TELKOMNIKA Telecommunication Computing Electronics and Control
Vol. 23, No. 4, August 2025, pp. 1084~1096
ISSN: 1693-6930, DOI: 10.12928/TELKOMNIKA.v23i4.26241

Energy-efficient certificateless signcryption for secure data transfer in wireless sensor networks

Paruvathavardhini Jaganathan, Sargunam Balusamy
Department of ECE, School of Engineering, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, India

Article Info

Article history:

Received Apr 29, 2024
Revised Mar 21, 2025
Accepted May 10, 2025

Keywords:

Censored regression
Cryptography
Jaccard index certificateless signcryption
Secure and energy-efficient data transmission
Wireless sensor networks

ABSTRACT

Wireless sensor networks (WSN) have gained high popularity in the realm of technological innovation and have a prime responsibility of transferring the data safely to the sink despite the vulnerable situation presiding around the network. There needs to be a compromise made between energy consumption and the intricate network security system because they are inversely correlated. To create a safe and effective data transfer between the communicating nodes, a new censored regressive jaccard indexed certificateless signcryption (CEJICS) technique is suggested. Initially, the Gaussian likelihood censored regression is applied to identify the energy-efficient node which supports enhancing the network lifetime. The security is implemented using the rabin cryptographic jaccard indexive certificateless signcryption (RCJICS). To create a signcryption system with the characteristics of digital signature and ciphertext authenticity, the proposed work focuses on certificateless cryptography. The NS-2 simulator is used for the simulation, and performance metrics are used to evaluate it. According to the observed quantitative results, the suggested CEJICS method outperforms the other conventional methods by improving the packet delivery ratio (PDR) by 93%, achieving a minimum drop of 7%, reducing delay by 22%, reducing overhead to 17%, minimizing energy consumption by 15%, and ultimately extending the network lifetime by 10%.

Corresponding Author:

Paruvathavardhini Jaganathan
Department of ECE, School of Engineering
Avinashilingam Institute for Home Science and Higher Education for Women
Coimbatore, India
Email: vardhini.jpv@gmail.com

1. INTRODUCTION

Wireless sensor networks (WSN) form the epitome of modern technological progress and have, in the course of time, demonstrated key applications in environmental monitoring and tracking, precision agriculture, smart cities, and automation, among others [1]. These networks are characterized by highly dense deployment and self-configuration, realized within compact, low-cost sensor nodes that, in the course of computing, storage, and communication, are subject to severe energy constraints [2]. Despite all the applications, WSNs face massive energy efficiency, effective secure data transmission, and network longevity challenges. Basic to WSNs is reliable and efficient data transfer [3]. However, the limited energy supply for sensor nodes demands intelligent usage strategies that give the highest network lifetime with guaranteed security during communication [4]. Many techniques have been proposed so far to enhance transmission efficiency and extend the network lifetime by optimizing various parameters in sensor processing and power consumption [5]. For

instance, the quantized index energy-aware clustering-depend combinatorial stochastic sampled bat optimization (QIEAC-CSSBO) technique has been introduced to improve energy efficiency and secure routing.

Wireless communication channels introduce a vulnerability with security in WSNs; thus, they use cryptographic methods like encryption and decryption, along with digital signatures composed of the generation of keys and algorithms for signing and verification, in order to build confidence and integrity and prevent any form of authentication [6]–[10]. Typically, traditional digital certificates based on public key infrastructures are most widely used due to their less complexity and fewer overheads introduced; however, this is least desirable in highly resource-constrained environments of WSNs [10]–[18]. Considering the shortcomings, this paper introduces a new censored regressive jaccard indexed certificateless signcryption (CEJICS) technique, which optimizes energy consumption and strengthens security in WSNs. Gaussian likelihood censored regression is used for energy-efficient node selection, whereas Rabin cryptographic Jaccard indexic certificateless signcryption (RCJICS) is applied for secure data transmission. Simulation results using NS-2 show that CEJICS significantly enhances packet delivery ratio, reduces delay, minimizes energy consumption, and extends lifetime in terms of comparisons. The proposed CEJICS technique, addressing both the security and sustainability of energy in WSNs, is a robust and scalable solution for next-generation wireless sensor applications.

Motivation

However, low processing power, limited memory, limited energy resources, and the use of unstable wireless communication channels are some of the difficulties that WSNs encounter. Therefore, it is necessary to efficiently organize the available energy to convey the data in a highly protected manner [19], [20]. In Oladipupo *et al*. [21], an optimized version of the elliptic curve cryptography algorithm (IECC) was created. However, it did not concentrate on multicore WSN systems' ideal power consumption. To provide secure transmission, a lightweight secure aggregation and transmission scheme (SATS) was presented in [22]. However, there was no improvement in the data delivery performance. In Hayouni and Hamdi [23], a brand-new ultra-lightweight encryption method called ultra-lightweight encryption algorithm (ULEA) was created. A certificateless aggregate signature scheme (CL-ASS) was introduced in [24] to minimize bandwidth. Hence, we see that there are many research works regarding the implementation of security, but none have concentrated on efficient power consumption planning. A better technique has to be proposed so that the data is transmitted with great integrity and authenticity using RCJICS, and at the same time, the energy can be planned by picking the more energetic nodes and censoring the nodes with less energy using regression analyses.

The security services in WSNs are usually centered on cryptography [25]. An automated, lightweight cryptographic method, FlexCrypt, was designed in [26]. However, it failed to examine the feasibility of adapting FlexCrypt. A lightweight security transmission model was introduced in [27] to guarantee confidential data. To reduce the cost, a paillier cryptosystem and compressive sensing-based routing (PC2SR) protocol [28] was created. To ensure security, the secure encryption random permutation pseudo algorithm was created in [29]. In Cao *et al*. [30], an enhanced identity-based encryption algorithm (IIBE) was created. However, the security of various attacks was not examined.

An encryption and trust evaluation model was developed in [31]. But the delay was not minimized. In Meshram *et al*. [32], an identity-dependent offline/online signature approach (IBOOST) that is lightweight and provably secure for a large number of devices was created. For WSN, a well-structured routing technique based on trust estimation [33] was created. However, ETERS had a higher latency. To prevent DoS attacks, the biometric-based authenticated geographic opportunistic routing (BAGOR) method [34] is used. A pairing-free, certificateless, secure certification approach is suggested to avoid unnecessary resource usage [34]. There is no definition for the network lifespan extension. In Han *et al*. [35], an energy-conscious, trust-based routing protocol was created. The algorithm known as crossover mutated marriage in honey bee (CM-MH) was first presented in [36]. However, the cryptographic algorithm was not implemented.

A hybrid session key management method was introduced in [37]. However, the method concentrates on a particular attack. A lightweight authentication scheme [38], a one-way associated key management model [39], and a multidimensional secure clustered routing approach [40] were introduced for secure data transmission. But overhead remained unaddressed. An elliptic curve digital signature (ECDSA) cryptographic method was introduced in [41] to provide an appropriate mechanism. A mechanism for key agreement and secure anonymous authentication was introduced in [42] for WSNs. A new pairing-free signing encryption method is proposed [43]. Energy harvesting shall be included in power management [44]. Some of the research gaps identified from the existing approaches are as follows: (i) the developed method focuses on only specific attacks, a better model can be proposed to defend the attacks; (ii) reduced convergence time and minimization of data loss, delay, and overheads are required; (iii) better energy planning can be done to enhance the network lifetime; and (iv) a standard cryptographic algorithm can be developed to discover a secured route and enhance security in transmission.

Contribution, the main aspects of the suggested CEJICS is as follows: (i) energy-efficient node selection: introduces the concept of Gaussian likelihood censored regression to find high-energy efficient nodes in order to optimize network lifetime with minimal packet drop and delay; (ii) secure data transmission: RCJICS, a technique to provide both confidentiality, authentication, and integrity, without relying on third-party certificate authorities; (iii) integrated certificateless cryptography: achieves both signcryption and unsigncryption, inheriting both encryption and digital signature properties, with enhanced security and reduced overheads of computation; and (iv) scalability and future extensions: a flexible cryptographic framework is proposed that allows more advanced security attributes and energy harvesting mechanisms in order to further optimize WSN sustainability and resilience. The structure of the manuscript is as detailed: the recommended approach is enlightened in section 2. Section 3 describes the findings and debates, while section 4 provides the conclusion.

2. METHOD

In this paper, design and implement an advanced certificateless signcryption with the CEJICS technique that not only provides an improved channel for secure data transmission but also reduces energy consumption in WSN. It uses GLCR for determining residual energy and identifying energy-efficient nodes to maximize the network lifetime and RCJICS for employing simultaneous encryption and digital signature without resulting in complex certificate management. It opposes extra access to disallowed entities while achieving modest computational overhead and power use. Thus, CEJICS's way of doing key generation, signcryption, and un-signcryption effectively for the delivery of data securely and in less time consumes less delay and overhead and is scalable in utility, making it highly applicable in resource-scarce WSNs.

2.1. System model

In this section, a novel CEJICS technique is proposed to fill out the research gaps discussed. The technique involves two processes: (i) Gaussian likelihood censored regression-based energy-efficient node selection and (ii) RCJICS-based secure data transmission. The first process discusses in detail the selection of higher energy nodes and dodging the low energy nodes. The second process involves three steps: (a) key generation—each energy-efficient sensor node's time-synchronized session private and public keys are generated during the deterministic congruential key generation procedure; (b) signcryption: to alter the input data to ciphertext, the source node encrypts it utilizing the reciever's public key. The process uses the private key of the source to generate a digital signature; and (c) unsigncryption: after confirming the signature, the ciphertext is decrypted using unsigncryption.

The architecture of the suggested CEJICS technique for secure data flow between the source and sink nodes in WSN is displayed in Figure 1. The designed architecture contains numerous sensor nodes '$SN_1, SN_2, SN_3, \ldots SN_n$' and one sink node '$S$' in WSN. The source node broadcasts the data packets '$Dp_1, Dp_2, .., Dp_m$' to sink through the neighboring sensor nodes $NN_1, NN_2, NN_3, \ldots NN_B$ in a secure manner. By applying the proposed CEJICS technique, energy-efficient sensor nodes are initially identified using Gaussian likelihood censored regression. It is an ML technique that assesses the relationship between the power of the sensor hubs. Once the energy-efficient sensor nodes have been identified, RCJICS is used to transmit data securely. A novel type of public key cryptography called certificateless signcryption logically completes both public key One-step digital signature and encryption. The primary benefit of the suggested cryptographic method is that it is substantially less expensive than the conventional signature algorithm and encryption algorithm used individually. The many steps in the recommended CEJICS approach are briefly explained in the sequent section.

2.2. Gaussian likelihood censored regression-based energy-efficient node selection

The likelihood of the Gaussian one ML method for determining the relationship among the independent (or output) and dependent (or input) variables is censored regression. A class of models known as censored regression involves censoring the dependent variable, or sensor nodes, above or below a predetermined threshold. Let's assume that there are different quantities in the network. To suppress the WSN's entire energy usage, a limited quantity of sensor nodes are chosen as energy-efficient nodes in the first phase.

The primary resource used by the sensor nodes to enhance transmission is energy. In WSN, energy is crucial for carrying out important functions; when node energy decreases, the network connection shortens the network lifetime. Each node's energy levels are initially comparable. A specific value of its energy level is reduced as a consequence of the data receiving, transmission, and internal processes including processing, linking, and updating. Consequently, (1) provides an estimate of the sensor node's energy consumption level.

$$e_i(SN)^{Cons} = [e_i{}^{Sen} + e_i{}^{Rec} + e_i{}^{com}] \quad (1)$$

where, $e_i(SN)^{Cons}$ indicates a consumed energy level of 'i^{th}' sensor node, $e_i{}^{Sen}$ indicates energy for data sending, $e_i{}^{Rec}$ specifies energy for data receiving, $e_i{}^{com}$ denotes energy for computing.

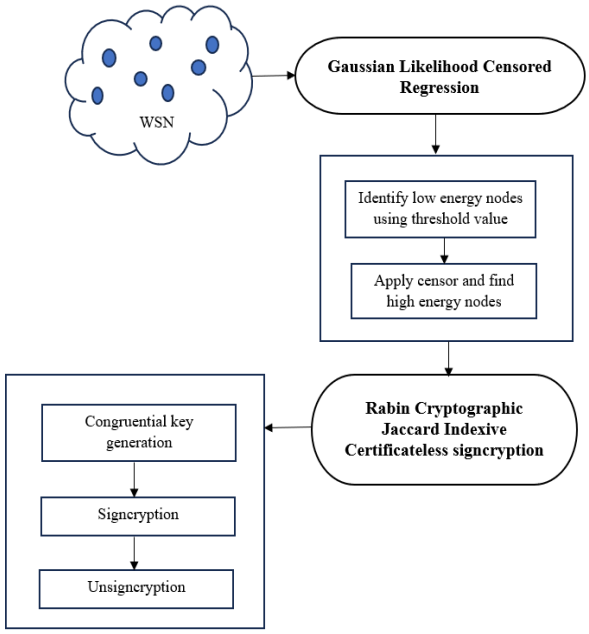

Figure 1. Flow diagram of proposed CEJICS technique

As a result, using (2), the node, s remaining energy is calculated as the alteration between the original and energy (consumed).

$$e_i(SN)^{res} = [e_i{}^{Int} - e_i{}^{Cons}] \tag{2}$$

where, $e_i(SN)^{res}$ indicates a residual energy level of i^{th} sensor nodes, $e_i{}^{Int}$denotes an initial energy of nodes, $e_i{}^{Cons}$ denotes the energy usage of sensor nodes.

Following sensor node energy level calculations, censored regression is used to recognize nodes that use less energy based on the statistical analysis of the Gaussian maximum likelihood to ascertain whether the threshold energy and residual energy levels are similar. As shown in (3) provides an estimate of the Gaussian maximum likelihood-test statistical analysis.

$$\omega_t = \frac{1}{\sqrt{2\pi v}}\left(\exp^{(-0.5*|e_i(SN)^{res}-T|2)}\right) \tag{3}$$

where, ω_t is the Gaussian maximum likelihood-test, $e_i(SN)^{res}$ denotes residual energy, T indicates threshold, v denotes variation. Then the sensors with maximum deviation are censored as given in (4),

$$Y = \begin{cases} if\ \omega_t = 1; & Select\ sensor\ nodes \\ otherwise & censored\ sensor\ nodes \end{cases} \tag{4}$$

Here Y denotes a censored regression, where, '1' denotes a sensor node with higher residual energy, else the sensor nodes are censored. In WSN, the chosen higher-energy nodes for sensors are utilized for safe data transfer.

To define the Gaussian likelihood censored regression procedure, an algorithm is created. The remaining energy-efficient sensor nodes are measured for every sensor node involved in the communication process. The Gaussian likelihood between residual energy and threshold is then calculated. Higher energy sensor nodes are found using likelihood estimation, while lower energy sensor nodes are found using the regression function. Lastly, the remaining sensor nodes are restricted and the higher-energy nodes for sensors are chosen for secure data transmission.

2.3. RCJICS based secure data transmission

Following the selection of energy-efficient sensor nodes, RCJICS is used to transmit data securely. Public key cryptography that logically completes both public key encryption and digital signature tasks in a single step is known as certificateless signcryption. The primary benefit of the suggested method is that it is substantially less expensive than the conventional signature algorithm and encryption algorithm used individually.

Sensitive data packets are protected during data transfer among the source and sink nodes in the cloud by using the suggested signcryption. Public-key cryptography is utilized in certificateless signcryption to ensure increased security [24]. Deterministic congruential key creation, signcryption, and unsigncryption are the three main processes in the certificateless signcryption process.

2.3.1. Deterministic congruential key generation

For each energy-efficient sensor node, the private and public key pairs is generated using the Rabin cryptosystem (RC). RC is a type of public-key encryption that works with two distinct items: a private key for unsigncryption and a time-synchronized session public key for signing. Hence the name of cryptography is called asymmetric key cryptography. For each session, the different key pairs are generated to avoid the attacks. Once the session is completed, the generated keys are automatically disabled.

The RC uses the Deterministic congruential random number generator to generate two large different prime numbers as in (5) and (6).

$$p = (b\ x_0 + e)\ mod\ n \tag{5}$$

$$q = (b\ x_1 + e)\ mod\ n \tag{6}$$

Where, n denotes a modulus, b denotes a multiplier, e denotes an increment, x_0, x_1 denotes a starting value.

Let us consider the two large various prime numbers p and q. The user's private and public keys are produced using (7).

$$K = p * q \tag{7}$$

where, K denotes a deterministic congruential public key and (p, q) denotes a deterministic congruential user of private key. While the private key is retained confidential and only known by the relevant sensor node, the public key is shared. The key generation process is said to be carried out in this manner.

2.3.2. Signcryption

The signcryption procedure is considered to be completed for the secure conveyance of data between the source nodes and sink nodes by using an RC after the sensor node's private and public key pair has been created. In the signcryption procedure, encryption and digital signatures are carried out concurrently. To confirm the integrity and confidentiality of data transfer, these two procedures are referred to as fundamental cryptographic procedures. Signcryption has the benefit of cutting down on computation time [44].

A block structure of the signcryption procedure to enhance data transfer between the supply and destined nodes is shown in Figure 2. Using the recipient public key, encryption is first operated to transform the entered data into the ciphertext. The sender performs both the encryption and the digital signature.

Let's look at the packets of data. $Dp_1, Dp_2, Dp_3, \ldots . Dp_n$. Next, the encryption procedure is carried out according to (8).

$$\delta = (Dp_i)^2\ mod\ K \tag{8}$$

where, 'δ' denotes a ciphertext of the data packet. Dp and K denote the receiver's deterministic congruential public key. Using the suggested method, the sender's deterministic congruential private key is utilized to create a digital signature for that specific data packet. To verify the contents of a sent ciphertext and the sender's individuality, a digital code called a digital signature is appended.

This digital signature is produced by the sender node as a hash value. Any function that converts a random-sized data packet into a fixed-length one is referred as hash value. Each data packet's hash is generated during transmission using the Snefru hash algorithm.

Each input data packet of arbitrary length is hashed into 128-bit values using the Snefru cryptographic hash. The padding technique used by the Snefru cryptographic hash combines the length of the input data packets with an additional padding block. As seen in Figure 3, the input data packets are first separated into several message blocks.

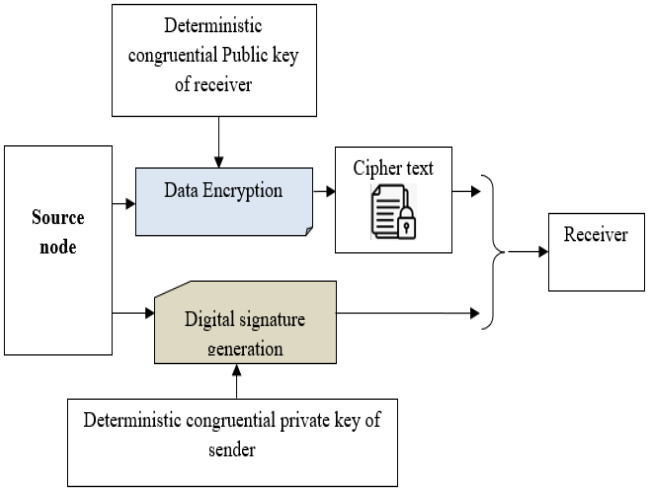

Figure 2. Block diagram of the signcryption process

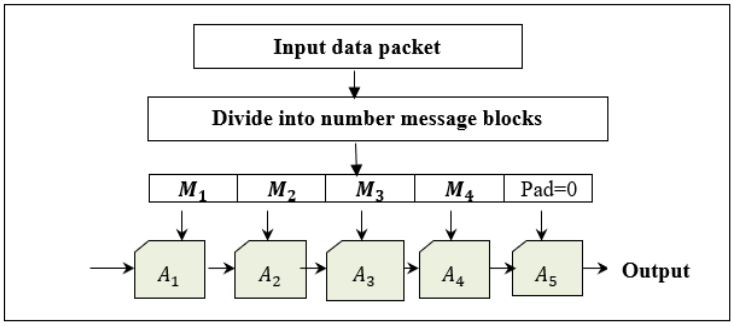

Figure 3. Block diagram of Snefru cryptographic hash generation

Figure 3 depicts the flow process of the Snefru cryptographic hash function to generate the output hash. Initially, the number of message blocks 'M_1, M_2, M_3, M_4' is initialized to hash function. After that, the Miyaguchi–Preneel compression function 'A_1, A_2, A_3, A_4' is applied to the last block padded with '0's (i.e., Pad=0). The Miyaguchi–Preneel compression function is used by the Snefru cryptography algorithm to determine the final hash value. Applying the compression algorithm results in a hash output that is XORed with both the preceding hash value and the message block. The subsequent hash value is generated by this hash value. In the event that no previous hash value exists, a pre-specified beginning value is utilized in the first round ($h_0 = 0$). The compression's output is produced using (9).

$$h = [W_{p_{h_{i-1}}}(M_i) \oplus h_{i-1} \oplus M_i] \quad (9)$$

Where, message block 'M_i' and the last hash value (h_{i-1})is initially preset to '0'. 'W' denotes a block cipher, p indicates a key to a block cipher 'W' XORed with the previous hash value 'h_{i-1}' and the message block (M_i). The final hash'h' and the recipient sensor node receive the encrypted text.

2.3.3. Unsigncryption

To guarantee the transfer of data packets security in WSN, the suggested method completes the unsigncryption process, which is made up of two main steps: decryption and signature verification at the receiving end. After confirming the signature, the recipient decrypts the original data to obtain the ciphertext from the source node.

The unsigncryption procedure to recover the original data packet at the recipient node is shown in Figure 4. The process of verifying signatures is considered to be completed first. The hash value h_{new} is generated at the receiving end using the same Snefru cryptographic hash function.

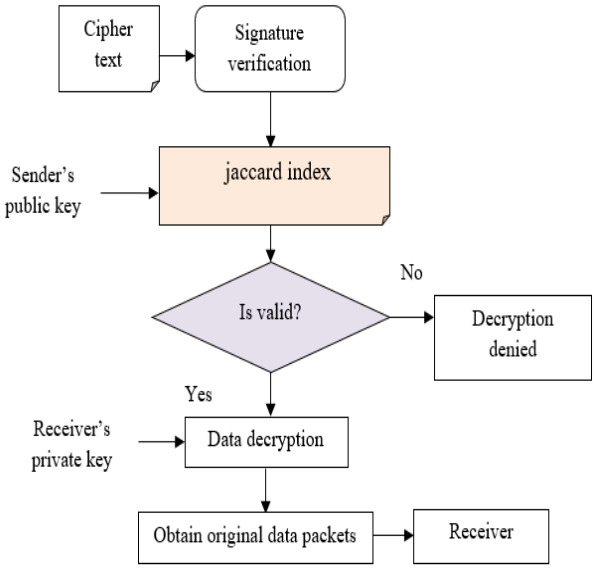

Figure 4. Flow process of unsigncryption

Lastly, uses the Jaccard index to confirm that the created signature h_{new} matched a signature generated at the sender$h$. The hash value is matched using the Jaccard Index similarity function. The mathematical expression for the similarity is found in (10).

$$\vartheta = \frac{h \cap h_{new}}{\sum h + \sum h_{new} - h \cap h_{new}} \tag{10}$$

where, ϑ indicates a Jaccard similarity coefficient, h denotes the hash value generated at the sender, h_{new} indicates a reciepient side produced hash value, the intersection symbol '∩' designates mutual independence between the hash which are statistically dependent, $\sum h$ is the sum of h score, $\sum h_{new}$ is the sum of h_{new} score. The Jaccard similarity coefficient provides the output values from 0 to 1 as given (11),

$$\vartheta = \begin{cases} 1 \; ; & Signature\ matched \\ 0 \; ; & Signature\ not\ matched \end{cases} \tag{11}$$

The recipient decrypts the original data if the signature matches. If not, the nodes are considered unauthorized, which includes flooding, grayhole, and blackhole assaults. Lastly, the decryption process is carried out by the approved sensor nodes using (12).

$$Dp = \left(c.p.x_p + d.q.x_q \right) mod\ K \tag{12}$$

where, $x_p = \delta^{\frac{1}{4}(p+1)}\ mod\ p$,

$$x_q = \delta^{\frac{1}{4}(q+1)}\ mod\ q\ ,\ c.p + d.q = 1$$

Where, Dp denotes the original data packet, δ denotes a cipher text, p, q are private keys, K indicates a public key, and c, d are variables. This is how data packet transmission security is carried out. For RCJICS, an algorithmic method for safe data transfer is created. Key creation, signcryption, and unsigncryption are its three distinct steps. First creates a pair of keys for each network node that uses energy-efficient sensors. The input data packets are then encrypted by the sender node, and the signature is produced as a hash value using the Snefru cryptographic hash function. To guarantee security, the encrypted data is transmitted to the recipient, where the unsigncryption procedure is completed. The Jaccard index is used at the recipient end to verify signatures. The recipient node decrypts the data packet if the signature is legitimate. Lastly, the approved sensor node uses its private key to decode the original data. Data packet transmission and security are enhanced as a result.

3. RESULTS AND DISCUSSION

3.1. Simulation settings

Using the NS2.34 simulator with WSN-DS, the modeling of the suggested CEJICS is contrasted with current techniques [21], [22]. The intrusion detection dataset was obtained from https://www.kaggle.com/datasets/bassamkasasbeh1/wsnds. Table 1 lists the simulation factors that were employed. In simulation system, the random waypoint is used as mobility model to perform secure data transmission. The DSR routing protocol is applied in experimental for attack detection in WSN.

Table 1. Simulation parameters

Simulation parameter	Value
Simulator	NS2.34
Data packets	100-1000
Mobility model	Random way point
Number of runs	10
Network area	1100×1100 m
Sensor nodes speed	0-20 m/s
Routing protocol	DSR
Number of sensor nodes	50-500
Simulation time	300 s

3.2. Simulation results

Several performance indicators are examined in this part together with the simulation study of CEJICS and the current IECC [21], SATS [22]. A table and graphical representation are used for analysis. The performance indicators like energy consumption, packet delivery ratio, packet drop rate, throughput, end-to-end delay, and communication overhead are analysed. A table and graphical representation are used to represent the analysis.

3.2.1. Impact of energy consumption

It is quantified as the energy usage of the sensor hubs to detect the data. It is mathematically calculated as given (13).

$$Cons_E = n * Cons_E(Sn) \tag{13}$$

In (13), $Cons_E$ is the energy consumption, n represents sensor nodes, $'Cons_E(Sn)'$ is the energy amount utilized by individual node (Sn). It is computed in joule (J).

Analysis of energy use is shown in Table 2. In comparison to [21], [22], the energy consumption statistics are reduced by 11% and 18%, respectively. This is because of applying a Gaussian likelihood censored regression to find the energy-efficient sensor nodes by censoring low-energy nodes. This process minimizes energy consumption.

Table 2. Energy consumption comparison

Number of sensor nodes	Energy consumption (J)			
	CEJICS	IECC	SATS	CEJICS
50	11.5	14	16	50
100	13	16	17	100
150	16.5	18	20.25	150
200	18	20.4	22	200
250	20	22.5	25	250
300	22.5	24	27	300
350	24.15	26.25	28	350
400	26	28	30	400
450	28.35	30.6	31.5	450
500	29	32	35	500

3.2.2. Impact of PDR

It is calculated by dividing the entire number of data packets sent from the starting node by the number of data packets received at the base station or sink node. It is stated as (14).

$$Ratio_{PD} = \left(\frac{[dp_{received}]}{[dp_{sent}]}\right) * 100 \tag{14}$$

From (14), $Ratio_{PD}$ indicates a PDR, $dp_{received}$ denotes received data packets quantity, dp_{sent} indicates the number of data packets sent. It is expressed as a percentage (%).

Figure 5 shows the PDR result. Compared to current approaches, the CEJICS technology results in a 3% and 6% increase in the PDR. This improvement is achieved by CEJICS to pick energy-efficient nodes. Moreover, CJICS is to avoid unauthorized attacks to improve the packet delivery rate. CEJICS achieves the highest PDR for any of the data packets it considers, and consistently beats IECC [21] and SATS [22]. IECC does decently well but is still behind CEJICS, while SATS registers the least PDR, proving to be a less reliable one. The results confirm that CEJICS allows for the delivery of higher amounts of data and more reliable network operation, hence the best.

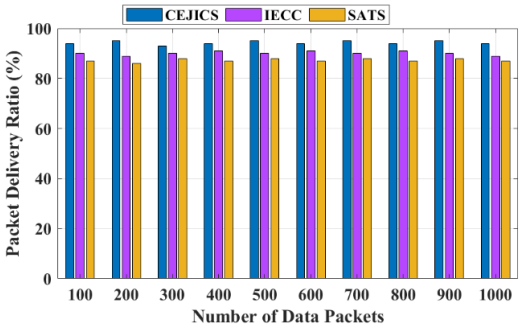

Figure 5. Performance analysis of PDR

3.2.3. Impact of end-to-end delay

It is quantified as the discrepancy between the observed and expected arrival times of sink node information sets. It is calculated using (15).

$$D_{EE} = T\ (dp)_{ex} - T\ (dp)_{obs} \quad (15)$$

where, D_{EE} be the end-to-end delay, $T\ (dp)_{ex}$ denotes an anticipated time of arrival for the data packet, the data packet's observed arrival time at the destination is shown by $T\ (dp)_{obs}$. Milliseconds (ms) were used for measurement.

In Figure 6, the end-to-end delay is analyzed. As a result, end-to-end delay is reduced by 17% and 27%, respectively, compared to IECC [21] and SATS [22]. With reduced source-to-destination delay, the suggested CEJICS technique uses regression analysis to choose more energy-efficient sensor nodes. CEJICS attains the minimal end-to-end latency across varying sensor node counts, demonstrating its efficiency in reducing transmission latency compared to IECC and SATS.

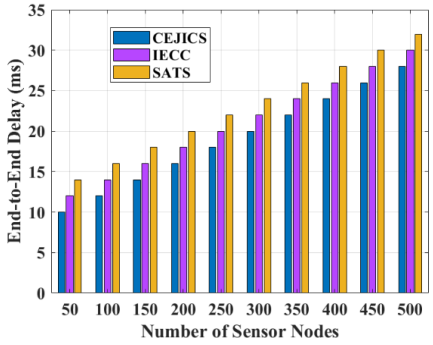

Figure 6. Performance analysis of end-to-end delay comparisons

3.2.4. Network lifetime

The period between deployment and the location where the network is no longer operational is referred to as the network lifetime as given in (16).

$$N_L = m * [time_{dep} - time_{nbn}] \quad (16)$$

where 'N_L' denotes a network lifetime, 'm' is the sensor hubs numbers, '$time_{dep}$' is the time of deployment and '$time_{nbn}$' represents the time when the network is non-functional. It is computed in milliseconds (ms).

The network lifetime improvement is depicted in Figure 7. In comparison to IECC [21] and SATS [22], the CEJICS approach improves the network lifetime by 19% and 29%, respectively. CEJICS significantly extends network lifetime compared to IECC [21] and SATS [22], ensuring better energy efficiency and prolonged operation in WSNs.

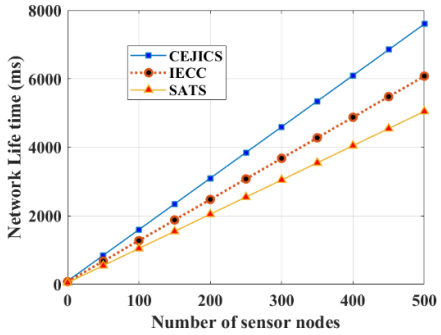

Figure 7. Network lifetime of three techniques

3.3. Discussion

The process is critically important to preserve the validity of the findings accumulated and to prevent distortions of knowledge in the scientific field. Quality and accuracy of results are the foundation of good research; nonetheless, identification of obvious fraud or misconduct poses a formidable task. Investigators may bias data or methodologies, and this makes it necessary to put measures that champion research integrity in place. Peer review is a basic element of quality control since it lets key researchers scrutinize strategies, calculations, and outcomes. Again, independent replication confirms the outcome, or offers a degree of check, on these studies. Ensuring open access to data and expressing methodologies also helps in finding discrepancies and builds credibility in the findings. Widespread implementation of measures ensuring responsibility and skepticism helps to minimize threats from fraud-related activities. Thus, by combining these approaches, the research community will be capable of increasing the reliability and effectiveness of its findings, protecting science and society from inaccurate results. It will be necessary for future work to adhere to these principles to expand the research and maintain its credibility.

4. CONCLUSION

This paper proposed a new CEJICS technique to increase WSNs' sustainability and secure data transfer. The approach integrates Gaussian likelihood censored regression for selecting high-energy-efficient nodes with minimal packet drop and delay, and RCJICS for ensuring secure communication through deterministic congruential key generation, signcryption, and unsigncryption. Simulation results show that CEJICS can greatly outperform the other methods namely, IECC and SATS with an average packet delivery ratio of 93%, minimum of 7% PDR, 22% delay, 17% overhead, 15% saving in energy consumption, and 10% enhancement of network lifetime. These values and comparisons prove that CEJICS is effective in optimizing security and energy efficiency in WSNs. Future work can be the addition of more security attributes to protect data additionally. Additionally, integration of energy harvesting in the current architecture would improve the power management capabilities and extend the lifespan of the network, making WSNs quite sustainable and resilient in real-world applications.

ACKNOWLEDGMENTS

The author would also like to express sincere thanks to Dr. R. Sudarmani for contributing her knowledge to this study.

FUNDING INFORMATION

No funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Paruvathavardhini Jaganathan	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	
Sargunam Balusamy		✓				✓		✓	✓	✓	✓	✓		

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

WSN uses a dataset from https://www.kaggle.com/datasets/bassamkasasbeh1/wsnds for intrusion detection systems. In this study, no additional datasets were employed. The article includes relevant citations for the works that were used as references. Author [J. Paruvathavardhini] completed the entire job and carried it out under the supervision of Dr. B. Sargunam.

REFERENCES

[1] A. Sumithra, "Quadratic poly certificateless inductive signcryption for network security," *Mobile Networks and Applications*, vol. 26, no. 4, pp. 1586–1596, Aug. 2021, doi: 10.1007/s11036-019-01496-0.

[2] Z. Wang, W. Zeng, S. Yang, D. He, and S. Chan, "UCRTD: An unequally clustered routing protocol based on multihop threshold distance for wireless sensor networks," *IEEE Internet of Things Journal*, vol. 11, no. 17, pp. 29001–29019, Sep. 2024, doi: 10.1109/JIOT.2024.3406343.

[3] M. Majid *et al.*, "Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review," *Sensors*, vol. 22, no. 6, Mar. 2022, doi: 10.3390/s22062087.

[4] M. E. S. Saeed, Q.-Y. Liu, G. Tian, B. Gao, and F. Li, "Remote authentication schemes for wireless body area networks based on the Internet of Things," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4926–4944, Dec. 2018, doi: 10.1109/JIOT.2018.2876133.

[5] X. Liu and W. Ma, "CDAKA: A provably-secure heterogeneous cross-domain authenticated key agreement protocol with symptoms-matching in TMIS," *Journal of Medical Systems*, vol. 42, no. 8, Aug. 2018, doi: 10.1007/s10916-018-0985-7.

[6] B. Kavya, V. Vani, and H. Roopa, "Efficient cluster head rotation based on residual energy to extend network lifetime," in *2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA)*, Jul. 2020, pp. 774–777. doi: 10.1109/ICIRCA48905.2020.9182843.

[7] C. Wang, X. Liu, H. Hu, Y. Han, and M. Yao, "Energy-efficient and load-balanced clustering routing protocol for wireless sensor networks using a chaotic genetic algorithm," *IEEE Access*, vol. 8, pp. 158082–158096, 2020, doi: 10.1109/ACCESS.2020.3020158.

[8] N. Us Sama, K. Bt Zen, A. Ur Rahman, B. BiBi, A. Ur Rahman, and I. A. Chesti, "Energy efficient least edge computation LEACH in wireless sensor network," in *2020 2nd International Conference on Computer and Information Sciences (ICCIS)*, Oct. 2020, pp. 1–6. doi: 10.1109/ICCIS49240.2020.9257649.

[9] N. Ma, H. Zhang, H. Hu, and Y. Qin, "ESCVAD: An energy-saving routing protocol based on voronoi adaptive clustering for wireless sensor networks," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 9071–9085, Jun. 2022, doi: 10.1109/JIOT.2021.3120744.

[10] V. G. Krishnan, P. V. Rao, and V. Divya, "An energy efficient routing protocol based on SMO optimization in WSN," in *2021 6th International Conference on Communication and Electronics Systems (ICCES)*, Jul. 2021, pp. 1040–1047. doi: 10.1109/ICCES51350.2021.9489163.

[11] Y. Zaied, W. Saad, and M. Shokair, "Energy efficient of grid clustering based TEEN protocol for cognitive radio wireless sensor networks," in *2021 International Conference on Electronic Engineering (ICEEM)*, Jul. 2021, pp. 1–6. doi: 10.1109/ICEEM52022.2021.9480632.

[12] A. F. E. Abadi, S. A. Asghari, M. B. Marvasti, G. Abaei, M. Nabavi, and Y. Savaria, "RLBEEP: Reinforcement-learning-based energy efficient control and routing protocol for wireless sensor networks," *IEEE Access*, vol. 10, pp. 44123–44135, 2022, doi: 10.1109/ACCESS.2022.3167058.

[13] Shalika, U. Meena, and A. Agarwal, "An analysis of energy efficient clustering based techniques in WSN," in *2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS)*, May 2022, pp. 715–721. doi: 10.1109/ICICCS53718.2022.9788421.

[14] S. L. Rex B R, S. T. Tumma, J. Chandra, L. Giffina, and S. R. Devi, "Particle swarm optimization method for energy efficient secondary grid cluster head selection to avoid energy holes in WSN," in *2021 Asian Conference on Innovation in Technology (ASIANCON)*, Aug. 2021, pp. 1–7. doi: 10.1109/ASIANCON51346.2021.9544990.
[15] J. Paruvathavardhini and B. Sargunam, "Stochastic bat optimization model for secured WSN with energy-aware quantized indexive clustering," *Journal of Sensors*, vol. 2023, no. 1, Jan. 2023, doi: 10.1155/2023/4237198.
[16] J. Paruvathavardhini, B. Sargunam, and R. Sudarmani, "A review on energy efficient routing protocols and security techniques for wireless sensor networks," *Applied Mechanics and Materials*, vol. 912, pp. 55–75, Feb. 2023, doi: 10.4028/p-5s9p7j.
[17] M. Hussain, A. Mehmood, S. Khan, M. A. Khan, and Z. Iqbal, "Authentication techniques and methodologies used in wireless body area networks," *Journal of Systems Architecture*, vol. 101, Dec. 2019, doi: 10.1016/j.sysarc.2019.101655.
[18] R. Prodanović *et al.*, "Trustworthy wireless sensor networks for monitoring humidity and moisture environments," *Sensors*, vol. 21, no. 11, May 2021, doi: 10.3390/s21113636.
[19] F. Saleem *et al*., "Ant lion optimizer based clustering algorithm for wireless body area networks in livestock industry," *IEEE Access*, vol. 9, pp. 114495–114513, 2021, doi: 10.1109/ACCESS.2021.3104643.
[20] R. Kaur and J. Kaur Sandhu, "A study on security attacks in wireless sensor network," in *2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, Mar. 2021, pp. 850–855. doi: 10.1109/ICACITE51222.2021.9404619.
[21] E. T. Oladipupo *et al.*, "An efficient authenticated elliptic curve cryptography scheme for multicore wireless sensor networks," *IEEE Access*, vol. 11, pp. 1306–1323, 2023, doi: 10.1109/ACCESS.2022.3233632.
[22] G. Said, A. Ghani, A. Ullah, M. Azeem, M. Bilal, and K. S. Kwak, "Light-weight secure aggregated data sharing in IoT-enabled wireless sensor networks," *IEEE Access*, vol. 10, pp. 33571–33585, 2022, doi: 10.1109/ACCESS.2022.3160231.
[23] H. Hayouni and M. Hamdi, "A novel energy-efficient encryption algorithm for secure data in WSNs," *The Journal of Supercomputing*, vol. 77, no. 5, pp. 4754–4777, May 2021, doi: 10.1007/s11227-020-03465-x.
[24] J. Kar, X. Liu, and F. Li, "CL-ASS: An efficient and low-cost certificateless aggregate signature scheme for wireless sensor networks," *Journal of Information Security and Applications*, vol. 61, Sep. 2021, doi: 10.1016/j.jisa.2021.102905.
[25] S. V. G, R. Nagarajan, and S. Kannadhasan, "Performance analysis of blended NIDS model for network intrusion detection system in WSN," in *2023 Fifth International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, Feb. 2023, pp. 1–6. doi: 10.1109/ICECCT56650.2023.10179781.
[26] O. A. Khashan, R. Ahmad, and N. M. Khafajah, "An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks," *Ad Hoc Networks*, vol. 115, Apr. 2021, doi: 10.1016/j.adhoc.2021.102448.
[27] L. Zhou, M. Kang, and W. Chen, "Lightweight security transmission in wireless sensor networks through information hiding and data flipping," *Sensors*, vol. 22, no. 3, Jan. 2022, doi: 10.3390/s22030823.
[28] S. Ifzarne, I. Hafidi, and N. Idrissi, "Compressive sensing and paillier cryptosystem based secure data collection in WSN," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 5, pp. 6243–6250, May 2023, doi: 10.1007/s12652-021-03449-6.
[29] S. Nagaraj *et al.*, "Improved secure encryption with energy optimization using random permutation pseudo algorithm based on internet of thing in wireless sensor networks," *Energies*, vol. 16, no. 1, Dec. 2022, doi: 10.3390/en16010008.
[30] C. Cao, Y. Tang, D. Huang, W. Gan, and C. Zhang, "IIBE: An improved identity-based encryption algorithm for WSN security," *Security and Communication Networks*, vol. 2021, pp. 1–8, Sep. 2021, doi: 10.1155/2021/8527068.
[31] S. Awan, N. Javaid, S. Ullah, A. U. Khan, A. M. Qamar, and J.-G. Choi, "Blockchain based secure routing and trust management in wireless sensor networks," *Sensors*, vol. 22, no. 2, Jan. 2022, doi: 10.3390/s22020411.
[32] C. Meshram, A. L. Imoize, A. Elhassouny, A. Aljaedi, A. R. Alharbi, and S. S. Jamal, "IBOOST: A lightweight provably secure identity-based online/offline signature technique based on FCM for massive devices in 5G wireless sensor networks," *IEEE Access*, vol. 9, pp. 131336–131347, 2021, doi: 10.1109/ACCESS.2021.3114287.
[33] T. Khan *et al.*, "ETERS: A comprehensive energy aware trust-based efficient routing scheme for adversarial WSNs," *Future Generation Computer Systems*, vol. 125, pp. 921–943, Dec. 2021, doi: 10.1016/j.future.2021.06.049.
[34] G. Wei and K. Wu, "Paring-free certificateless security authentication scheme for WSN based on ECC," in *2019 3rd International Conference on Electronic Information Technology and Computer Engineering (EITCE)*, Oct. 2019, pp. 1355–1360. doi: 10.1109/EITCE47263.2019.9094944.
[35] Y. Han, H. Hu, and Y. Guo, "Energy-aware and trust-based secure routing protocol for wireless sensor networks using adaptive genetic algorithm," *IEEE Access*, vol. 10, pp. 11538–11550, 2022, doi: 10.1109/ACCESS.2022.3144015.
[36] M. Alotaibi, "Improved blowfish algorithm-based secure routing technique in IoT-based WSN," *IEEE Access*, vol. 9, pp. 159187–159197, 2021, doi: 10.1109/ACCESS.2021.3130005.
[37] G. Mehmood *et al.*, "An efficient and secure session key management scheme in wireless sensor network," *Complexity*, vol. 2021, no. 1, Jan. 2021, doi: 10.1155/2021/6577492.
[38] L. Xiong, N. Xiong, C. Wang, X. Yu, and M. Shuai, "An efficient lightweight authentication scheme with adaptive resilience of asynchronization attacks for wireless sensor networks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 9, pp. 5626–5638, Sep. 2021, doi: 10.1109/TSMC.2019.2957175.
[39] S. Li *et al*., "A secure scheme based on one-way associated key management model in wireless sensor networks," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2920–2930, Feb. 2021, doi: 10.1109/JIOT.2020.3021740.
[40] W. Fang, W. Zhang, W. Chen, J. Liu, Y. Ni, and Y. Yang, "MSCR: multidimensional secure clustered routing scheme in hierarchical wireless sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2021, no. 1, Dec. 2021, doi: 10.1186/s13638-020-01884-1.
[41] R. Qazi, K. N. Qureshi, F. Bashir, N. U. Islam, S. Iqbal, and A. Arshad, "Security protocol using elliptic curve cryptography algorithm for wireless sensor networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 1, pp. 547–566, Jan. 2021, doi: 10.1007/s12652-020-02020-z.
[42] Y. Chen and J. Chen, "Anonymous and provably secure authentication protocol using self-certified cryptography for wireless sensor networks," *Multimedia Tools and Applications*, vol. 80, no. 10, pp. 15291–15313, Apr. 2021, doi: 10.1007/s11042-020-10259-z.
[43] P. N. Kasyoka, M. Kimwele, and S. A. Mbandu, "Efficient certificateless signcryption scheme for wireless sensor networks in ubiquitous healthcare systems," *Wireless Personal Communications*, vol. 118, no. 4, pp. 3349–3366, Jun. 2021, doi: 10.1007/s11277-021-08183-y.
[44] J. Paruvathavardhini and R. Sudarmani, "Adaptive smart power saving techniques for machine-to-machine communication-enabled wireless sensor networks," in *Adaptive Power Quality for Power Management Units using Smart Technologies*, Boca Raton: CRC Press, 2023, pp. 223–253. doi: 10.1201/9781003436461-9.

BIOGRAPHIES OF AUTHORS

Paruvathavardhini Jaganathan received the B.Eng. degree in ECE from the Avinashilingam University, Coimbatore, Tamilnadu, in 2009, and the Master's degree in Wireless Sensor Networks from Karpagam Univeristy, Coimbatore, Tamil Nadu in 2011 and pursuing Ph.D. in the field of Wireless sensor Networks, Avinashilingam University, Coimbatore, Tamilnadu. She is currently working as Assistant Professor (Sr.Gr) in the Department of ECE in Jai Shriram Engineering College, Tiruppur, Tamilnadu. Her Current research interests include Wireless sensor networks, Signal Processing and WBN (Healthcare). She can be contacted at email: paruvathavardhinijaganathan@gmail.com, vardhini.jpv@gmail.com.

Sargunam Balusamy received the B.E. degree in Electronics and Communication Engineering, M.E. degree, and Ph.D. from Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore. She is currently serving as Professor and Dean in the School of Engineering at Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore. Her current research interests include digital design, VLSI design, and image processing. She can be contacted at email: sargunamb@gmail.com.