International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2024/224445 Volume 11, Issue 2, March – April (2024)

RESEARCH ARTICLE

Laplacian Kernel Clustering-Based Improved Certificateless Signcryption for a Secure Marine Data Aggregation in Network of Wireless Sensors

K. E Hemapriya
Sri Krishna Arts and Science College, Coimbatore, Tamil Nadu, India.
kehemapriya@gmail.com

S. Saraswathi
Nehru Arts and Science College, Coimbatore, Tamil Nadu, India.
saraswathisubbian@gmail.com

Received: 24 December 2023 / Revised: 10 March 2024 / Accepted: 26 March 2024 / Published: 30 April 2024

Abstract – Wireless Sensor Networks (WSNs) are collected from several inexpensive sensor nodes with three key capabilities: sensing, computation, and communication. During communication, these sensor nodes consume a specific amount of energy. It's often organized in marine surroundings for data monitoring and collection, requiring the transmission of data gathered to a sink node or base station. The sink node is answerable for aggregating information as of deployed sensor nodes. Ensuring secure data aggregation in WSNs presents unique challenges due to the dynamic nature of the marine environments. Therefore, an efficient cryptographic mechanism is required to guarantee the integrity of data transmission among sensor nodes (Sn) in addition to sink nodes to enhance secure data aggregation, an innovative approach called the Laplacian Kernel Clustering-based Improved Certificateless Signcryption (LKC-ICS) method is developed. The primary intent of LKC-ICS is to improve the security of data aggregation with energy efficiency in WSNs.The LKC-ICS technique consists of two main processes: clustering and secure data aggregation. Initially, Sn are distributed throughout the marine surroundings to sense objects underwater. The Laplacian Kernelized BFR clustering algorithm is applied in LKC-ICS to group Sn depending on their residual energy echelon. Subsequently, cluster heads are selected for secure data transmission. Cluster members transmit collected information to their respective cluster heads (H_C). Then H_C data aggregates from sensor nodes and is securely transmitted in sink node. The LKC-ICS technique employs an improved certificateless signcryption method for secure data aggregation from H_C to a base station. The cryptographic technique involves the key generation, signcryption, and unsigncryption processes. During signcryption, the original data packet is transformed into encrypted data while generating a digital signature. Unsigncryption involves signature verification to authenticate the user. Upon successful verification, the receiver decrypts the data if the signature is valid. This process minimizes data aggregation delays and packet loss. Different parameters simulate the proposed LKC-ICS technique. Quantitative analysis demonstrates that the LKC-ICS technique's performance improved compared to conventional methods in secure data aggregation and delivery.

Index Terms – WSN, Security, Data Aggregation, Energy Efficiency, Laplacian Kernelized BFR Clustering, Improved Certificateless Signcryption.

1. INTRODUCTION

Wireless Sensor Network (WSN) comprises dedicated Sn with sensing and computing capabilities. These nodes are dependable for sensing and monitoring physical parameters, transmitting the gathered data wirelessly to the central base station. It deploys multiple sensors to enhance system reliability, particularly in monitoring marine environments. This environment includes Sn, sink nodes, BS.Sn are placed with underwater object sensing and monitoring, transmitting collected data wirelessly to sink nodes. In the communication between sensor nodes and sink nodes, security is crucial in protecting aggregated data from unauthorized alterations. Several researchers have been devoted to improving safe data aggregation methods at WSNs.

In communicating between sensor nodes and sink nodes, security plays a primary role in defending the data aggregated from unauthorized alterations. The aggregation data aids in saving energy and prolonging the network's era. It is a network processing method that combines data processes and deals with extra transmission. Encrypted data helps preserve privacy, but delay and energy consumption are not reduced. To overcome the issue, LKC-ICS is designed with higher security of aggregation data and minimum energy consumption in WSNs.

An optimized Elliptic Curve Cryptographic (ECC) technique called IECC was introduced in [1] to enhance secure communication against various attacks. The key exchange

RESEARCH ARTICLE

algorithm was performed by EC_Diffie_Helman (ECDH). The Elliptic Curve Digital Signature Algorithm (ECDSA) was performed using maintained WSN security. However, the developed technique failed to design an optimal energy consumption model to enhance network lifetime. A secure routing method was developed in [2] for secure data aggregation by preventing the intrusion of malicious nodes. An efficient authentication method was employed for communication among cluster heads. The designed method improves the packet delivery ratio with minimum delay. However, effective encryption methods were not integrated to ensure robust security with minimal overhead.

A novel secure data aggregation protocol was designed in [3] to enhance information security by detecting Denial of Service (DOS) attacks. The Blowfish EAX-RSA algorithm was utilized to improve confidentiality and integrity. However, achieving energy-efficient data aggregation was a significant challenge. An Improved Blowfish algorithm (IBFA) was developed in [4] for secured authentication. A method of CM-MH was determined to select the optimal path and achieve secure transmission. However, the cluster-based secure data transmission failed to reach the minimum delay.

An asymmetric Elliptic Curve Cryptography (ECC) technique was designed [5] to improve energy effectiveness and data security. The generated key was developed to perform encrypts and decrypting. However, delay performance was not reduced. SHSDA method was developed in [6]. Lightweight symmetric encryption was employed to ensure higher data security. However, the designed technique was inefficient in enhancing the packet delivery ratio. An authorization and verification model was introduced in [7] to perform secure data collection. A TLMS filter was determined to execute data aggregation. However, the latency in gathering data was not reduced.

TrustAssisted Global and Greedy Congestion-aware model was developed in [8] for data collection with lesser energy consumption and improved reliability. Energy usage of the sensors and communication overhead were minimized. However, it failed to incorporate cryptographic techniques to enhance the security of data aggregation. A one-way associated key management approach was presented in [9] to facilitate safe data broadcast. But, consideration of energy-aware data broadcast was not included in the secure data transmission. In [10], a four-stage security level (FS-SSL) was designed to secure data broadcasts. Throughput was enhanced. However, the performance of energy consumption was not minimized.

1.1. Problem Statement

Several types of research have been developed for aggregation and secure authentication. Data aggregation protocols are determined to be based on improved network era and minimum energy consumption. In clustering data, the data density flows via a smaller network, which enhances the network's lifespan. Residual energy, energy consumption, and efficiency are vital criteria in data clustering. However, security is still determined to be another severe factor. In addition, the optimal energy consumption model was not considered with the maximum network lifetime. Also, the overhead was not reduced by combining encryption methods. The proposed LKC-ICS technique is introduced to overcome the issue of secure data communication with lesser energy consumption and overhead.

An innovative contribution of the LKC-ICS technique is introduced as follows:

- A novel LKC-ICS technique is developed to enhance energy-effective secure data aggregation in WSN, which depends on clustering and certificateless signcryption.
- The LKC-ICS technique utilizes the Laplacian Kernelized BFR clustering algorithm to use the residual energy of both sensors, as well as minimum energy consumption and aggregation delay. Nodes with higher energy levels and cluster heads are chosen based on energy estimation using the Laplacian kernel function.
- An improved certificateless signcryption technique is employed in LKC-ICS for secure data aggregation. Rabin cryptography is integrated into the certificateless signcryption for encryption and signature generation. The Ratcliff-Obershelp pattern matching is utilized for signature verification. This process enhances secure data aggregation with minimal loss.
- Finally, a simulation is performed to calculate the performance of the LKC-ICS method and other associated approaches using various evaluation metrics.

The organization of this paper is structured as follows: discusses the literature survey in section 2. Section 3 gives a detailed elucidation of LKC-ICS method through a neat diagram. Section 4 explains simulation analysis and provides outcomes that validate the performance of the LKC-ICS method as well as conventional techniques. Finally, the conclusion is described in section 5.

2. LITERATURE SURVEY

In [11], a secure and verifiable continuous data collection (SVCDC) method was designed using sensory data. Extended Homomorphic Encryption was developed to extract a single piece of data. Verification of integrity and privacy were ensured. However, the secure signature algorithm failed to improve data collection security. A quantum data aggregation approach was developed in [12] for safe transmission and a genetic algorithm to transmit data to its trusted neighbors. A secret sharing scheme was utilized to discover the trusted

RESEARCH ARTICLE

nodes. The genetic method was employed with higher efficiency. However, the system performance of secure communication was not improved.

For privacy preservation and ensuring data integrity, continuous integration and energy-aware secure data aggregation methods were introduced in reference [13]. The slice-mixing method was utilized to preserve confidentiality. An optimal slicing was selected with Fuzzy logic. Key authentication was carried out using GNY logic. However, it did not succeed in achieving data integrity in the results of data aggregation. A lightweight aggregated data encryption model was developed in [14] for WSN. Multiple pairwise shared keys among sensors were utilized to preserve data. But it failed to reduce the performance of delay.

An energy-efficient data aggregation approach was introduced in [15] to give on-demand trusted services via edge computing. Edge was confirmed with blockchain to offer security. However, adequate protection and energy strategies were not implemented to establish efficient communication. A lightweight SATS was developed [16] to enhance safety. The scheme reduces computational overhead, but it did not improve the packet delivery rate.

A new EECS clustering technique was performed in [17] with minimum energy consumption. An optimum value of cluster head was measured with minimum data transmission. However, efficient security analysis was not performed. An improved identity-basis of encryption algorithm (IIBE) was developed in [18] to enhance network security. Key escrow and key revocation issues were avoided. However, the designed algorithm was not applied to the larger area of the WSN network. In [19], a trust strategy based on a dynamic Bayesian game (TSDBG) approach was developed with less packet dropping in transmission. Secure suite was generated between the nodes in the network. Trust and Payoff were estimated. Bayes' rule updated trust value. However, the delay aware transmission was a major challenging issue. An automated lightweight cryptographic method was introduced in [20] to improve the security between the sensor nodes. Dynamic clustering method was developed with support mobility to minimize the overhead. However, the technique did not examine the feasibility of applying various applications. Secure Encryption Random Permutation Pseudo Algorithm (SERPPA) was considered in [21] to ensure network security. A novel anonymous certificateless multi-receiver signcryption mechanism was developed in [22] via private key. But, the time was higher. Certificateless key encapsulated signcryption model was designed in [23] with flying ad hoc networks. Certficateless signcryption method was introduced in [24] by discovering different types of attacks. The PC2SR method was studied in [25] to reduce energy consumption costs. Nevertheless, the packet drop rate was not minimized. The summary is shown in Table 1.

Table 1 Summary Table of Literature Survey

S.No	Method	Contribution	Advantages	Disadvantages
1.	IECC	IECC [1] was developed to improve secure communication	The packet delivery ratio was decreased	Optimal energy consumption was not considered
2.	A secure routing method	The secure routing method [2] was examined with higher secure data aggregation	Delay was minimized	Encryption methods were not utilized
3.	Secure data aggregation protocol	Secure data aggregation protocol [3] was presented to improve security	Confidentiality and integrity were increased	Data aggregation was not sufficient
4.	IBFA	IBFA [4] was developed for secured authentication	The optimal path was selected	Cluster-based secure data transmission was not considered
5.	Asymmetric ECC method	The asymmetric ECC [5] method was employed with higher energy efficiency	Data security was achieved	Delay performance was not minimized

RESEARCH ARTICLE

6.	SHSDA	SHSDA [6] was executed by maximum security	Energy consumption was minimized	Packet delivery was not enhanced
7.	Authorization and verification model	An authorization and verification model [7] was developed for executing secure data collection	The packet loss rate was minimized	The delay was not reduced
8.	TrustAssisted Global and Greedy Congestion-aware model	TrustAssisted Global and Greedy Congestion-aware model [8] was introduced by lesser energy consumption	Reliability was enhanced	Security in data aggregation was not achieved
9.	A one-way associated key management approach was designed in [9] to facilitate secure data transmission	One-way associated key management approach was investigated for secure data transmission.	Delay was minimized	Energy-aware data transmission was not considered
10.	FS-SSL	FS-SSL [10] was carried out with less delay	Throughput was enhanced	Energy consumption was not decreased

3. PROPOSED METHODOLOGY

A WSN comprised numerous powerless sensing devices with restricted communication resources. WSNs are utilized in different applications, namely environmental, health, traffic, agriculture, and energy management. Due to the challenging environments and unique characteristics of WSNs, the security of sensitive information during digital transmission is ensured by sending the sender to the base station or sink by the complex task of middle nodes.

Attackers alter the communicated data or attach unauthorized devices to a network. Unauthorized nodes or attacks can disrupt data communication, leading to packet loss and difficulty achieving a higher delivery rate at the base station.

Consequently, security is vital when transmitting sensed information to isolated base stations. A novel LKC-ICS technique is introduced based on the motivation to achieve energy-efficient aggregated data with an improved network era. The LKC-ICS technique utilizes cryptographic algorithms and energy-efficient security mechanisms to expand the network era.

3.1. System Model

Initially, the number of sensor nodes is $Sn_i = Sn_1, Sn_2, Sn_3 \ldots Sn_n$ employed in marine environments for sensing as well as gathering data of objects in terms of data packets $Dp_1, Dp_2, Dp_3, \ldots . Dp_n$ inside the underwater with initial battery powers. The LKC-ICS technique includes two processes: Laplacian kernelized BFR clustering algorithm and improved certificateless signcryption-based secure data transmission. At first, the whole network is partitioned into different clusters, $C_1, C_2, \ldots . C_k$ Based on power level by applying a Laplacian kernelized BFR clustering algorithm.

After that cluster head 'H_C' is selected to improve the network lifetime of data broadcast in WSN. With the clustered output, improved certificateless signcryption is performed using key generation, signcryption, and unsigncryption. At key generation, the keys are created employing a linear congruential generator.

In Signcryption, the node determines the encryption with the receiver's public key during data transmission into cipher text. The signature generation utilizes a private key to create the digital signature. In unsigncryption, signature verification is performed using ratcliff-obershelp pattern matching.

While the signature obtained matches, the receiver executes decryption to improve secured data transmission with the cluster head and base station. Figure 1 shows the structure of the proposed LKC-ICS technique.

Figure 1 describes the structure of the LKC-ICS technique to achieve energy-efficient and secure data aggregation in WSN.

International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2024/224445 Volume 11, Issue 2, March – April (2024)

RESEARCH ARTICLE

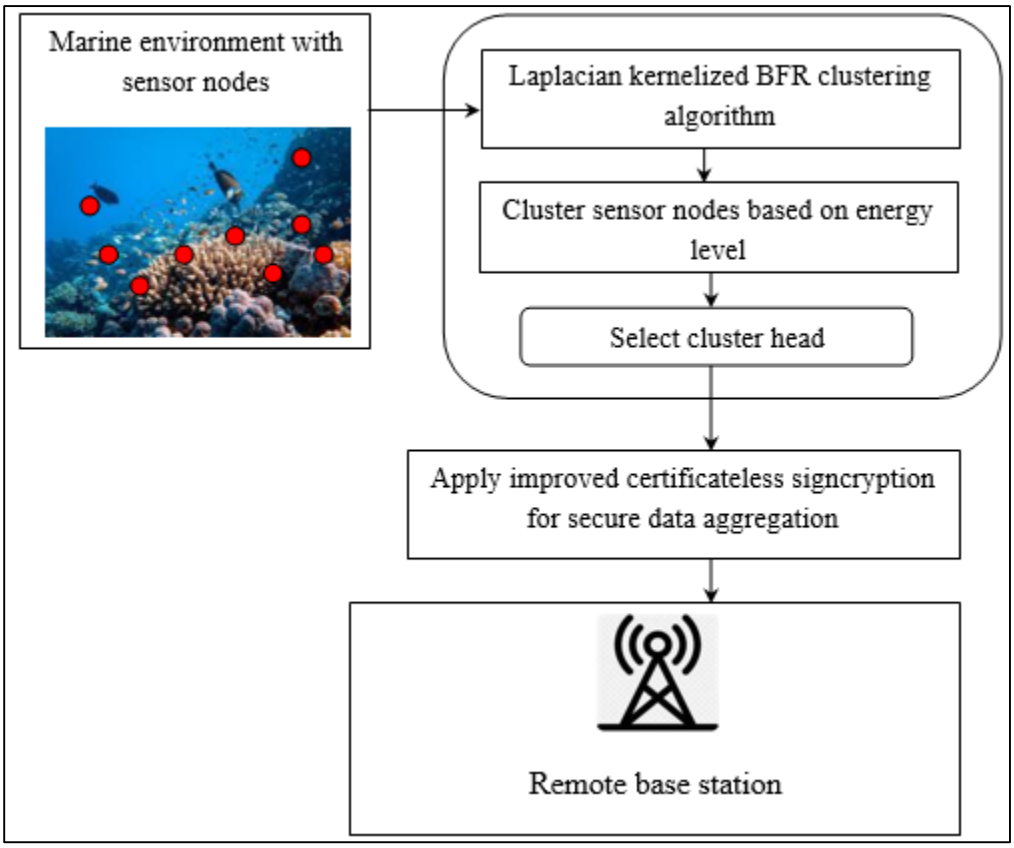

Figure 1 Architecture Diagram of the LKC-ICS Technique

3.2. Laplacian kernelized BFR Clustering Algorithm

The LKC-ICS method performs a clustering process using the BFR clustering algorithm. The clustering process in WSNs is a fundamental technique for efficiently organizing and managing the network's operation. It includes clustering Sn to different clusters for aggregating and forwarding information as of Sn to base station, reducing overall energy utilization of individual Sn.

Energy efficiency is significant in WSN because of the resource-constrained nature of Sn. Therefore, managing and consuming energy is essential to ensure network lifetime and efficient operation.

In node deployment, every sensor node requires an identical initial energy level. The initial energy level decreases due to the sensing and monitoring of the objects in the marine environment. Consequently, the residual energy of Sn is measured by considering the difference between total energy and energy consumed for sensing and monitoring tasks.

The energy of Sn is computed depending on the product of power and time.

$$EG(Sn_i) = p * ti \quad (1)$$

From equation (1),$EG(Sn_i)$ Indicates energy level of Sn, p denotes power in watts, ti is denotes the time. Total energy is measured in joules (J).

After that, the residual energy of Sn, also called remaining energy, defines the amount of energy that remains obtainable in the nodes for performing tasks and other operations.

$$EG_{Res}(Sn_i) = [T\ EG(Sn_i) - CEG(Sn_i)] \quad (2)$$

From equation (2), $EG_{Res}(Sn_i)$ indicates residual energy of Sn,$\mathrm{T}EG\ (Sn_i)_i\ CEG(Sn_i)$ Indicates utilized energy of Sn.

Energy consumption of Sn is measured as follows,

$$CEG\ (Sn_i) = [(EG_T * Dp_F) + (EG_R * Dp_R)] \quad (3)$$

From equation (3), $CEG(Sn_i)$ indicates the energy utilization of Sn,EG_T denotes the energy utilized in single data packet transmission,Dp_F Is the amount of data packets sent by Sn, EG_R indicates energy consumed during a single data packet received, Dp_R Denotes the number of data packets received through Sn.

Then, the clustering process is initiated according to energy levels of Sn present within the marine environment. The

RESEARCH ARTICLE

proposed technique uses the Laplacian kernelized BFR clustering algorithm to group the sensor nodes.

Authors Bradley, Fayyad, and Reina define BFR clustering. Hence, it is called aBFR clustering. It is a k-means algorithm variant employed to cluster sensor nodes based on the centroid. The K-means algorithm is a centroid clustering algorithm. The algorithm clusters the data into k clusters based on similarity. The Laplacian kernel function is employed to calculate the similarity.

Initially, a set of 'k' clusters. 'C_j' is randomly initialized.

$$C_j = C_1, C_2, \ldots. C_k \ where \quad J = 1,2,3 \ldots k \qquad (4)$$

For each cluster, a centroid 'Q_j' is assigned depending on energy levels of Sn.

$$Q_j = Q_1, Q_2, \ldots. Q_k \ where \quad J = 1,2,3..k \qquad (5)$$

From equation (4 and 5), 'C_j' denotes clusters and 'Q_j' centroid of the cluster.Distances between sets of sensor nodes) '$Sn_i = Sn_1, Sn_2, Sn_3 \ldots Sn_n$' is measured as given below.

$$Distance = \sqrt{\left(Sn_{ii} - Sn_{ij}\right)^2 + \left(BS_{ii} - BS_{ij}\right)^2} \qquad (6)$$

From equation (6), the distance 'Dis' is computed by taking into consideration the coordinates of the initial point (i.e., sensor node),'Sn_{ii}', 'Sn_{ij}', and synchronize of the second point (i.e., base station) 'BS_{ii}', 'BS_{ij}'.Subsequently, the clustering process is executed utilizing Laplacian kernel functions. These mathematical functions are used for data clustering, involving the quantification of similarity among cluster centroid as well as $EG_{Res}(Sn_i)$. It assigns higher similarity values to nearby nodes and lower values to farther distant nodes.

The Laplacian kernel function is formulated as follows,

$$L\left(Q_j, EG_{Res}(Sn_i)\right) = exp\left(\frac{|Q_j - EG_{Res}(Sn_i)|}{\vartheta}\right) \qquad (7)$$

From equation (7), Where, $L\left(Q_j, EG_{Res}(Sn_i)\right)$ indicates a Laplacian kernel function, Q_j denotes a centroid of the cluster, $EG_{Res}(Sn_i)$ Denotes residual energy of Sn, ϑ indicates standard deviation. Depending on kernel results, sensors with similar energy levels are grouped into particular clusters. After that, the clustering is selected to cluster heads randomly based on one or more criteria.

The cluster head is gathered with better residual energy with additional cluster members. The selection of cluster heads primarily affects WSN's lifetime. The cluster head is the one that has the remaining power, the number of neighbor nodes, and a lesser distance from the base station. Finally, cluster members send the gathered data to the cluster head for the improved network era.

Input: Sensor nodes $Sn_i = Sn_1, Sn_2, Sn_3 \ldots Sn_n$, collected data packets $Dp_1, Dp_2, Dp_3, \ldots. Dp_n$

Output: Clustering the sensor nodes

Begin

Step 1: For eachSn_iin network

Step 2: Measure residual energy '$EG_{Res}(Sn_i)$' using (2)

Step 3: Initialize 'k' number of clusters 'C_j' and centroid 'Q_j'

Step 4: for eachSn_i with residual energy' $EG_{Res}(Sn_i)$'

Step 5 For each centroid 'Q_j'

Step 6: Measure the similarity '$L\left(Q_j, EG_{Res}(Sn_i)\right)$' using (6)

Step 7: Cluster the sensor nodes into the clusters

Step 8: End for

Step 9: End for

Step 10: For each cluster C_j

Step 11: Select cluster head 'H_C' with higher residual energy

Step 12: The sensor node sends data packets$Dp_1, Dp_2, Dp_3, \ldots. Dp_n$ to cluster head

Step 13: End for

End

Algorithm 1 Laplacian Kernelized BFR Clustering Algorithm

Algorithm 1, given above, depicts the clustering process aimed at enhancing the network lifetime during the data aggregation process in a WSN. Every sensor node within the WSN's residual energy is measured for the dissimilarity between total and consumed energy. Subsequently, a certain number of clusters and their corresponding centroids are initialized randomly. The similarity is computed with each sensor by using the Laplacian kernel function. This similarity measurement guides the grouping of Sn to respective clusters. Within each cluster, H_C, It is chosen depending on higher residual energy to facilitate efficient data aggregation. Lastly, the Snwithin each cluster transmit their collected data packets to their respective H_C.

3.3. Improved Certificateless Signcryption for Secure Data Aggregation

Next, the proposed LKC-ICS technique is comprised of secure data aggregation. Data aggregation is the primary

RESEARCH ARTICLE

technique in WSNs. It's the process of integrating sensor data for reduced data transmission. The data aggregation is obtained with maximum throughput and less communication. In WSN, nodes are dispersed by unwanted data. Due to redundant data transmission, power consumption is reduced to collect and transmit suitable data packets to the base station. It receives the parallel packets and transforms them into a single data packet called an aggregator node. The procedure to send several similar data packets to a single one is called data aggregation. The cluster head is securely sent to the collected data and the base station or sink node in this phase. The primary purpose of this LKC-ICS technique is to improve the data aggregation model for WSN with consent and verification methods. The proposed LKC-ICS technique utilizes the improved certificateless signcryption to enhance security.

Recently, the encryption and decryption process has been named cryptography. The cryptography comprises different secure algorithms for encrypting and decrypting messages. These are all focused on the use of secret named keys. Secure communication is achieved by using cryptography techniques. It is utilized for sensitive information to offer protection from unauthorized access. Signcryption is a cryptographic method. It utilizes public-key technology, capable of executing both digital signatures and encryption functions concurrently. Encryption and digital signatures represent two fundamental cryptographic procedures that ensure the data communication process's confidentiality and integrity. The conventional signcryption method failed to achieve security. Contrary to traditional signcryption, the Rabin cryptosystem is applied to a certificateless signcryption to enhance the safety of data broadcast as a source to sink node.

The proposed signcryption algorithm includes key generation, signcryption, and unsigncryption.

3.3.1. Key Generation

It defines the procedure of generating cryptographic keys used for signcryption and unsigncryption operations. A key is employed to encrypt, and decrypt data, and it is encrypted/decrypted. Cryptographic keys are necessary components of various cryptographic algorithms to ensure the security and confidentiality of sensitive information in data aggregation.

The linear congruential generator is a high-speed and pseudo-random number generator algorithm. It is employed for measuring pseudo-random numbers by discontinuing piecewise linear equations. By applying a linear congruential generator, two distinct prime numbers are generated as follows,

$$A = x_i + r.\ mod\ Z \quad (8)$$

$$B = y_i + s.\ mod\ Z \quad (9)$$

From equation (8 and 9), A, B indicates a prime number, x_i, y_i Denotes initial value, P represents prime number, multiplier r, s is a component of elevated multiplicative order modulo M.

Let us assume two different prime numbers A and B. Therefore, the private and public key of the sensor nodes is generated as given below,

$$G = A * B \quad (10)$$

From equation (10), G denotes the public key, and (A, B) denotes a private key of Sn. The public key is dispersed as a private key reserved covertly and only identified by the corresponding sensor node. Thus, private and public keys created in signcryption and unsigncryption

3.3.2. Signcryption

It is a cryptographic method that integrates digital signature and encryption into solitary operation. Signcryption is a probabilistic algorithm used to generate the cipher text for a given data using both public and private keys. It aims to provide efficient and secure communication by ensuring data confidentiality and integrity.

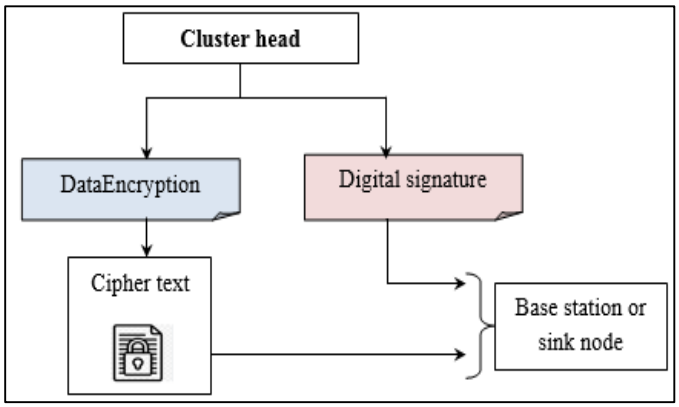

Figure 2 A building Block of Signcryption Process

Figure 2 illustrates a building block of the signcryption process, wherein two distinct operations, namely encryption and digital signature, are executed simultaneously. Encryption is a cryptographic procedure used to convert plaintext data (original data) into ciphertext (unreadable information) with the help of the receiver's public cryptographic key. The primary goal of encryption is to ensure data confidentiality by preventing unauthorized entities from accessing the data during data aggregation in WSN. Next, the electronic signature is produced by the sender's private key. This integration aims to improve the data transmission from the cluster head to the base station or sink node.

The algorithm takes input data packets Dp, and the cipher text is generated as follows,

International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2024/224445 Volume 11, Issue 2, March – April (2024)

RESEARCH ARTICLE

$$\varphi_T = [Dp^2 \, mod G_R] \quad (11)$$

From equation (11), 'φ_T indicates a ciphertext of the original collected data packet 'Dp' in $H_C$and G_R Indicates the public key of the receiver, i.e., base station. Likewise, the digital signature is produced with the help of the sender's private key. A digital signature is a cryptographic method employed to give authenticity to the data.

A digital signature is a fixed-size hash value through the sender's private key uniquely representing contented.

$$S_{Sen} = H_c(Dp \| R) \quad (12)$$

From equation (12), S_{Sen} denotes a digital signature, H_c denotes a hash function, $(Dp \| R)$ Denotes concatenation of the input data and the random value 'R'. Finally, the generated signature and the cipher text are transferred into the base station.

3.3.3. Unsigncryption

Unsigncryption is a cryptographic technique that performs digital signature verification and decryption. Confirmation of signatures is a demanding task. Hence, unsigncryption is required for a system differentiating between genuine and fake signatures to evade the probability of robbery or deception. To enhance security, unsigncryption is executed to attain the original data on the receiver side.

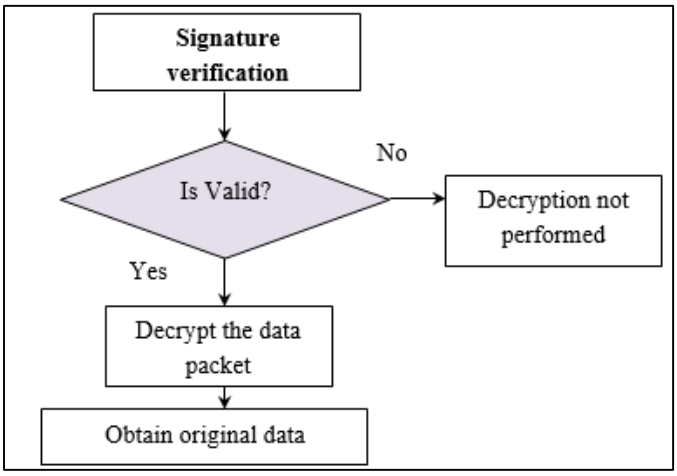

Figure 3 Process of Unsigncryption Process

Figure 3 above shows the process of unsigncryption, which comprises two distinct operations, namely signature confirmation and decryption. The receiver obtains cipher text and then executes the digital signature verification process. If the signature is matched with the sender's digital signature, then the signature is valid. Otherwise, the signature is invalid. The receiver can provide original data way if the signature is valid. This step ensures the authenticity and integrity of the information received. At the receiver part, a hash function is generated for generating the hash value 'S_{Rec}'. Lastly, confirm that 'S_{Rec}' matched through signature produced by the sender. 'S_{Sen}' by ratcliff-obers help pattern matching. Pattern matching is the method of finding specific patterns or sequences within data. The aim of Ratcliff-obers help pattern matching is utilized to measure the similarity between the two hashes.

$$O_{PM} = 2 * \frac{S_{Sen} \cap S_{Rec}}{|S_{Sen}| + |S_{Rec}|} \quad (13)$$

From equation (13), O_{PM} Denotes a Ratcliff-obers help pattern matching, $S_{Sen} \cap S_{Rec}$ denotes the number of matching characters in the two hash values, $|S_{Sen}|$ and $|S_{Rec}|$Denotes a cardinality of a set is the total number of words in a setS_{Sen} and S_{Rec}.This matching provides the value between zero and one.

$$O_{PM} = \begin{cases} 1, & matched \\ 0, & not\ matched \end{cases} \quad (14)$$

From equation (14), the signature gets matched, and the receiver performs decryption and obtains the original data packet. Otherwise, decryption is not performed. The ratcliff-obers help pattern matching and provide accurate results of unsigncryption process.

$$Dp = (u \, . A . X + v . B . Y) \, mod \, G \quad (15)$$

Where, $X = \varphi_T{}^{\frac{1}{4}(A+1)} \, mod \, A$, $= \varphi_T{}^{\frac{1}{4}(B+1)} \, mod \, B$, $u \, . A + v . B = 1$

From equation (15), Dp indicates an original data packet, φ_TDenotes cipher text, A, B represents private key, G denotes public key. After decryption, the original data gets obtained at the base station or sink node. In this way, security is performed.

Input: Dataset, Energy efficient sensor nodes, data packets$Dp_1, Dp_2, Dp_3, \ldots . Dp_n$, cluster head H_c

Output: increase the secure data aggregation

Begin

1. $H_c$collects some data packets $Dp_1, Dp_2, Dp_3, \ldots . Dp_n$from sensor nodes
2. Apply linear congruential generator
3. Generates pair of keys using (8) (9)
4. End for

// Signcryption

5. For each data packet, 'Dp'
6. Convert the data into cipher text. 'φ_T' using (11)
7. Generate the digital signature. 'S_{Sen}'
8. Send ciphertext 'φ_T' and digital signature 'S_{Sen}' to receiver

RESEARCH ARTICLE

9. End for

// Unsigncryption

10. The receiver generates the signature 'S_{Rec}'using (12)
11. Apply ratcliff-obers to help pattern matching using (13)
12. If ($O_{PM} = 1$)then
13. Signature is valid
14. The receiver is said to be authorized
15. Decrypt the data packets using (15)
16. else
17. The signature is not valid
18. Receiver is unauthorized
19. Decryption is denied
20. end if
21. Obtain secure data aggregation

End

Algorithm 2 Improved Certificateless Signcryption

Algorithm 2 delineates different steps concerned with securely aggregating data packets from H_C To base station by improved certificateless signcryption approach. The proposed signcryption process encompasses key generation, signcryption, and unsigncryption. First, the cluster head gathers several data packets from sensor nodes. Key pairs are generated with the aid of a linear congruential generator. Following this, the signcryption process is performed using two steps: encryption and digital signature. The cluster head encrypts the input data packets and generates their corresponding signatures. Encryption is utilized to alter the data into cipher text. The encrypted data and generated signatures are then transmitted by cipher text to the intended receiver. At the receiver's end, an unsigncryption process is implemented to guarantee the data's security. Upon receiving the data, the receiver performs signature verification using a ratcliff-obers to help the pattern-matching process. If the signature is invalid, the receiver is unauthorized and does not perform the decryption process. Then, the secure data transmission is not achieved. If the signature is valid, the receiver proceeds authorized with the decryption process using its private key. This results in the retrieval of original data. This approach greatly enhances the security of data aggregation within WSN.

4. EXPERIMENTAL RESULTS AND EVALUATION

Simulation arrangement of LKC-ICS and conventional techniques are IECC [1] , and secure routing method [2] is executed in NS3 network simulator. To perform simulation, 500 Sn are distributed across the square dimension area. A^2 ($1100\ m\ *\ 1100\ m$) aiming for safe and energy-efficient data aggregation in marine environments. The simulation is set to run for 300 seconds, during which the speeds of the Sn are varied from 0 to 20 m/s. The simulation parameters are listed in Table 2.

Table 2 Simulation Parameters

Simulation Parameter	Value
Simulator	NS3
Number of sensor nodes	50, 100, 150, 200, 250, 300, 350,400,500
Network area	1100m * 1100m
Simulation time	300s
Mobility model	Random Way Point
Routing protocol	DSR
Sensor nodes speed	0-20m/s.
Data packets	100,200,300,400,500,600,700,800,900,1000
Number of runs	10

4.1. Quantitative Analysis

The quantitative analysis of the LKC-ICS method alongside existing methods IECC [1] and the secure routing method [2] are determined by different evaluation metrics. The performance of these dissimilar metrics is analyzed through tabular representation and graphical illustrations.

4.1.1. Analysis of Energy Consumption

Energy utilization of Sn during data aggregation is quantified as the amount of energy utilized. The mathematical calculation for determining the overall energy-efficient sensor node is presented below:

$$E_{Cons} = E_{Cons}(Sn) * \sum_{i=1}^{n} Sn_i \qquad (16)$$

From (15), E_{Cons} indicates energy consumption, n denotes number of sensor nodes, $'E_{Cons}(Sn)'$ denotes the amount of energy utilized through a single sensor node (Sn). It is calculated in joule (J).

Performance study of E_{Cons} Using the proposed -ICS method and conventional methods is presented in Table 3 and Figure 4. Energy consumption is calculated based on the number of sensor nodes ranging from 50 to 500. For each technique, ten distinct outcomes were obtained across various input counts. The overall outcomes indicate that the LKC-ICS method is better than existing techniques in achieving minimal energy consumption. A statistical example supports this conclusion. In the initial iteration with 50 sensor nodes, the energy

RESEARCH ARTICLE

consumption of the LKC-ICS technique was 22.5 Joules, while the existing methods [1] and [2] showed energy consumption of 25 Joules and 27.5 Joules, respectively. Similar performance variations were observed across different scenarios for each method. The results obtained from the LKC-ICS technique were compared to those of conventional techniques. Subsequently, average values of the ten comparison outcomes were calculated, demonstrating which proposed LKC-ICS technique reduces energy consumption by 8% and 16% compared to [1] and [2], respectively. This reduction is achieved by utilizing the Laplacian Kernelized BFR algorithm, which performs clustering of Sn depending on estimated residual energy. Laplacian kernel function is used to identify sensor nodes with energy proximity to the centroid and group them into relevant clusters. Within each cluster, a leader with an efficient energy consumption node is selected to perform secure data aggregation, thereby enhancing network lifetime.

Table 3 Comparison of Energy Consumption

Number of Sensor Nodes	Energy Consumption (J)		
	LKC-ICS	IECC	Secure Routing Method
50	22.5	25	27.5
100	25	30	35
150	31.5	33	36
200	34	38	40
250	37.5	40	43.75
300	42	45	49.5
350	45.5	49	52.5
400	48	52	56
450	49.5	54	58.5
500	52.5	55	60

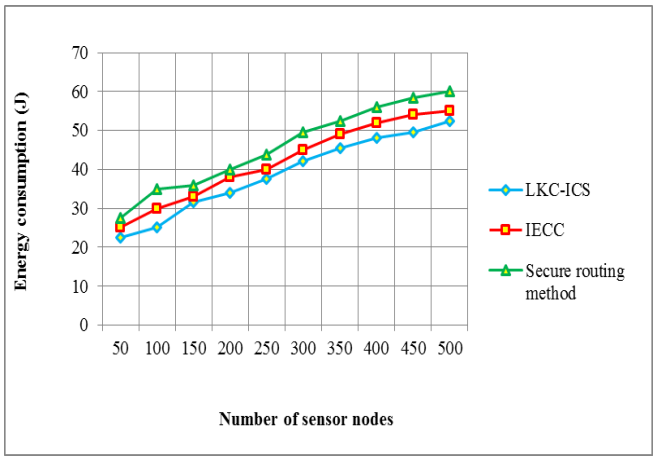

Figure 4 Graphical Analysis of Energy Consumption

4.1.2. Analysis of PDR

The packet delivery ratio is computed by dividing the total amount of data packets effectively received at base station by the overall number of data packets transmitted from the source node. This calculation is represented using the following formula:

$$PDR = \left(\frac{Dp\ received}{Dp\ sent}\right) * 100 \qquad (17)$$

From (17), PDT indicates a packet delivery ratio, $Dp\ received$ denotes a data packet received, $Dp\ sent$ indicates data packet sent. It is in percentage (%).

Table 4 Comparison of Packet Delivery Ratio

Number of Data Packets	Packet Delivery Ratio (%)		
	LKC-ICS	IECC	Secure Routing Method
100	94	90	87
200	94.5	88	85
300	93.33	90	88.33
400	94.5	88.75	86.25
500	94	89	85.6
600	92.16	87.5	84.16
700	90.71	89.28	87.14
800	93.12	88.12	85.62
900	92.77	88.88	86.11
1000	92.5	87.5	85

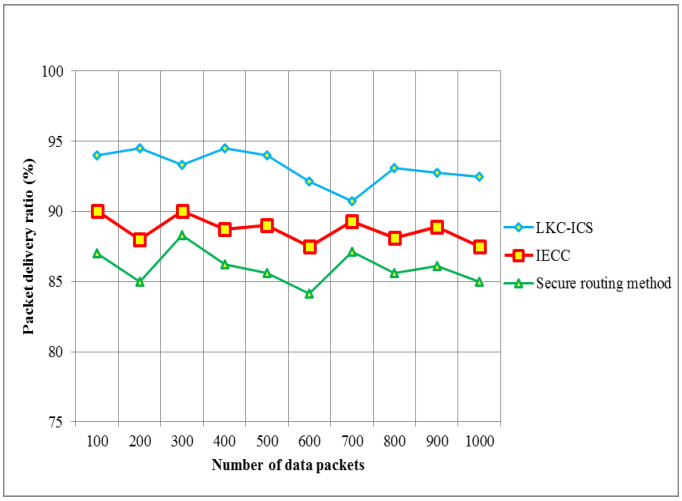

Figure 5 Graphical Analysis of Packet Delivery Ratio

The Table 4 and Figure 5 describe the analysis ofPDR. The results indicate that overall PDR performance using the newly LKC-ICS method outperformed the other existing approaches. During the initial iteration, employing 50 sensor nodes, PDR with LKC-ICS was 94%, while the packet

RESEARCH ARTICLE

delivery ratio of IECC [1] and secure routing method [2] was observed to be 90% and 87%, respectively. Similar divergent performance outcomes were observed across all three methods. Upon obtaining ten sets of results, a comparative study of PDT was conducted between LKC-ICS and the outcomes of the existing methods. The comprehensive comparison shows that of PDT isincreased by 5% and 8% compared to existing [1] and [2], respectively. This notable improvement is achieved by utilizing energy-efficient node selection and securing data transmission mechanisms. To execute data aggregation, nodes through superior residual energy levels are selected, thus widening the network's overall lifetime. An improved certificateless signcryption technique is applied to encrypt original data packets, ensuring their secure transmission to the base station. Consequently, authorized receivers access the original data, and this directly improves PDT.

4.1.3. Analysis of PLR

The packet loss rate is the total amount of data packets lost at the base station by overall data packets transmitted from the source node. This calculation is represented using the following formula:

$$PLR = \left(\frac{Dp\ Lost}{Dp\ sent}\right) * 100 \qquad (18)$$

From (18) PLRindicates a packet loss rate,$Dp\ Lost$denotes a data packetslost, $Dp\ sent$ ndicates data packet sent. It is estimated in percentage (%).

Table 5 Comparison of Packet Loss Rate

Number of Data Packets	Packet Loss Rate (%)		
	LKC-ICS	IECC	Secure Routing Method
100	6	10	13
200	5.5	12	15
300	6.66	10	11.66
400	5.5	11.25	13.75
500	6	11	14.4
600	7.83	12.5	15.83
700	9.28	10.71	12.85
800	6.87	11.87	14.37
900	7.22	11.11	13.88
1000	7.5	12.5	15

Table 5 and Figure 5 present the packet loss rates using three methods, LKC-ICS, and two existing methods, IECC [1] and secure routing method [2]. The graph depicts PLR for all three techniques depending on the amount of data packets. The simulation involved 50 nodes, and outcomes demonstrated PLR of 6% using LKC-ICS, 10% for method [1], and 13% for method [2] in data aggregation. Likewise, various numbers of data packets were analyzed for different performance outcomes. The findings reveal that LKC-ICS significantly reduces the packet loss rate in data aggregation by 32% and 51% compared to methods [1] and [2], respectively. This improvement is achieved through the implementation of an improved certificateless signcryption approach. In the signcryption process, H_C Encrypts input information packets as well as transfer them to a remote sink node. During this process, a signature as a hash value is generated and sent to the receiver. At the receiver's end, the Ratcliff-Obershelp pattern matching is applied to verify the signature. This process effectively minimizes data packet loss caused by unauthorized nodes.

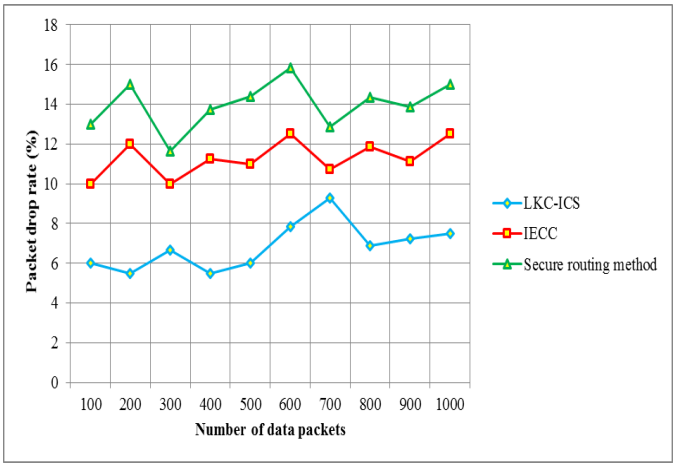

Figure 5 Graphical Analysis of Packet Loss Rate

4.1.4. Analysis of E_{ED}

It is defined as difference based on estimated arrival time at the sink node and the observed arrival time of data packets. It is computed as follows,

$$E_{ED} = [t\ (Dp)_{EXP} - t\ (Dp)_{OBS}] \qquad (19)$$

From equation (19), E_{ED} be an end-to-end delay, $t\ (Dp)_{EXP}$ Denotes the expected arrival time of the data packet, $t\ (Dp)_{OBS}$ Indicates an observed arrival time. End-to-end delay is calculated in milliseconds (ms).

Table 6 Comparison of End-to-End Delay

Number of Sensor Nodes	End-to-End Delay (ms)		
	LKC-ICS	IECC	Secure Routing Method
50	12	15	18
100	14	17	20
150	16	20	24
200	20	22	25
250	22	25	28
300	25	28	33

RESEARCH ARTICLE

350	27	30	35
400	33	35	40
450	35	38	42
500	38	40	44

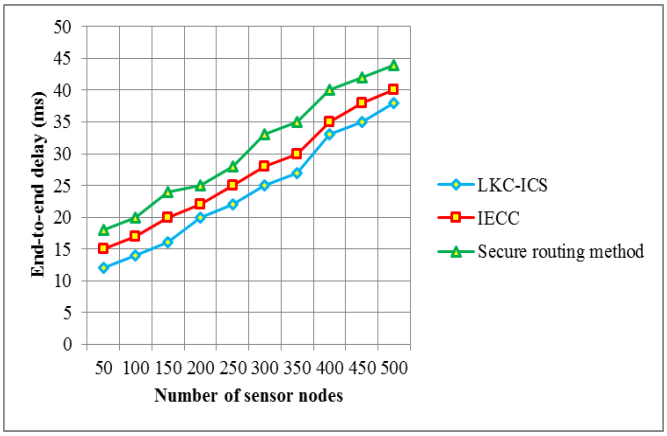

Figure 6 Graphical Analysis of End-to-End Delay

Table 6 and Figure 6 depict the performance analysis of E_{ED} Concerning the number of sensor nodes. Graph demonstrates which E_{ED} Performance using three methods, LKC-ICS, IECC [1], and secure routing method [2], increases as the number of nodes is enhanced. However, comparatively, the E_{ED}Outcomes using LKC-ICS were minimized compared to existing methods. This is because the underwater sensor node identifies energy-efficient head nodes to relay data packets to the base station instead of using the entire Sn. Nodes in the cluster that have higher residual energy than other nodes are selected as cluster heads. For every technique, ten different outcomes are observed and compared. Comparison outcomes indicate which performance of E_{ED} Using LKC-ICS is minimized by 12% and 23% than the [1] and [2].

4.2. Discussion

This section mentions the LKC-ICS method and existing [1] and [2] methods. The limitations of existing methods were higher energy consumption, failure to consider delay, PDR and PLR . The proposed LKC-ICS methods were developed. Contrary to existing works, the LKC-ICS technique employs a Laplacian Kernelized BFR clustering algorithm for examining the residual energy of each sensor with minimum energy consumption and delay. An improved certificateless signcryption technique was developed to encrypt and decrypt unique data to achieve a better delivery ratio. Quantitative analysis of the results demonstrates that the LKC-ICS technique significantly improves energy efficiency and secures data aggregation in WSNs, achieving higher delivery ratios by 7% and minimal packet loss by 42%, energy consumption by 12%, and delay by 18% compared to conventional methods.

5. CONCLUSION

The paper introduces the LKC-ICS technique to enhance data aggregation safety while reducing sensor energy consumption to prolong network lifespan. This technique combines node clustering and encryption methods to improve data aggregation performance in WSNs. Initially, the sensor network consists of marine terminals, onboard sensors, and a land-based base station. The clustering process employs the Laplacian Kernelized BFR algorithm to group Sn depending on their energy levels. After clustering, secure data communication occurs between H_C . Simulations are conducted with varied parameters that consider different numbers of nodes and data packets. The outcomes concluded that the proposed method is better than its competitor in terms of energy consumption and delay, and it has a low loss rate for obtaining secure data transmission. The summary key findings are as follows: proposed LKC-ICS obtained an improved packet delivery ratio by 7% when compared [1] and [2]. LKC-ICS also minimizes energy consumption by 12%, packet loss by 42%, and delay by 18% compared to existing methods.

5.1. Future Work

Our goal was to investigate if our suggested approach may be modified for use in other WSN applications in the future. Security of target detection in WSNs is vital to prevent unauthorized access, preserve the privacy of tracked objects, and guarantee the integrity and reliability of tracking information. Novel certificatelss signcryption method is utilized for accurate target object detection with less time.

REFERENCES

[1] E. T. Oladipupo et al., "An Efficient Authenticated Elliptic Curve Cryptography Scheme for Multicore Wireless Sensor Networks," in IEEE Access, vol. 11, pp. 1306-1323, 2023, doi: 10.1109/ACCESS.2022.3233632.

[2] Ataei Nezhad, M., Barati, H. & Barati, A. “An Authentication-Based Secure Data Aggregation Method in Internet of Things”, J Grid Computing 20, 29 (2022). https://doi.org/10.1007/s10723-022-09619-w.

[3] Murat Dener , SDA-RDOS: “A New Secure Data Aggregation Protocol for Wireless Sensor Networks in IoT Resistant to DOS Attacks”, Electronics 2022,Vol. 11,Issue no:22,(1-30). https://doi.org/10.3390/electronics11244194.

[4] 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.

[5] Shabana Urooj, Sonam Lata, Shahnawaz Ahmad, Shabana Mehfuz, S Kalathil,Cryptographic Data Security for Reliable Wireless Sensor Network, Alexandria Engineering Journal, Volume 72,2023,Pages 37-50,ISSN 1110-0168,https://doi.org/10.1016/j.aej.2023.03.061.

[6] Naghibi, M., Barati, H. SHSDA: “secure hybrid structure data aggregation method in wireless sensor networks”, J Ambient Intell Human Comput 12, 10769–10788 (2021). https://doi.org/10.1007/s12652-020-02751-z.

RESEARCH ARTICLE

[7] S.Ninisha Nels and J. Amar Pratap Singh (2021) ,"Security-aware authorization and verification based data aggregation model for wireless sensor network", International Journal of Numerical Modelling: Electronic Networks, Devices and Fields, vol. 34 ,Issue no:3,(1-20) https://doi.org/10.1002/jnm.2844.

[8] Uvarajan, K.P., Gowri Shankar, C." An Integrated Trust Assisted Energy Efficient Greedy Data Aggregation for Wireless Sensor Networks". Wireless Personal Communications,Vol.114, 813–833 (2020). https://doi.org/10.1007/s11277-020-07394-z.

[9] S. Li et al., "A Secure Scheme Based on One-Way Associated Key Management Model in Wireless Sensor Networks", in IEEE Internet of Things Journal, vol. 8, no. 4, pp. 2920-2930, 15 Feb.15, 2021, doi: 10.1109/JIOT.2020.3021740.

[10] Uras Panahi, Cüneyt Bayılmış,"Enabling secure data transmission for wireless sensor networks based IoT applications", Shams Engineering Journal, Volume 14, Issue 2, 2023,101866, ISSN 2090-4479,https://doi.org/10.1016/j.asej.2022.101866.

[11] Wang, T., Lv, C., Jin, X. et al. "A Secure and Verifiable Continuous Data Collection Algorithm in Wireless Sensor Networks". Wireless Personal Communications, Vol. 119, 2265–2285 (2021). https://doi.org/10.1007/s11277-021-08330-5.

[12] T. -H. Kim and S. Madhavi, "Quantum Data Aggregation Using Secret Sharing and Genetic Algorithm," IEEE Access, vol. 8, pp. 175765-175775, 2020, doi: 10.1109/ACCESS.2020.3026238.

[13] Hajian, R., Erfani, S.H. CHESDA: "continuous hybrid and energy-efficient secure data aggregation for WSN". The Journal of Super Computing, Vol. 77, 5045–5075 (2021). https://doi.org/10.1007/s11227-020-03455-z.

[14] L. Harn, C. -F. Hsu, Z. Xia and Z. He, "Lightweight Aggregated Data Encryption for Wireless Sensor Networks (WSNs)," IEEE Sensors Letters, vol. 5, no. 4, pp. 1-4, April 2021, Art no. 6000704, doi: 10.1109/LSENS.2021.3063326.

[15] A. Ahmed, S. Abdullah, M. Bukhsh, I. Ahmad and Z. Mushtaq, "An Energy-Efficient Data Aggregation Mechanism for IoT Secured by Blockchain," IEEE Access, vol. 10, pp. 11404-11419, 2022, doi: 10.1109/ACCESS.2022.3146295.

[16] 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.

[17] H. H. Rizvi, S. A. Khan, R. N. Enam, M. Naseem, K. Nisar and D. B. Rawat, "Adaptive Energy Efficient Circular Spinning Protocol for Dynamic Cluster Based UWSNs," IEEE Access, vol. 10, pp. 61937-61950, 2022, doi: 10.1109/ACCESS.2022.3181589.

[18] Xuedong Ji, Yuqi Chen, Weikang Yang, Qingjun Wu,"Security and data encryption effect of high ciphertext based on improved RC6 algorithm for WSN", Results in Physics, Volume 53,2023,106959,ISSN 2211-3797,https://doi.org/10.1016/j.rinp.2023.106959.

[19] Muthukkumar, R., Manimegalai, D." Secured transmission using trust strategy-based dynamic Bayesian game in underwater acoustic sensor networks." J Ambient Intell Human Comput 12, 2585–2600 (2021). https://doi.org/10.1007/s12652-020-02418-9.

[20] Osama A. Khashan, Rami Ahmad, Nour M. Khafajah,"An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks", Ad Hoc Networks,Volume115,2021,102448,ISSN15708705,https://doi.org/10.1016/j.adhoc.2021.102448.

[21] S. Nagaraj, Atul B. Kathole, Leena Arya, Neha Tyagi, S. B. Goyal, Anand Singh Rajawat, Maria Simona Raboaca, Traian CandinMihaltan, Chaman Verma and George Suciu (2023) "Improved Secure Encryption with Energy Optimization Using Random Permutation Pseudo Algorithm Based on Internet of Thing in Wireless Sensor Networks", Energies vol. 16, (1-8). https://doi.org/10.3390/en16010008.

[22] L. Pang, M. Kou, M. Wei and H. Li, "Anonymous Certificateless Multi-Receiver Signcryption Scheme Without Secure Channel," IEEE Access, vol. 7, pp. 84091-84106, 2019, doi: 10.1109/ACCESS.2019.2924654.

[23] M. A. Khan et al., "An Efficient and Provably Secure Certificateless Key-Encapsulated Signcryption Scheme for Flying Ad-hoc Network," IEEE Access, vol. 8, pp. 36807-36828, 2020, doi: 10.1109/ACCESS.2020.2974381.

[24] L. Cao, Y. Liu and S. Cao, "An Authentication Protocol in LTE-WLAN Heterogeneous Converged Network Based on Certificateless Signcryption Scheme With Identity Privacy Protection," in IEEE Access, vol. 7, pp. 139001-139012, 2019, doi: 10.1109/ACCESS.2019.2941913.

[25] Ifzarne, S., Hafidi, I. & Idrissi, N. "Compressive sensing and paillier cryptosystem based secure data collection in WSN". J Ambient Intell Human Comput 14, 6243–6250 (2023). https://doi.org/10.1007/s12652-021-03449-6.

[26] Hemapriya, K.E., Saraswathi, S. (2024). An Energy Efficient, Spontaneous, Multi-path Data Routing Algorithm with Private Key Creation for Heterogeneous Network. In: Aurelia, S., J., C., Immanuel, A., Mani, J., Padmanabha, V. (eds) Computational Sciences and Sustainable Technologies. ICCSST 2023. Communications in Computer and Information Science, vol 1973. Springer, Cham. https://doi.org/10.1007/978-3-031-50993-3_20.

Authors

Mrs. K. E Hema Priya a Research Scholar, Her field of study is networking. She currently working as Assistant Professor in the Department of CT & DS at Sri Krishna Arts and Science College. She has ten years of experience teaching computer science. She has completed the NPTEL course, presented papers in national and international conferences, she had a chapter published in the book "New Approaches to Data Analytics and Internet of Things Through Digital Twin" titled" Cybertwin-Driven Resource Provisioning for IoE Applications at6G-Enabled Edge Networks."

Dr. S. Saraswathi, MCA. M.Phil., Ph.D, Dean, Academic Affairs Since 2022, she has been connected to Nehru Arts and Science College in the capacity of Dean of Academic Affairs. She has sixteen years of academic and administrative experience prior to this. She began working as a lecturer at Sri Krishna College of Engineering and Technology in Coimbatore in 2006 and remained there till 2013. Joined Sri Krishna Arts and Science College's Department of Information Technology in 2013 and served as an assistant professor there until 2015. In 2015, he was appointed to Head of the Department of Computer Applications, a position he held until 2022. Additionally, she travelled to the United States, where she experienced the western education offered by Harvard, Clayton State, Concordia, and Washington State universities. She also learnt about the skill-based practices that were added to the Higher Education System in 2019. Her areas of expertise are curriculum development with an outcome-based education focus, effective mentoring, and technology-based teaching methods. She has served in a number of leadership roles, including those of department head, chairman of the computer science study board, member of the academic council, institutional website administrator, malpractice committee member, and other academic committees. Her focus areas are data mining, networking, and evolutionary computing. She has presented numerous research article at national and international conferences, and organised research conferences for the benefit of the faculty and student body. She holds the OCJP Certified Professional designation and has completed a number of online courses, including NPTEL and Spoken Tutorial, which are integrated with the Faculty Development Programme.

RESEARCH ARTICLE

How to cite this article:

K. E Hemapriya, S. Saraswathi, "Laplacian Kernel Clustering-Based Improved Certificateless Signcryption for a Secure Marine Data Aggregation in Network of Wireless Sensors", International Journal of Computer Networks and Applications (IJCNA), 11(2), PP: 177-190, 2024, DOI: 10.22247/ijcna/2024/224445.