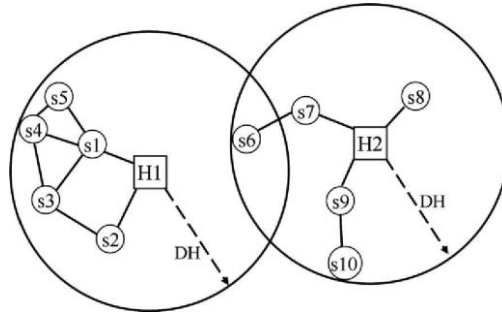


Figure 3. A simple network of cluster partition

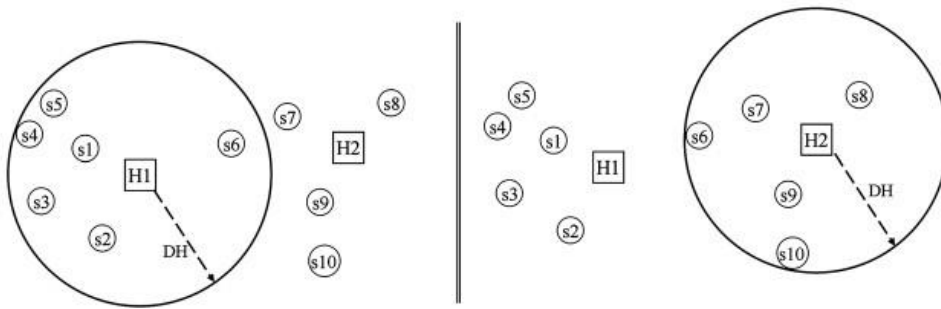


Figure 4. The messages of H_1 and H_2 are aired in turn

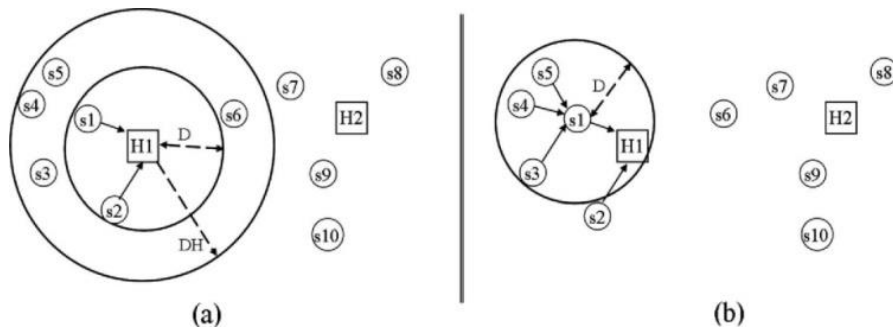


Figure 5. Because they are within D of H_1 , it will send a message: (a) S_1 and S_2 respond H_1 's message and (b) S_1 discovers S_3 , S_4 , and S_5

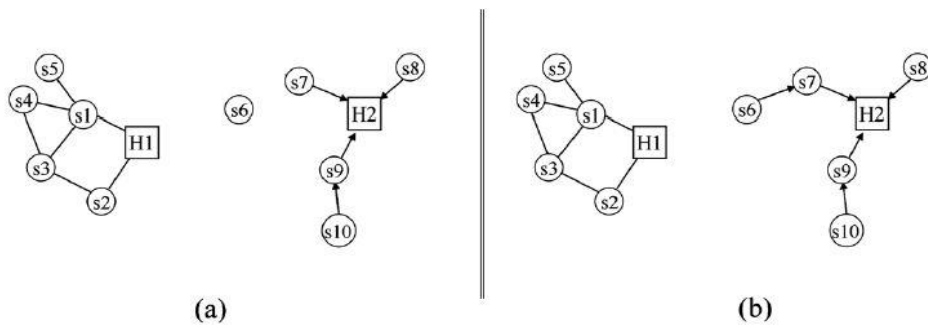


Figure 6. Described the scenarios to join clusters as: (a) H_2 discovers S_7 to S_{10} and (b) S_6 joins the cluster of H_2

4. ENCRYPTION ALGORITHMS (ECDH AND RSA)

4.1. Elliptic curves Diffie-Hellman (ECDH)

In a variety of cryptographic contexts, elliptic curves were already in use worked independently on this project [20]-[23]. At that time, integer factorization and primality proof are two examples. ‘Domain parameters’ ECC is a good example of a constant like this. Unlike private key cryptography, public key cryptography does not require the communication parties to disclose a secret, but it is substantially slower. An elliptic curve can be conceived of as being given by an affine equation of them for the purposes of encryption:

$$y^2 = x^3 + ax + b \tag{1}$$

Where a and b are elements of a finite field containing p elements, and p is a prime greater than 3. (The equations for binary and ternary fields differ slightly). For every L-sensor in the network, the initial step before data transfer between the L-Sensor, ECDH, and a base point p that sits on the curve must be known. The collection of ordered pairs (x, y) having coordinates in the field and such that x and y satisfy the relation given by the equation describing the curve is the set of points on the curve. A group is also formed by a set of points on an elliptic curve that have coordinates in a finite field, and the procedure is as follows: to increase the curve by two points Q_1 and Q_2 together. Then a straight line is drawn through the curve to find the third point of intersection R_1 . Then point R_1 is reflected along the X-axis to obtain $(-R_1)$. That is to say, the total of Q_1 and Q_2 results $(-R_1)$. This group operation's concept is that the three points $Q_1, Q_2,$ and R_1 Lie down in a straight line, and the points that sum up to zero as a result of a function intersecting a curve as shown in Figure 7 [22].

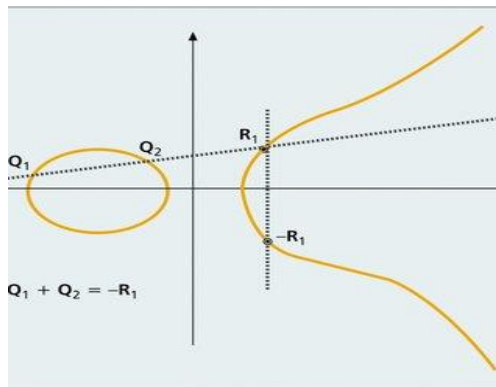


Figure 7. Group law on an elliptic curve

Because the majority of wireless sensor environments are unsecured and difficult to connect, it's difficult to reliably exchange keys in them. One of the elliptic curve types that offers service or solves the difficulty outlined is the Diffie-Hellman key. When two parties exchange keys, but those keys are subjected to particular processes by the same party after the switch until it becomes a key encryption by that party. The difficulty of guessing the type of operation and the digits in which the layer of inquiry led to this exit is the principle of power in the Diffie-Hellman key [22].

Therefore, it's crucial to get the group operation up and running as efficiently as possible. Many options have been considered, however how to optimize the L-main sensor's group operation is typically influenced by the underlying system [20], [22]. That some points on an elliptic curve with affine coordinates, as defined above, must be represented. Then to add two $Q_1 = (x_1, y_1)$ and $Q_2 = (x_2, y_2)$, where $x_1 \neq x_2$, it is necessary to get the slope of the line that passes through them:

$$\lambda = (y_2 - y_1)/(x_2 - x_1) \tag{2}$$

This necessitates division in the limited field beneath. Then figure out where the line intersects the curve for the third time, it is found that $(-R_1) = (x_3, y_3)$, where:

$$x_3 = \lambda^2 - x_1 - x_2 \tag{3}$$

for the finite field ($P \neq 2$ or 3), forming the sum necessitates one division, one squaring, and one multiplication, when two affine points with different x –coordinates are combined, are occasionally utilized.

Triples of coordinates are used in weighted projective coordinates (x, y, z) , corresponding to the affine coordinates $(x/z_2, y/z_3)$ whenever $z \neq 0$. Weighted projective coordinates have the advantage of allowing point addition on an elliptic curve to be done in 16 field multiplications instead of all field divisions [20], [22]. The steps of the ECDH algorithm are as follows:

- Select a number (P) which must be primary and larger than 3.
- Select two numbers (a, b) . Where $((4a^3 + 27b^2) \bmod P \neq 0)$.
- Find the set of points (G) on the elliptic curve through this equation $y^2 = x^3 + ax + b$ over Z . The addition rule:
 - i. $P + Q = Q + P$ for all $P \in E(Z_P)$
 - ii. if $P = (x, y) \in E(Z_P)$, then $(x, y) + (x_1, -y) = Q$
 $(x_1, -y)$ is denoted by $-P$, and is called the negative of P ; that $-P$ is indeed a point on the curve.
 - iii. Let $P = (x_1, y_1) \in E(Z_P)$ and $Q_2 = (x_2, y_2) \in E(Z_P)$, where $P \neq -Q$.
 Then $P + Q = (x_3, y_3)$, where:

$$x_3 = \lambda^2 - x_1 - x_2 \quad (4)$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \quad (5)$$

$$\text{and } \lambda = (y_2 - y_1)/(x_2 - x_1) \text{ if } P \neq Q \quad (6)$$

$$\lambda = (3x_1^2 + a_1)/2y_1 \text{ if } P = Q \quad (7)$$

Then a random point is chooses from set of points (G) from set of points:

- Choice of a large number n .
- User a key generation:
 - i. Select privet n_A with condition $n_A < n$
 - ii. Calculate public p_A

$$p_A = n_A \times G \quad (8)$$

- User B key generation:
 - i. Select privet n_B with condition $n_B < n$
 - ii. Calculate public p_B

$$p_B = n_B \times G \quad (9)$$

- The two sides exchange keys (p_A, p_B) .
- Calculate of secret key by user A:

$$K = n_A \times p_B \quad (10)$$

- Calculate of secret key by user B:

$$K = n_B \times p_A \quad (11)$$

- Convert the packet data to a set of points (P_m) . And then use the following encryption eq. for P_m :

$$C_m = \{kG, P_m + kP_B\} \quad (12)$$

- Decryption for C_m , use the following:

$$P_m + kP_B - n_B(kG) = P_m + k(n_BG) - n_B(kG) = P_m \quad (13)$$

4.2. RSA algorithm

The original RSA algorithm was publicly illustrated in 1977. This algorithm consists of three stages namely key generation, the encryption and finally the decoding stage. RSA is one of the cryptographic algorithms, which are a non-symmetric type and thus need a pair of keys, one of which is used for encryption and may be non-confidential. The other is the key to decryption, which is private and confidential and authorized only to decrypt the data sent. This algorithm employs two large prime numbers, p and q . The strength of this scheme is based on the difficulty of finding these large initial numbers that are indispensable for finding the secret key while the public key can be freely distributed. The RSA phases and steps of each phase are as follow [24]:

Key generation algorithm:

Step 1: Select or generate two large random prime numbers, p and q .

Step 2: Compute $n = p \times q$.

Step 3: Compute $\phi = (p - 1)(q - 1)$.

Step 4: Select random integer, $1 < e < \phi$, such $GCD(e, \phi) = 1$.

Step 5: Compute, where $d = e^{-1} \text{ mod } \phi$.

Step 6: Public Key: (e, n) .

Step 7: Private Key: (d) .

Encryption process:

Step 1: Suppose entity R needs to send message m to entity S . When m : plaintext.

Step 2: Entity S should send his public key to entity R .

Step 3: Entity R will encrypt m as $m^e \text{ mod } n$, and will send C to entity S .

Where C : cipher text.

Decryption process:

Step 1: Entity S will decrypt the received message as $m = c^d \text{ mod } n$.

4.3. Data aggregation in a secure environment

In CCRM-based HWSN, because it receives, processes, and retransmits data. When compared to an L-Sensor, an H-Sensor requires more energy. This level attempts to reduce the utilization of the H-energy Sensor by allowing it to collect encrypted data from cluster members without having to decrypt it. As a result, the attacker will be unable to listen in on data sent between intermediate nodes. As a result, standard aggregation approaches provide far less privacy. To do that, we use the RSA encryption's addition characteristic. Which allows us to execute arithmetic operations on ciphertext, as it described at previous part from this section A.

In this proposed scheme, each L- sensor senses data m_i , and encrypts it with its key e_i^r as shown in (14) and sends it to its H-Sensor. Where r is the round index in which the node produced the key e_i :

$$c_i = m_i^{e_i^r} \text{ mod } n \quad (14)$$

the H-Sensor collects n messages after receiving sensed data and aggregates them by simply adding them up. as shown in (15):

$$c = \sum_{i=1}^{|N|} c_i = \sum_{i=1}^{|N|} m_i^{e_i^r} \text{ mod } n \quad (15)$$

where $|N|$ is the count of L-sensors in the cluster. After aggregating the data, the final step is to send it to the BS. In order to organize the data that has been aggregated, at the end of the message. H-Sensor will attach all node indexes. Thus, the final version of the sent ciphertext CT to BS in terms of total size $(N * 176 + N * 13)$ bits.

5. SIMULATION PERFORMANCE RESULTS

The system throughput was used to assess the system's performance, energy consumption and the total data rate for sensor nodes rounds [25]. In this section will be describerd the simulation paremeters by matlab and implantation these parameters in second part from this section. Simulation Result to compute the System Performane to get result better than other methods which compared with proposed method.

5.1. Simulation analysis setup

MATLAB R2018a is used to run the simulations. For our suggested technique, 200 L-sensors and 10 H-sensors are randomly deployed in a topographical dimensional for region (100 m x 100 m). Under the chessboard clustering concept H-sensors used the cluster technique, whereas L-sensors were spread around them. On the other hand, for heterogeneous sensor networks the costs of an H-sensor and an L-sensor vary depending on the type of sensor. The manufacturer, other factors, and this is outside the scope of this paper. The simulation runs for 1000 transmission packets (rounds). A single base station gathers data from nodes all throughout town (90 m and 90 m). The 20 and 80 meters of detected transmission, respectively, the starting energy of all L-sensors and H-sensors is 0.5 and 2.5 J, respectively. All sensors are stationary and their locations are known, if adequate energy is available each sensor can communicate directly with the base station. The first radio model is used to implement the methods, it is commonly used in WSNs for evaluating routing protocols [10]. The network simulation parameters are detailed in Table 1. In addition, while constructing the network structure with CC, the nodes are randomly positioned in the field, and the field

center is positioned at a random distance from the base station. To assess the network's security and efficiency, comparison studies are carried out using several state-of-the-art technologies

Table 1. Network simulation parameters

Parameters	Value
Area of Sensor field (meters)	(100 × 100 m)
Sink location (meters)	(90 × 90 m)
Idle State energy	50 nJ/bit
Data aggregation energy	5 nJ/bit
Amplification energy $d \geq d_0$	10 pJ/bit/m ²
H- sensor to base station $d < d_0$	0.0013 pJ/bit/m ²
Amplification energy $d \geq d_1$	$E_{fs}/10 = E_{fs1}$
L-Sensor to H-Sensor	$E_{mp}/10 = E_{mp1}$

5.2. Simulation results

In this section, the ECDH-RSA method under CCRM, the mentioned algorithms ECDH and RSA which described at (section 4.1 and 4.2) are used to encrypt the transmitted data through that network. In this section, the simulation scenarios are really specific to show the effect of encryption operation on the energy consumed of the network sensors under the performance of chessboard clustering, balancing energy consumption by comparing with three methods (Sec-LEACH [26] and SL-LEACH [7], and our proposed). Figure 8 depicts the proposed method's flowchart.

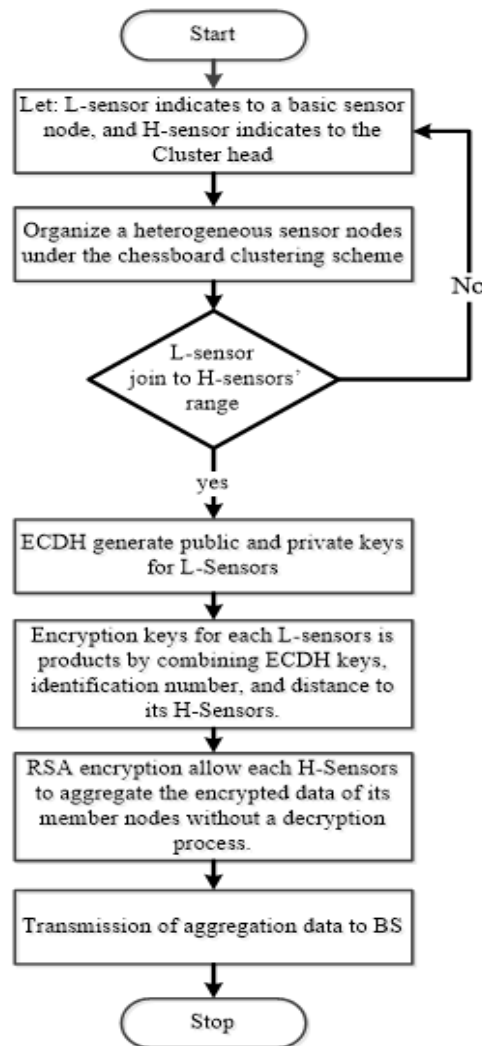


Figure 8. Flowchart for proposed method

Figure 9 depicts the proposed approach as can be observed, outperforms ECDH-RSA in this area. The proposed strategy extended the network lifetime by almost (47% and 35.7%) compared to the (Sec-LEACH, and SL-LEACH) security approaches, respectively. Furthermore, as shown in Figure 9, the suggested method's number of living nodes is always greater than both Sec-LEACH and SL-LEACH. Table 2 displays the various time intervals related to the first dead node as determined by the three different approaches. Clearly, the time it takes for the first node to die in the suggested technique is much longer than in Sec-LEACH and SL-LEACH.

Table 2. Number of rounds to extend the network lifetime by compute first dead node for different approaches

Approaches	Sec-LEACH	SL-LEACH	Proposed
Lifetime of the first dead node (Rounds)	682	917	1439

For the three techniques, Figure 10 shows the total energy consumed by a WSN as a function of transmission rounds. Because it uses less power and has the longest network lifetime, the suggested method outperforms two other ways (Sec-LEACH and SL-LEACH) when the round number in the region grows. This suggests that the proposed strategy achieves a better energy balance in a WSN. The Figures 10-12 shows the energy usage in relation to data rate, simulation rounds, and the number of sensors, respectively. When compared to traditional cheeseboard clustering, the energy consumption during encryption is lower. Table 3 shows that the suggested method beats existing alternatives in terms of energy usage, data rate, and sensor node highest path. When compared to existing ways, we see that the proposed method uses less energy. As a result of the increased power consumption, other nodes were subjected to increased load, reducing the network life node over time. This resulted in lower power usage and a longer network life. In an ideal world, all nodes should have the same amount of leftover energy.

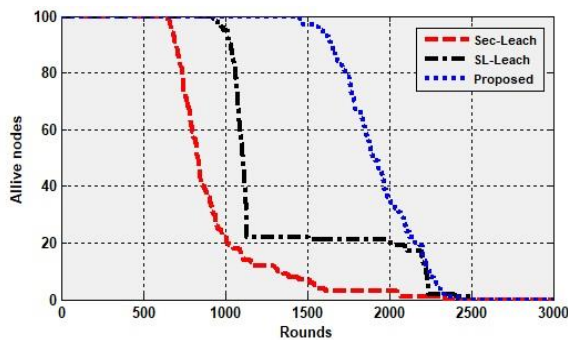


Figure 9. Lifetime simulation of alive node for different different three approaches (Sec-LEACH, SL-LEACH, and proposed method)

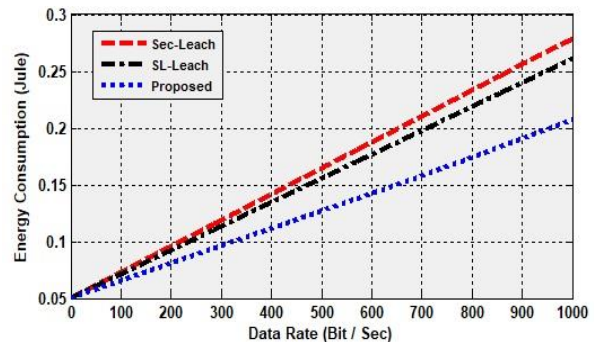


Figure 10. Total energy consumed with respect to data rate for different three approaches (Sec-LEACH, SL-LEACH, and proposed method)

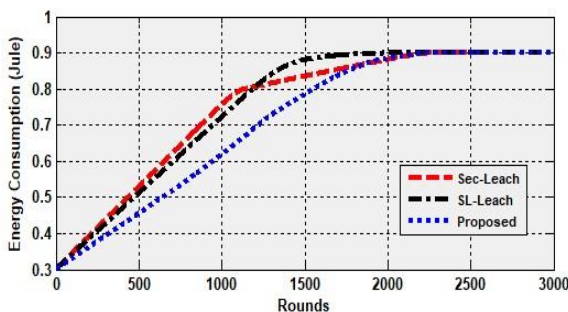


Figure 11. Network energy consumption for different three approaches (S-LEACH, sec-LEACH, and proposed method)

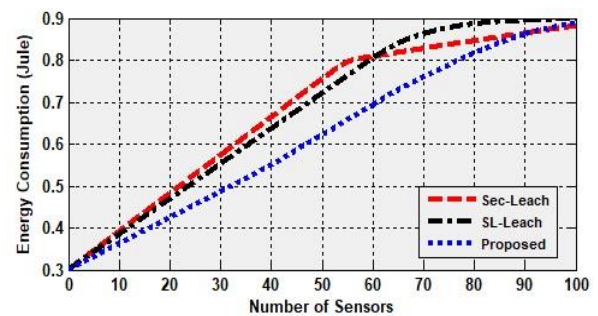


Figure 12. Total energy consumed with respect to number of sensors for different three approaches (Sec-LEACH, SL-LEACH, and proposed method)

Table 3. Energy consumption for three approaches (Sec-LEACH, SL-LEACH, and proposed method)

Method	Data Rate	Simulation Rounds	Sensor Node
Sec-Leach	13.9 %	25.025 %	14.115 %
SL-Leach	17 %	23.884 %	16.926 %
Proposed Method	23 %	18.706 %	20.742 %

6. CONCLUSION

Cheeseboard clustering wireless sensor network has an advantage of choosing the proper path for transmitting the data from the sensors to the base station. The power consumption of encryption during the encryption operation is increased as a tax to make the data transmitted over the network secure. Despite significant advances in secure WSN clustering. In this paper, to secure data transmission in HWSNs with dynamic clustering, we present a unique encryption schema based on ECDH and RSA encryption. The cheeseboard clustering algorithm is used to find the most suitable sensor nodes as H-sensors to relay messages to the base station, with the purpose of maximizing the network's lifetime. Then as a result, even if the H-sensor is compromised, the attacker will not be able to see anything because the H-sensor is not responsible for encrypting signals. In comparison to other ways, the provided results show that this strategy enhances network performance in terms of energy usage significantly.





REFERENCES

- [1] A. Oudjaout, M. Bagaa, A. Bachir, Y. Challal, N. Lasla, and L. Khelladi, "Information Security in Wireless Sensor Networks," in *Encyclopedia on Ad Hoc and Ubiquitous Computing: Theory and Design of Wireless Ad Hoc, Sensor, and Mesh Networks*, 2010, pp. 427-471, doi: 10.1142/9789812833495_0017.
- [2] Y. Sabri and N. El Kamoun, "Attacks and Secure Geographic Routing in Wireless Sensor Networks," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 5, no. 1, pp. 147-158, 2017, doi: 10.11591/ijeecs.v5.i1.pp147-158.
- [3] M. Mohanapriya, N. Joshi, and M. Soni, "Secure dynamic source routing protocol for defending black hole attacks in mobile Ad hoc networks," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 21, no. 1, pp. 582-590, 2021, doi: 10.11591/ijeecs.v21.i1.pp582-590.
- [4] J. Lee, K. Kapitanova, and S. H. Son, "The price of security in wireless sensor networks," *Computer Networks*, vol. 54, no. 17, pp. 2967-2978, 2010, doi: 10.1016/j.comnet.2010.05.011.
- [5] H. Banerjee, S. Murugaanandam, and V. Ganapathy, "A decentralized paradigm for resource-aware computing in wireless Ad hoc networks," *Telecommunication, Computing, Electronics and Control (TELKOMNIKA)*, vol. 17, no. 2, pp. 676-682, 2019, doi: 10.12928/telkomnika.v17i2.9621.
- [6] S. Christodoulou, A. Agathokleous, S. Xanthos, S. Kranioti, and A. Gagatsis, "Analytical and Numerical Models for the Risk-of-Failure Analysis of Urban Water Distribution Network Components," 2012.
- [7] W. Xiao-yun, Y. Li-zhen, and C. Ke-fei, "Sleach: Secure low-energy adaptive clustering hierarchy protocol for wireless sensor networks," *Wuhan University Journal of Natural Sciences*, vol. 10, no. 1, pp. 127-131, 2005, doi: 10.1007/BF02828633.
- [8] S. K. Singh, P. Kumar, and J. P. Singh, "A survey on successors of LEACH protocol," *IEEE Access*, vol. 5, pp. 4298-4328, 2017, doi: 10.1109/ACCESS.2017.2666082.
- [9] M. Masdari, S. M. Bazarchi, and M. Bidaki, "Analysis of secure LEACH-based clustering protocols in wireless sensor networks," *Journal of Network and Computer Applications*, vol. 36, no. 4, pp. 1243-1260, 2013, doi: 10.1016/j.jnca.2012.12.017.
- [10] S. Prakash and A. Rajput, "Hybrid Cryptography for Secure Data Communication in Wireless Sensor Networks," in *Ambient Communications and Computer Systems*, 2018, pp. 589-599, doi: 10.1007/978-981-10-7386-1_50.
- [11] S. Ozdemir, "Secure and reliable data aggregation for wireless sensor networks," in *International Symposium on Ubiquitous Computing Systems*, pp. 102-109, 2007, doi: 10.5555/1775574.1775585.
- [12] V. Krishnaswamy and S. K. S. Manvi, "Clustering and data aggregation scheme in underwater wireless acoustic sensor network," *Telecommunication, Computing, Electronics and Control (TELKOMNIKA)*, vol. 17, no. 4, 2019, doi: 10.12928/telkomnika.v17i4.11379.
- [13] Q. Zhou, G. Yang, and L. He, "A secure-enhanced data aggregation based on ECC in wireless sensor networks," *Sensors*, vol. 14, no. 4, pp. 6701-6721, 2014, doi: 10.3390/s140406701.
- [14] G. De Meulenaer, F. Gosset, F.-X. Standaert, and O. Pereira, "On the energy cost of communication and cryptography in wireless sensor networks," in *Networking and Communications, 2008. WIMOB'08. IEEE International Conference on Wireless and Mobile Computing*, 2008, pp. 580-585, doi: 10.1109/WiMob.2008.16.
- [15] O. Younis and S. Fahmy, "HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks," *IEEE Transactions on mobile computing*, no. 4, pp. 366-379, 2004, doi: 10.1109/TMC.2004.41.
- [16] A. D. Amis, R. Prakash, T. H. Vuong, and D. T. Huynh, "Max-min d-cluster formation in wireless ad hoc networks," in *Proceedings IEEE INFOCOM 2000. Conference on Computer Communications. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies (Cat. No. 00CH37064)*, 2000, pp. 32-41, doi: 10.1109/INFCOM.2000.832171.
- [17] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proceedings of the 33rd annual Hawaii international conference on system sciences*, 2000, doi: 10.1109/HICSS.2000.926982.
- [18] Z. Zhang, M. Ma, and Y. Yang, "Energy-efficient multihop polling in clusters of two-layered heterogeneous sensor networks," *IEEE Transactions on Computers*, vol. 57, no. 2, pp. 231-245, 2008, doi: 10.1109/IPDPS.2005.198.
- [19] B. Abood and Y. K. Al-Rikabi, "Lifetime enhancement for clustering protocols in heterogeneous wireless sensor networks," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 14, no. 3, pp. 1305-1314, 2019, doi: 10.11591/ijeecs.v14.i3.pp1305-1314.
- [20] R. R. Ahirwal and M. Ahke, "Elliptic curve diffie-hellman key exchange algorithm for securing hypertext information on wide area network," *International Journal of Computer Science and Information Technologies*, vol. 4, no. 2, pp. 363-368, 2013.





- [21] M. Elhoseny, H. Elminir, A. Riad, and X. Yuan, "A secure data routing schema for WSN using elliptic curve cryptography and homomorphic encryption," *Journal of King Saud University-Computer and Information Sciences*, vol. 28, no. 3, pp. 262-275, 2016, doi: 10.1016/j.jksuci.2015.11.001.
- [22] K. Lauter, "The advantages of elliptic curve cryptography for wireless security," *IEEE Wireless communications*, vol. 11, no. 1, pp. 62-67, 2004, doi: 10.1109/MWC.2004.1269719.
- [23] Q. Jiang, J. Ma, F. Wei, Y. Tian, J. Shen, and Y. Yang, "An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks," *Journal of Network and Computer Applications*, vol. 76, pp. 37-48, 2016, doi: 10.1016/j.jnca.2016.10.001.
- [24] J. Surekha and M. Anita, "Analysis of RSA and ELGAMAL Algorithm for Wireless Sensor Network," *International Journal of Computer Techniques*, vol. 2, no. 4, pp. 25-31, 2015, doi: 10.1007/978-3-642-14478-3_18.
- [25] M. Tamrin and M. Ahmad, "Simulation of adaptive power management circuit for hybrid energy harvester and real-time sensing application," *International Journal of Power Electronics and Drive Systems (IJPEDS)*, vol. 11, no. 2, p. 658, 2020, doi: 10.11591/ijpeds.v11.i2.pp658-666.
- [26] L. B. Oliveira, A. Ferreira, M. A. Vilaça, H. C. Wong, M. Bern, R. Dahab, and A. A. Loureiro, "SecLEACH-On the security of clustered sensor networks," *Signal Processing*, vol. 87, no. 12, pp. 2882-2895, 2007, doi: 10.1016/j.sigpro.2007.05.016.

BIOGRAPHIES OF AUTHORS







Basim Abood     was born in Thi-Qar City, Iraq, in 1984. He received the B.Sc. degree from University of Basra (UoB), Basra, Iraq, in Electrical Engineering, in 2007. He received his M.Sc. and Ph.D degrees from Huazhong University of Science and Technology (HUST), China, in 2013 and 2016 respectively, in Telecommunication and Information Engineering. Currently he is Assistance Proof, working Head of Computer Science Department, College of Computer Science and Information Technology, university of Sumer, Iraq. His research interests include digital communication, wireless sensor networks, mobile and Ad-hoc network (MANET), network security, artificial intelligence, and LTE- A cellular network. He can be Contacted at email: bas.eng1984@gmail.com, b.abood@uos.edu.iq.



Abeer Naser Faisal     received the B.Sc. degree in computer science from the University of Thi-Qar, Iraq, the M.Sc. degree in computer science from the University of Basrah, Iraq. She is currently a director in the Department of Computer Information Systems, University of Sumer. She has supervised more than 10 graduate projects. She has authored or coauthored more than 15 publications, with 2 H-index and more than 10 citations. Her research interests include image processing, biometrics, and pattern recognition and machine learning. She can be contacted at email: a.nasir@uos.edu.iq, abeernaser13@gmail.com.



Qasim Abduljabbar Hamed     was born in Thi-Qar City, Iraq, He received the B.Sc. degree from University of Baghdad, Baghdad, Iraq, in Information Technology, in 2010. He received his M.Sc in information technology in 2015 Russia Workplace. He is Currently Working as manager for Computer Center in University of Sumer-Iraq. His research interests include digital communication, wireless sensor networks, mobile and Ad-hoc network (MANET), network security, artificial intelligence, and LTE-A cellular network. He can be contacted at email: qalrikabi@gmail.com, q.alrikabi@uos.edu.iq.