JOURNAL OF SOFT COMPUTING AND DATA MINING
e-ISSN: 2716-621X

JSCDM

Vol. 5 No. 2 (2024) 52-61
https://publisher.uthm.edu.my/ojs/index.php/jscdm

Optimizing Security in LEACH-based WSN Using Advanced n-RSA Encryption

Ruwaida Mohammed Yas[1]*, Sanaa Ahmed Kadhim[2], Saad Abdual Azize Abdual Rahman[3], Ali Kadhim Bermani[4,5], Taher M. Ghazal[6]

[1] *Information Institute for Postgraduate Student, University of Information Technology and Communications, 10066, Baghdad, IRAQ*
[2] *Bioinformatics, Biomedical Informatics college, University of Information Technology and Communications, 10066, Baghdad, IRAQ*
[3] *Department of Computer Engineering Techniques, Almamoon University Collage, Baghdad, IRAQ*
[4] *Computer Techniques Engineering Department, College of Engineering and Technologies, Al-Mustaqbal University, 51001, Babylon, IRAQ*
[5] *College of Information Technology, University of Babylon, 51001, Babylon, IRAQ*
[6] *Research Innovation and Entrepreneurship Unit, University of Buraimi, 512 Buraimi, OMAN*

*Corresponding Author: roueida.m.yas@iips.edu.iq
DOI: https://doi.org/10.30880/jscdm.2024.05.02.004

Article Info

Received: 1 May 2024
Accepted: 11 November 2024
Available online: 18 December 2024

Keywords

Wireless sensor networks (WSNs), low-energy adaptive clustering hierarchy (LEACH) protocol, cryptosystem, n-RSA

Abstract

Wireless sensor networks (WSNs) have had many problems up until now because they are open, adaptable, and limited in resources. These problems have included privacy, effectiveness, and consumption of energy. Sensitive information should always be transmitted over wireless networks with extreme caution because public communications on these networks are sometimes unreliable. Although hierarchical routing methods may handle many applications, there are difficult problems with cluster head (CH) selection and network overload distribution. The secure low energy adaptive clustering hierarchy (SLEACH) protocol Cryptographic n-RSA method (SLEACH-n-RSA) is introduced in this work to improve network longevity, reduce energy consumption, and guarantee high security. The initial step of the SLEACH-n-RSA protocol is to use the improved LEACH protocol, which is based on the estimated remaining energy (ERE) and depleted energy (DE) for setting the threshold function value that will decide who will be the CH and how the cluster will form. In the second step, the suggested n-RSA encryption algorithm has been used to ensure the confidentiality of the transmitted data. The performance analysis of the proposed SLEACH-n-RSA protocol shows better performance results when compared with other currently used protocols in terms of network lifetime, packet delivery ratio, energy consumption, and execution time. The experimental results show that the proposed protocol outperforms other existing protocols.

1. Introduction

The environment surrounding us is replete with various phenomena, several of these phenomena may offer different advantages for human beings, while others have the potential to result in various disasters. Preventing troubles and getting the maximum benefits will be gained by essentially monitoring the environment's events. Wireless sensor networks (WSNs) are employed to achieve that objective. One of the most critical problems with the traditional tools used for such applications is the import ability, the limited area structure caused by wires, and the large sizes of those devices. Therefore, WSN overcomes these problems and is the most appropriate instrument for remotely monitoring environment events due to its ability to be configured and positioned in different locations without predefined structure limitations [1].

WSN is built from tens of sensors that can sense the environment despite their low cost and limitations, such as limited storage, energy, range of communication, and processing power. These devices collect data about the environment area from sensors and then send it to the base station (BS) or a sink [2]. WSNs are built either as a flat architecture or as a clustered-based architecture. A flat architecture is built when the sensed data is transmitted to BS directly or through another WSN node. In the clustered architecture, the cluster is built by grouping many sensor nodes. Within this cluster, one node assumes the role of a CH and manages the communication among all the nodes. The sensor nodes (SNs) communicate with the BS via the CHs [3].

However, WSNs have several difficulties [4], [5], the most crucial being the energy consumption required to perform different functions such as sensing, processing, and transmitting/receiving. The primary concern for WSN is energy consumption. Each node in the network operates on a finite energy source, and a significant amount of energy is expended during transmission. Another crucial factor is the interaction with the base station. Typically, nodes possess a limited communication range. Hence, the selection and implementation of routing protocols significantly impact the communication and overall performance of WSNs. The topic of security is important and is seen as a grave matter. In WSN, the data is transmitted across the air, where everybody can access it, allowing anybody to view and engage in communication [6, 7]. Therefore, enhancing the robust, fast, and lightweight public key encryption technique is important to safeguard the transmitted data in the WSN.

Correspondingly, the compact nature of the sensor is an essential feature of the WSN, enabling its portability and access to risky locations. However, this feature also creates certain limitations on the WSN, such as limited energy capacity and a short operational lifespan. Therefore, it is necessary to have an elastic routing protocol to use all the benefits of the WSN while increasing energy efficiency. From this perspective, a proposal has been made to improve the widely used routing algorithm for WSN, known as the low energy adaptive cluster hierarchy (LEACH). For all the reasons mentioned previously and others, the secure LEACH protocol with the new n-RSA Cryptographic approach (SLEACH-n-RSA) protocol is suggested to ensure network load security and balance. Security is a fundamental area of study in WSN. Hence, security analysis is conducted autonomously to enhance the secure transmission of data.

The main objective of this study is to introduce an improved LEACH protocol for increasing the network lifetime and a novel approach for generating cryptographic keys using given mathematical equations and applying these keys in the encryption of images conveyed via WSN. The major contribution of this proposed protocol is shown as follows:

- Suggest an enhanced adaptive routing protocol with low energy consumption based on the sensors' energy depletion (ED) to decrease the network's overall energy consumption and consequently prolong its operational lifespan.
- Utilize the energy for the threshold that is used for CH selection
- Introduce a novel n-RSA cryptographic algorithm designed to generate robust encryption keys for both sensed data (text and image) and transmitted data in the NW, thereby ensuring the security of transmitted data.
- Offer an encryption algorithm that operates at a high speed.

2. Literature Review

Several research studies have proposed various encryption algorithms, such as symmetric, public key, or hybrid encryption, to secure small devices in limited contexts like WSN. In [6], CH selection is determined by utilizing the swarm intelligence algorithm in conjunction with the LEACH protocol. The hybrid ant colony and modified Particle swarm method are employed to select the cluster heads. The CH selection is determined by residual energy and the number of successful transmissions by the node. The node's trustworthiness is evaluated based on transmission nodes and residual energy. These parameters play a crucial role in guaranteeing the security of both data and energy. The suggested system employs the modified RSA digital signature algorithm technique to provide network security during data cryptography. In this work, the security of images needed to be demonstrated.

The authors in [7] proposed a novel encryption scheme utilizing Elliptic Curve key selection and Hill Cypher encryption. The keys are permuted to increase the key size, ensuring compatibility with the image matrix size. This results in secure transmission through wireless sensor networks by effectively encrypting the transmitted

images. Presently, a secure transmission framework is suggested that utilizes clusters to enhance the effectiveness of the proposed secure routing algorithm, known as the Elliptic curve Hill cipher and Cluster-based Encrypted Routing Algorithm. This framework aims to increase security, reduce delay, and improve the packet delivery ratio. The main drawback of their proposal is that a heavy-weighted key was used. In their study, Paper [8] proposed a new approach to enhance the security of data transmission in WSN by utilizing the homomorphic encryption algorithm and the elliptic curve cryptography (ECC) algorithm. The ECC was employed to exchange public and private keys because it provides strong security using a compact key size. The suggested 176-bit encryption key is generated by combining the ECC key, node identification number, and distance to the CH. Homomorphic encryption enables energy savings by aggregating encrypted data without needing prior decryption. Certain nodes, specifically cluster-head nodes, are not responsible for encrypting communications. They demonstrated their technique's applicability for encrypting text and images, but they did not consider the duration of the encryption process.

The researchers in [9] introduced a LEACH using RSA encryption to ensure safe data transmission across sensor nodes in the WSN. Initially, energy is distributed to every sensor node in the WSN. The setup and steady-state constitute the initial two stages of implementation. Once the CH in the WSN is selected, the RSA algorithm encodes the data before being transmitted from the source node to the destination node. Then, it is decoded while it is received at the destination node. After completing rounds, the dead nodes and the consumed energy are computed. The researchers used the traditional asymmetric RSA algorithm, which is insecure enough and operates slowly.

In the paper [10], the researchers used an asymmetric ECC algorithm for cryptographic key generation. Then, the advanced encryption standard (AES) and ECC cryptography combinations are performed for data encryption and decryption. To improve energy efficiency, network lifetime, and data security, an enhanced algorithm that combines the regular LEACH protocol with both symmetric AES and symmetric ECC cryptographic algorithms. The proposed method effectively addresses the key exchange issue that impacts AES. In this study, the authors employ a combination of AES and ECC to enhance the security of data transmission using WSN. However, it is important to note that this approach may significantly delay data transmission.

Various methods have been suggested for securing the transmitted data in WSNs. Every one of them was effec-tive in many applications. However, no particular model provides fast execution, high security, and high throughput when interacting with WSNs. As a result, a new security algorithm is proposed for efficient data transmission with high security, fast, and high throughput.

3. Materials and Methods of Research

This section presents the original LEACH protocol and the proposed SLEACH-n-RSA protocol.

3.1. LEACH Protocol

The LEACH protocol is widely regarded as the main clustering-based routing protocol for extending the lifespan of networks and achieving scalable solutions. It accomplishes this by minimizing overall energy usage through equitable workload distribution across nodes at various locations [11]. The clusters in the sensor network consist of a hierarchical organization of sensor nodes, with each cluster having a CH. However, CH is utilized to gather data from all nodes, consolidate it, and direct it towards the SINK node [12].

The LEACH protocol selects a node as the CH if it has a probability, determined by a randomly generated value between 0 and 1, that is less than the specific threshold Th(n), which is calculated using (1) [13]. Within a specific cluster, the remaining nodes are connected based on the selection of the CH, which can be accessed with the minimum amount of communication energy. To prevent the depletion of the battery in a single sensor node, the role of the CH is rotated among all nodes [14].

$$Th(n) = \begin{cases} \dfrac{P}{1 - P[\left(r \bmod \frac{1}{P}\right)]}, if\ n \in G \\ 0 \qquad\qquad\qquad\qquad , otherwise \end{cases} \tag{1}$$

In this context, P represents the probability value, r is the round number, and $Th(n)$ denotes the threshold value of the nodes. Within the network, every node selects a random integer ranging from 0 to 1.

The LEACH operation consists of two distinct rounds: the setup phase, which organizes nodes into clusters, and the steady-state phase, which is responsible for data transmission from source to SINK nodes [15]. A longer duration characterizes the steady-state phase to minimize overhead when compared to the setup phase. Once a node is selected as a CH during the setup phase, it broadcasts an advertisement message. To be included in a specific cluster, each individual node that is not part of a cluster will be selected based on its ability to receive messages [15]. During the steady-state phase, each member node transmits data while aggregating the received data from other nodes within the cluster using a CH and sending it toward the SINK. The control information

originating from the SINK is unnecessary for LEACH because nodes do not require knowledge about the global network [1].

3.2. The Proposed Method

The suggested method, SLEACH-n-RSA, combines n-RSA cryptography with an improved LEACH protocol to optimize power usage and prolong the network's lifespan. This methodology consists of two steps that enhance the security of WSNs. The improved LEACH approach, which relies on ED and estimated remaining energy (ERE) for cluster formation and CH selection, is implemented in the initial phase. The second step utilizes the advanced n-RSA cryptography algorithm to ensure the security and integrity of data during transmission. The block diagram depicted in Fig. 1 illustrates the research technique and methods employed for hybrid cryptography and clustering-based secured and energy-efficient data transmission.

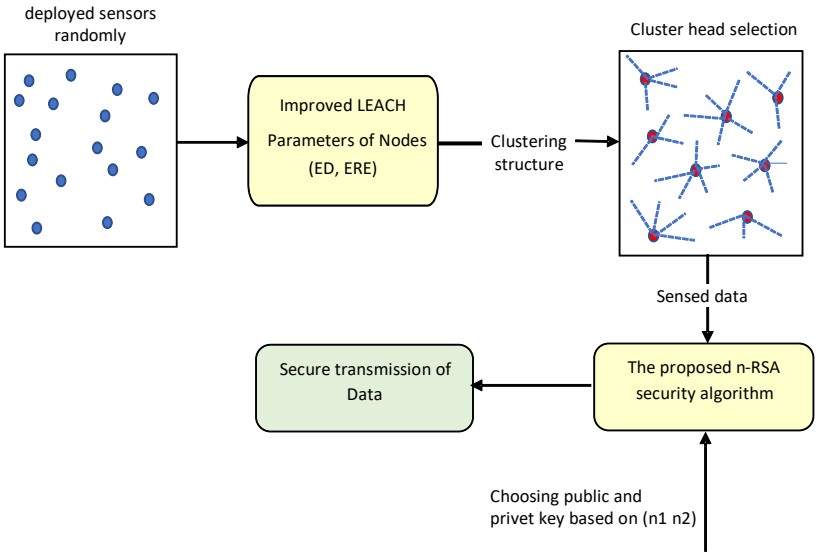

Fig. 1 *General structure for developing our proposed method for safe data transmission*

3.2.1. Key Generation Utilizing the Suggested n-RSA

Assume that n consists of six prime numbers that will be used as input for generating n1 and n2. Instead of using a single number for private and public keys, one number was used for encryption and another for decryption. The two numbers (n1, n2) were computed using the proposed approach to ensure they meet the requirements of the encoding-decoding procedure. This technique will increase the intricacy of uncovering the keys or even a portion thereof.

3.2.2. Proposed n-RSA Steps

In the proposed n-RSA algorithm, the following steps are used for encryption and decryption:
Let p_i be a set of prime numbers {p_i: i= 1 ...n, p_i is the prime number. Calculate n_1 and n_2 using the product operation as the following:

$$n_1 = \prod_{i=1}^{n} p_i \tag{2}$$

Where (i=1 to n)

$$n_2 = \prod_{i=1}^{n-1} p_i \tag{3}$$

Where (i=1 to n-1)

1. Select a value for e that is larger than 1 but less than n_1 (1 < e < n_1), ensuring that the greatest common divisor between e and n_1 is equal to 1 (gcd (e, n_1)=1).
2. public key will be: P(k) = (e, n_1)
3. Select the value of d to be the multiplication of e with d mod (n_2) equivalence to as shown in (3):

$$e \times d \bmod n = 1 \tag{4}$$

The Private key will be: S(k)=(d, n_2) and plain Message (M) encrypted using the following equation:

$$C = M * e \bmod (n_1) \tag{5}$$

Ciphered message (C) decrypted using the following equation:

$$M = C * d \bmod (n_2) \tag{6}$$

3.2.3. The Enhanced LEACH Protocol

In the traditional LEACH protocol, the selection of Cluster Heads (CH) begins with the nodes generating a random number. Subsequently, the randomly produced number is compared to the predetermined threshold. If the random value of a node is significantly smaller than the threshold, the node will transition to the state of CH for that round. Despite the various benefits offered by the LEACH protocol, the CH cannot guarantee its current residual energy. The original LEACH protocol uses threshold Th(n) to select the sensor node as a CH without considering their energy levels. So, CH selection based on minimum energy can lead to early death of these CHs, and this will lead to premature death of the WSN. To overcome this problem, a new technique is proposed, which is based on two factors for CH selection: ERE and ED. This technique aims to maximize the WSN lifetime and enhance its performance. To make the selection process of the CH more efficient in terms of energy, the value random number is modified by multiplying it with the generated random number with the ED and ERE values of the sensors' node. ED and ERE can be clarified as follows:

ED provides the percentage of the sensor's energy that was depleted during the previous rounds. Calculating this parameter in (7) is essential for preventing the selection of the same node as a CH in the next rounds.

$$ED = \frac{E(t)_{init} - E(t)_{res}}{(r-1)^t} \tag{7}$$

Where $E(t)_{init}$ represents the initial energy, while $E(t)_{res}$ represents the residual energy of each node. R represents the current round, and r – 1 represents the previous round at time t. The ED performance of the previous round will be used as a criterion for selecting CH in the next round. Where the node with the lowest ED at the end of the previous round will selected as a CH at the next round. Since a CH from the previous round has a higher ED than other non-CH nodes, it will be excluded from being selected as a CH in the next round.

ERE ratio is represented by calculating the difference between the initial energy ($Einit$) and the total energy (Etotal). In this scenario, the ERE is used instead of residual energy (E_{res}) to avoid selecting CH candidate networks from weaker nodes. The ERE of node (n) can be computed using (8) as follows:

$$ERE(n) = E_{init}(n) - E_{total}(n) \tag{8}$$

The E_{total} of node n can be determined using (9):

$$E_{total}(n) = E_{i,j} + E_{i\ to\ BS} + E_{elec} + E_{DA} \tag{9}$$

Here, $E_{i,i}$ and $E_{i\ to\ BS}$ represent the energy used to transmit "l" bits from node "i" to "j" and from node "i" to the base station or sink, respectively. In addition, E_{DA} refers to the total energy of a given data point, while E_{elec} represents the energy consumed by the receiving circuit for each individual bit.

The typical LEACH protocol uses the symbol (n) for random number representation. While in the suggested method, an altered random number $rand'(n)$ is used, and it can be calculated using (10):

$$rand'(n) = rand(n) * (DE_n + ERE_n) \tag{10}$$

Then, the value of $rand'(n)$ is compared to the sensor nodes' thresholds Th(n). The threshold function must be considered when deciding to choose CH, where the threshold function determines the node's probability of being a CH. For stabling the energy consumption of the network, each node has the possibility of being selected as a CH. There is an equal chance for each candidate node in the network to be selected as the CH. The capacity of a node to operate as a CH in the network is contingent upon its energy level. The proposed approach utilizes the energy of each node, starting with the initial node in the network and extending to the final node, to execute the threshold function.

At this point, the altered random number is assessed in reference to the threshold function (11).

$$ran(n)' \leq Th(n) \tag{11}$$

Where $Th(n)$can be represented as (12):

$$Th(n) = \begin{cases} \frac{P_n}{\{1-P_n[(r \bmod \frac{1}{P_n}} * (ED + ERE) + \frac{r}{P_n}, & if\ n \in G \\ 0, & otherwise \end{cases} \tag{12}$$

In the given equation, Pn represents the probability of n transitioning to CH, while r represents the round number. If the random number is below the threshold, the node is elevated to CH status; otherwise, the algorithm proceeds to the next node in the list. Once the CH selection process concludes, the CHs will disseminate the information to the remaining nodes in the network, notifying them of their selection to serve as the CH for this particular iteration. To properly complete this procedure, each CH node will inform every other node in the network through a broadcast message that is camouflaged as an advertisement. Each member node utilizes the signal strength of the message sent from the CH nodes to determine its participation in the cluster-building process. Fig. 2 illustrates the flow of the enhanced LEACH protocol.

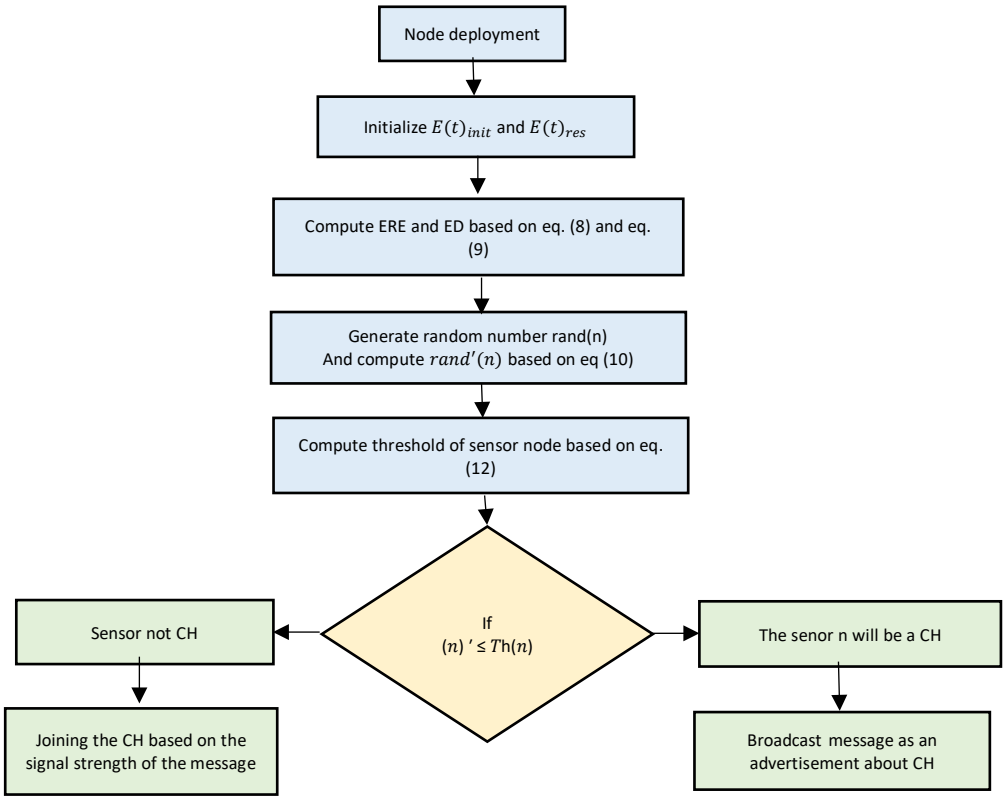

Fig. 2 *The flow of the enhanced LEACH protocol*

3.2.4. The Proposed SLEACH-n-RSA Routing Algorithm

The proposed SLEACH-n-RSA Protocol is presented in steps as described below:

Step 1: In the first round, the CH choosing and stabilization happen right away. A control packet sent through CH tells each sensor node in this cluster to send data to the BS.
Step 2: BS selects n of prime numbers, then calculates n_1, n_2 using eq. (2) and eq. (3)
Step 4: By applying eq. (4), BS determines its private key (d).
Step 5: Based on the data it receives from CHs, BS uses the control packet to broadcast its public key.
Step 6: Every individual node within the cluster sends the control packet to the SN within a designated region. The number of control packets received simultaneously with the total number of neighboring nodes is verified.

Step 7: Every cluster member meets the criteria to be a CH based on the expected threshold value from eq.(12), which is based on ED and estimated residual energy. In an actual round, it primarily checks to see if the selected sensor node becomes a CH.
Step 8: All SNs use BS's public key and eq. (5) to encrypt the sensed data.
Step 9: The SN sends control and data packets to the CH that include the most recent data and acquired information. The data is encrypted before being sent to the CH and subsequently from the CH to the BS.
Step 10: Redo the steps from 2 to 6.
Step 11: BS decrypts the received data using its private key and eq.(6).
Step 12: Upon the death of several nodes, the algorithm reaches a definitive conclusion.

The above algorithm steps show how to combine the enhanced LEACH clustering based on energy to prolong the network lifetime with the proposed n-RSA to protect data sent over the network; the use of two-key encryption guarantees the protection of data from forgery or interception.

4. Results and Discussions

This section has three subsections: the experiment's setup, evaluation metrics, and experiment analysis. The proposed protocol was evaluated using MATLAB R2019b with the settings listed in Table 1.

Table 1 *Simulation's parameters*

Parameter	Value
Initial sensor nodes' energy	0.5 J
Location of the Sink	(50,100)
Maximum communication range	100
$E_{ele}, \varepsilon_{fs}, \varepsilon_{mp}$	50nJ/bit,10pJ/bit/m2, 0.0013pJ/bit/m4
d0 (reference distance)	square root ($Efs/Eamp$) = 87 m
Data packet	4000 bit

The proposed (SLEACH-n-RSA) performance is evaluated using network lifetime (NWL), packet delivery ratio (PDR), and energy consumption (EC) parameters.

1. Network lifetime (NWL): This term refers to when the network is completely operational. Consider the first node transmitting data or packets with insufficient energy, which may result in lost functionality.
2. Packet delivery ratio (PDR): It compares the number of successfully received packets to the total number transmitted by the source node.
3. Energy consumption (EC): EC represents the total energy a sensor node consumes during data transmission.

The suggested system demonstrated exceptional speed and efficiency, making it very suitable for the WSN's constrained capabilities. This was demonstrated by comparing it to another encryption method. The following components are required to evaluate the n-RSA security algorithm speed: a key generation method, an encryption algorithm, and a decryption algorithm. The comparison takes place among the proposed n-RSA, the ECC with Hill cipher [11], RSA [13], and ECC with AES [14], as displayed in Table 2.

Table 2 *Comparison between execution time*

Text size (bytes]	Proposed n-RSA	Ref. [11]	Ref. [13]	Ref. [14]
192	5.72 s	9.04 s	15.12 s	62.08 s
786	6.61s	19.91 s	75.08 s	40.71 s
1216	7.31 s	21.75 s	79.36 s	23.11 s
1560	8.24 s	22.79 s	89.14 s	11.14 s

The data shown in the table demonstrates that the suggested method has a shorter execution time with different text sizes compared to other algorithms. The proposed n-RSA still takes less execution time even as the size of the text increases, which will reduce the sensor's energy consumption.

Our proposed algorithm extends the NWL more than other systems in [11], [13], and [14], Due to the use of the new formula for the enhanced LEACH protocol which depends on the ERE and ED for choosing the CH, as shown in Fig. 3. We can notice that the first node died in round number 1600, while the last node died in round 2100. Moreover, the proposed algorithm utilizes a secure cluster-based infrastructure for transferring data effectively and securely in WSNs, so the NWL of the network can be increased.

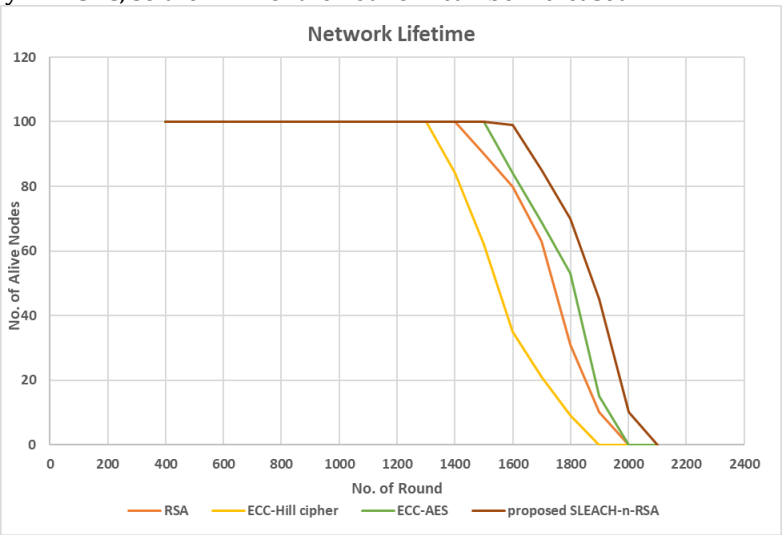

Fig. 3 *Comparison between the NWL*

Fig. 4 presents the improvement in PDR for the suggested (SLEACH-n-RSA) in comparison with [11], RSA [13], and [14]. As shown in the figure below, the amount of PDR in the proposed protocol was higher than in the comparative methods, which means that the amount of data processed in the proposed method was more than in the other methods. This is because enhanced encryption technology will protect the data during the routing process. When the network size is 1 (i.e., 100 nodes), 97% of the packets were delivered, while when the network size is 9 (i.e., 900 nodes), 81% of the packets were delivered to BS. Increasing the number of sensors in the network increases the load on the CHs and thus will lead to the dropping of the packets.

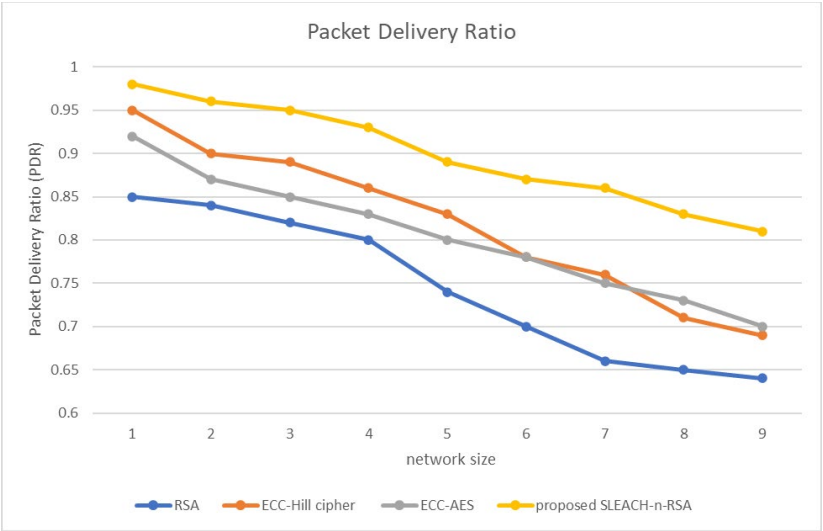

Fig. 4 *Comparison between the PDRs*

Because the sensors in WSN are not recharged and replaced, it is important to preserve their energy. Fig. 5 shows that the proposed (SLEACH-n-RSA) technique consumes less energy than other existing algorithms employed in [11], [13], and [14]. Which will extend the WSN lifetime. The reduction of energy consumption is because of the shorter execution time of the proposed n-RSA method, which needs less processing.

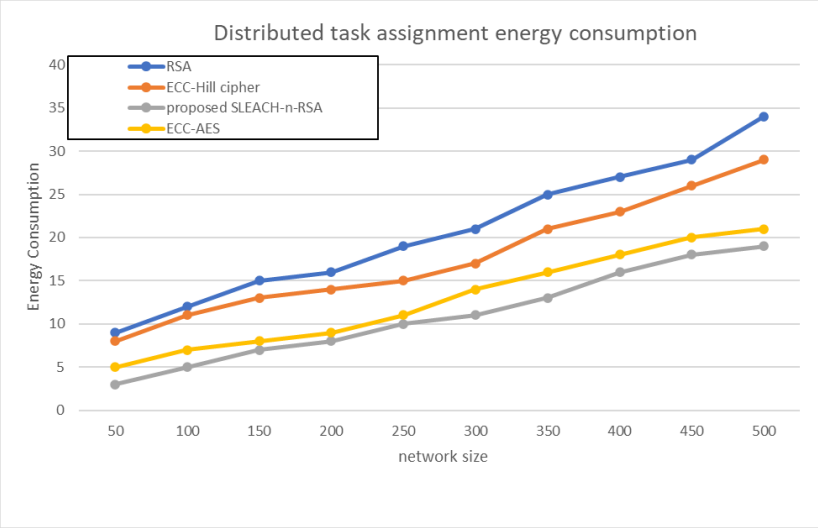

Fig. 5 *Comparison between ECs*

5. Conclusion

This work proposed a SEACH-n-RSA protocol to improve the WSN performance by balancing energy consumption, extending the network lifetime, and increasing PDR. The essential elements used to enhance WSN security are CH selection, cluster formation, and cryptography. Here, cluster creation and CH selection are carried out using the enhanced LEACH protocol, which is based on combining the ERE and ED to determine the value of the threshold function. The cryptographic phase uses the n-RSA algorithm to ensure data integrity and secure data transmission during the transmission. The proposed system has been evaluated; we notice an increase in the network lifetime by 30%, an increase in the PDR by 15%, and a reduction in energy consumption to 20%. The limitation of the proposed protocol is the single hop from CH to BS, which will reduce the scalability of the network. Future techniques involve the implementation of mobile sink nodes, which employ an assortment of meta-heuristic techniques to mitigate energy utilization. Furthermore, we intend to investigate and evaluate the most significant impacts of various distribution techniques on the security of WSN routing.

Acknowledgements

The authors have no financial support or academic advice for our research.

Conflict of interest

The authors declare that there are no conflicts of interest regarding the publication of this manuscript.

Author Contribution Statement

Ruwaida Mohammed Yas, Sanaa Ahmed Kadhim, and Saad Abdual Azize Abdual Rahman: ***proposed the research problem****. Ruwaida Mohammed Yas, Sanaa Ahmed Kadhim, Saad Abdul Azize Abdul Rahman, Ali Kadhim Bermani, and Taher M. Ghazal:* ***developed the theory and performed the computations****. Ruwaida Mohammed Yas, Sanaa Ahmed Kadhim, Saad Abdual Azize Abdual Rahman, Ali Kadhim Bermani, and Taher M. Ghazal:* ***verified the analytical methods and investigated and supervised the findings of this work****. All authors discussed the results and contributed to the final manuscript.*

References

[1] Mohammed, F. A., Mekky, N., Suleiman, H. H., & Hikal, N. A. (2022). Sectored LEACH (S-LEACH): An enhanced LEACH for wireless sensor network. IET Wireless Sensor Systems, 12(2), 56-66. https://doi.org/10.1049/wss2.12036

[2] Abu Salem, A. O., & Shudifat, N. (2019). Enhanced LEACH protocol for increasing a lifetime of WSNs. Personal and Ubiquitous Computing, 23(5), 901-907. https://doi.org/10.1007/s00779-019-01205-4

[3] Sinde, R., Begum, F., Njau, K., & Kaijage, S. (2020). Refining network lifetime of wireless sensor network using energy-efficient clustering and DRL-based sleep scheduling. Sensors, 20(5), 1540. https://doi.org/10.3390/s20051540

[4] Potnis, A., & Rajeshwari, C. S. (2015, March). Wireless sensor network: challenges, issues and research. In Proceedings of 2015 International Conference on Future Computational Technologies (ICFCT'2015) (pp. 224-228). https://doi.org/10.17758/ur.u0315268

[5] Farooq, U. (2019). Wireless sensor network challenges and solutions. Virtual University of Pakistan, 1-6.
https://doi.org/10.5772/intechopen.109238

[6] Jancy, Y., & Gomathy, B. (2023, December). An Optimized Cluster Head Selection and Secured Wireless Sensor Network Using MRSA. In Proceedings of the Bulgarian Academy of Sciences (Vol. 76, No. 12, pp. 1876-1884). https://doi.org/10.7546/crabs.2023.12.10

[7] Ramasamy, J., & Kumaresan, J. S. (2020). Image encryption and cluster based framework for secured image transmission in wireless sensor networks. Wireless Personal Communications, 112(3), 1355-1368. https://doi.org/10.1007/s11277-020-07106-7

[8] Elhoseny, M., Elminir, H., Riad, A., & Yuan, X. (2016). A secure data routing schema for WSN using elliptic curve cryptography and homomorphic encryption. Journal of King Saud University-Computer and Information Sciences, 28(3), 262-275. https://doi.org/10.1016/j.jksuci.2015.11.001

[9] Aruna Deepthi, S., Aruna, V., & Leelavathi, R. (2022). Image Transmission Using Leach and Security Using RSA in Wireless Sensor Networks. In Computational Vision and Bio-Inspired Computing: Proceedings of ICCVBIC 2021 (pp. 39-51). Singapore: Springer Singapore.
https://doi.org/10.1007/978-981-16-9573-5_3

[10] Hodowu, D. K. M., Korda, D. R., & Ansong, E. D. (2020). An enhancement of data security in cloud computing with an implementation of a two-level cryptographic technique, using AES and ECC algorithm. Int. J. Eng. Res. Technol, 9, 639-650.

[11] Urooj, S., Lata, S., Ahmad, S., Mehfuz, S., & Kalathil, S. (2023). Cryptographic data security for reliable wireless sensor network. Alexandria Engineering Journal, 72, 37-50.
https://doi.org/10.1016/j.aej.2023.03.061

[12] Yi, L., Tong, X., Wang, Z., Zhang, M., Zhu, H., & Liu, J. (2019). A novel block encryption algorithm based on chaotic S-box for wireless sensor network. IEEE Access, 7, 53079-53090.
https://doi.org/10.1109/access.2019.2911395

[13] Thakkar, A., & Kotecha, K. (2014). Cluster head election for energy and delay constraint applications of wireless sensor network. IEEE sensors Journal, 14(8), 2658-2664.
https://doi.org/10.1109/jsen.2014.2312549

[14] Khashan, O. A., Ahmad, R., & Khafajah, N. M. (2021). An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks. Ad Hoc Networks, 115, 102448. https://doi.org/10.1016/j.adhoc.2021.102448

[15] Mathur, S., Gupta, D., Goar, V., & Kuri, M. (2017, February). Analysis and design of enhanced RSA algorithm to improve the security. In 2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT) (pp. 1-5). IEEE.
https://doi.org/10.1109/ciact.2017.7977330

[16] Therar, H. M., & Ali, A. J. (2023). Personal Authentication System Based Iris Recognition with Digital Signature Technology. Journal of Soft Computing and Data Mining, 4(1), 13-29.
https://publisher.uthm.edu.my/ojs/index.php/jscdm/article/view/10588