Salud, Ciencia y Tecnología - Serie de Conferencias. 2024; 3:650
doi: 10.56294/sctconf2024650

Category: STEM (Science, Technology, Engineering and Mathematics)

ORIGINAL

An Energy-Efficient Cluster Head Selection and Secure Data Transmission in WSN using Spider Monkey Optimized Algorithm and Hybrid Cryptographic with Security

Una Selección de Cabeza de Cluster Energéticamente Eficiente y Transmisión de Datos Segura en WSN usando Algoritmo Optimizado Spider Monkey y Criptografía Híbrida con Seguridad

M. Yuvaraja[1] ✉, S. Sureshkumar[2] ✉, S. Joseph James[3], S. Thillaikkarasi[4]

[1]Department of ECE, P.A. College of Engineering and Technology. Pollachi, India.
[2]Department of Computer Science and Engineering, P. A. College of Engineering and Technology. Pollachi, India.
[3]Department of Computational Intelligence, Faculty of Engineering and Technology. SRM Institute of Science and Technology. Kattankulathur.
[4]Department of ECE, Sri Eshwar College of Engineering. Coimbatore, India.

Cite as: Yuvaraja M, Sureshkumar S, James SJ, Thillaikkarasi S. An Energy-Efficient Cluster Head Selection and Secure Data Transmission in WSN using Spider Monkey Optimized Algorithm and Hybrid Cryptographic with Security. Salud, Ciencia y Tecnología - Serie de Conferencias 2024; 3:650. https://doi.org/10.56294/sctconf2024650.

Submitted: 09-12-2023 **Revised:** 16-02-2024 **Accepted:** 09-03-2024 **Published:** 10-03-2024

Editor: Dr. William Castillo-González

ABSTRACT

To conserve energy in wireless sensor networks, clustering is the well-known strategies. However, choosing a cluster head that is energy efficient is crucial for the best clustering. Because data packets must be transmitted between cluster members and the sink node, improper cluster head selection (CHs) uses more energy than other sensor nodes. As a result, it lowers the network's performance and lifespan. Due to the requirement that this network implement appropriate security measures to guarantee secure communication. This paper provides a novel cluster head selection technique that addresses issues of networks' lives and energy usages using Spider Monkey Optimised Fuzzy C-Means Algorithm (SMOFCM). The CH is chosen using the Spider Monkey Optimisation method in the proposed SMOFCM approach, which builds on the Fuzzy C-means clustering framework. The hybrid cryptographic technique is appropriate for WSN for safe data transmission because it can address sensor challenges such processing power, storage capability, and energy. The Rivest-Shamir-Adleman (RSA), advanced encryption standards (AES), and the suggested algorithm are all used at various stages. Because asymmetric key cryptography makes key management simpler but symmetric key cryptography offers a high level of security. The AES algorithm has been created for phase 1. Phase 2 employed RSA, and all phases were carried out concurrently. According to the simulation results, it reduces energy use, lengthens the network's lifespan, and offers faster encryption, decryption, and execution times for secure data transmission.

Keywords: Wireless Sensor Network (WSN); Spider Monkey Optimised Fuzzy C-Means Algorithm (SMOFCM); Cluster Head (CH); Advanced Encryption Standard (AES); Hybrid Cryptographic; Rivest-Shamir-Adleman (RSA).

RESUMEN

Para conservar la energía en las redes de sensores inalámbricas, la agrupación es una estrategia bien conocida. Sin embargo, la elección de una cabeza de clúster que sea eficiente energéticamente es crucial para la mejor agrupación. Dado que los paquetes de datos deben transmitirse entre los miembros del cluster y el nodo sumidero, una selección inadecuada de la cabeza de cluster (CHs) consume más energía que otros nodos sensores. Como resultado, disminuye el rendimiento y la vida útil de la red. Debido al requisito de que esta red implemente medidas de seguridad adecuadas para garantizar una comunicación segura. Este

trabajo proporciona una novedosa técnica de selección de cabezas de clúster que aborda los problemas de la vida de las redes y el uso de energía utilizando el algoritmo Spider Monkey Optimised Fuzzy C-Means Algorithm (SMOFCM). El CH se elige utilizando el método de optimización Spider Monkey en el enfoque SMOFCM propuesto, que se basa en el marco de agrupación Fuzzy C-means. La técnica criptográfica híbrida es adecuada para la transmisión segura de datos en las WSN, ya que puede hacer frente a los retos que plantean los sensores, como la potencia de procesamiento, la capacidad de almacenamiento y la energía. El algoritmo Rivest-Shamir-Adleman (RSA), los estándares avanzados de cifrado (AES) y el algoritmo sugerido se utilizan en varias etapas. Porque la criptografía de clave asimétrica simplifica la gestión de claves, pero la de clave simétrica ofrece un alto nivel de seguridad. El algoritmo AES se ha creado para la fase 1. En la fase 2 se empleó RSA, y todas las fases se llevaron a cabo simultáneamente. Según los resultados de la simulación, reduce el consumo de energía, alarga la vida útil de la red y ofrece tiempos de cifrado, descifrado y ejecución más rápidos para la transmisión segura de datos.

Palabras clave: Red de Sensores Inalámbricos (WSN); Algoritmo Spider Monkey Optimised Fuzzy C-Means (SMOFCM); Cluster Head (CH); Advanced Encryption Standard (AES); Criptografía Híbrida; Rivest-Shamir-Adleman (RSA).

INTRODUCTION

Numerous sensor nodes are utilised in a wireless network to communicate, compute, and sense between base station and each sensor.[1] Environmental monitoring, traffic monitoring, building structure monitoring, military intelligence gathering and sensing, wildfire detection, habitat monitoring, pollution monitoring, and other domains are among the many areas in which WSN are applicable.[2] A wireless sensor is a node equipped with sensors, transceivers, computers, and power.[3] The computing power, storage, and communication bandwidth of the nodes are all constrained. They use Sinks/Gateways linked to external networks or internet and have wireless connections amongst themselves.[4] Security consequently becomes important featurein wireless sensor networks.[5]

Several different algorithms, cryptography, steganographic, and other approaches are used to safely transmit different types of information via networks. A crucial component of a secure wireless sensor network is cryptography.[6] Numerous cryptography methods, including symmetric, asymmetric, and hybrid ones, have been presented thus far. One secret key is utilized exclusively for decryption and encryption in symmetric key cryptography systems.[7] If that key is lost, the attackers are able to breach the system's entire security. Asymmetric key cryptography methods encode and decrypt data using two different keys.[8] The main problem in this case is key distribution among the communication parties.[9] When contrasted to the symmetric key and, asymmetric key cryptographic process presents superior security in a wide range of applications.

The problem of energy efficiency in Internet of Things (IoT) devices based on Wireless Sensor Networks (WSN) is very hard to tackle with the existing technique. In networks with limited resources, data transmission between nodes can be achieved with great efficiency by using cluster-based hierarchical routing algorithms. Because in order to provide safe communication, this network has to provide appropriate security measures. The hybrid cryptography method can handle issues with compute, storage, and energy for sensors, making it suitable for WSN.

SMOFCM algorithm for energy-based cluster head selection, was developed to address these problems. For safe data transfer, a hybrid cryptographic system with complete security is used. The suggested approach is utilized to extend network lifespan and use less energy. In the recommended SMOFCM method, the cluster formation is constructed utilizing Fuzzy C-means clustering frameworks, and CH is selected using Spider Monkey Optimization strategy. Six important activities have been completed to promote safe interaction within the WSN for secure data transmission. It introduces a new two-phase cryptography method that combines symmetric and asymmetric techniques. The Rivest-Shamir-Adleman (RSA) and advanced encryption standards (AES) algorithms are utilized in various stages of the proposed technique. Because asymmetric key cryptography makes key management simpler but symmetric key cryptography offers a high level of security. Finally, the experimental findings indicate that combining the data and producing the data to the receiver without any attacks increases network lifetime, lowers energy consumption, and prevents attacks.

Literature review

Samiayya et al.[10] The ideal CH is chosen from the cluster group via a new technique called Hybrid Snake Whale Optimisation (HSWO), which aids the information broadcasting network to the target. The initiation phase, the CHS phaseand the route maintenance phase are the three key phases that make up the suggested

concept. The distance model, network model, and energy model are created during the initialization step. Second, using the HSWO algorithm and taking into account the limitations of delay, energy, and distance, the best CHs are chosen by eliminating the worst ones from the clusters.During the route maintenance phase, the efficient way is chosen to transmit the sensed data to the target without link breakage. The suggested HSWO algorithm produced a greater network lifetime and normalised network energy compared to other current methodologies, according to the findings of testing the method's efficacy as measured by several metrics.

Narayan et al.[11] Fuzzy based method combined with Grey Wolf Optimisation Algorithm (FGWOA) is a new algorithm that has been introduced. The facilitates cluster formation by helping to detect the most effective path for data transmission to the network base station (BS) and best approach for selecting the aggregation sites utilising the cluster heads (CH). The node's lifetime is maximised by the recommended best option of numerous aggregation points. In comparison to different existing protocols, the simulation results of FGWOA demonstrate superior performance and longer network lifespan.

METHODOLOGY

The functioning of the SMOFCM technology is given in this section. Each protocol round's setup and steady state phases are distinct. The process of choosing the CH is accelerated during setup. During the setup phase, BS employs SMO as a device to build energy-efficient clusters for a certain NAN sensor, non-overlapping distance, and network residual energy.[12] The CHs gather information from the people in their local cluster during the steady-state intervals and transmit it to base stations (BS).

Fuzzy C-means(FCM) Clustering

The membership function in FCM ascertain extents to which individual data points are connected to clusters. Choosing the centroids of clusters are essential for efficient grouping. Channels are isolated from their own centroids for avoiding interchannel dependences.[13] By comparing similarities or dissimilarities of data points to cluster centroids, cluster memberships are established (y_a to f_{da}). Distances are measured using the Euclidean formula specified in equation 1.

$$FCM = \sum_{a=1}^{k} \sum_{d}^{N} X_{da}^{r} f_{da}^{2} \qquad (1)$$

Where ∑_(a=1)^k▒〖f_da=1〗

The fuzzifier parameter p was utilized to automate the objective function's membership degree control. Equations 2 and 3 were applied to the membership centroid and degree value, respectively.

$$x_{da} = \frac{1}{\sum_{n=1}^{k} (f_{da}^{2} / f_{dn}^{2})} \qquad (2)$$

$$y_a = \frac{\sum_{d=1}^{N} x_{da}^{r} i_d}{\sum_{d=1}^{N} x_{da}^{r}} \qquad (3)$$

The object's membership also reflects the level of input performed by each data object to the novel cluster centre being adjusted in the clustering centre update. While it is a relative number, the resultant membership not included when a typical representation is used. As a result, the cluster center indicated by these memberships may or may not be the true cluster center. It may eventually result in an unexpected cluster result.

Cluster Head Selection

The SMO approach is used to optimize network longevity. If any damaged nodes are incapable to send data, collaborate with surrounding nodes to replace them. The Cluster head SMO type reported in this study enhances on the original SMO's efficiency by leveraging node replacement.[14] The SMO was designed to address the challenge of keeping them contained within a small space. The arithmetic model for SMO is provided by equation 4.

$$T_y^x = \begin{cases} ET_y + q_1\left[(VC_y - NC_y)q_2 + NC_y\right] q_3 \geq 0 \\ ET_y - q_1\left[(VC_y - NC_y)q_2 + VC_y\right] q_3 < 0 \end{cases} \qquad (4)$$

https://doi.org/10.56294/sctconf2024650

Where, Ty^x is the yth dimension's first cluster head position, ET_y implies positions of food Sources in yth dimensions, VC_y represents yth dimensions''supper bounds, NCy is yth dimensions' lower bounds and q_1, q_2 are random numbers in the range [0,1]. Equation 5 uses the significant coefficient r1 to balance the food acquisition and consumption processes.

$$q_1 = 2f^{-\left(\frac{4m}{M}\right)^2} \quad (5)$$

The number L represents the recent round, and M represents the extreme number of rounds, where q 1 is a substantial SSA coefficient.

Spider Monkey Optimization

To replicate smart actions in spider monkeys, SMO use a mathematical model derived from the Fission Fusion Social Structure (FFSS).[15] According to the FFSS, 100 monkeys remain from greater groups to smaller ones to conduct a search. The subsequent are the FFSS's primary mechanisms:

- Every spider monkey begins life in a troop of 40–50 others. Each team has an organizer controlling investigations of food resources and are referred to as global leaders (GL).
- The global leader splits the whole group into segments with three to eight members each who can hunt on their own when there is not enough food for everyone. local leaders (LL) subsequently take charge of their groups.
- Each sub-group's food hunt was decided upon by the local leader.
- Group members use a distinctive sound to communicate with each other and with other members of the group for preserving social relationships and defensive boundaries.

The scientific model of SMO's searching behavior for optimization issues is divided into six parts. SMO generates starter populations of spider monkeys at arbitrarily. A D-dimensional vector represents spider monkeys. Let Q_{ab} represent a^{th} individual's b^{th} dimension. Each Q_{ab} in spider monkey optimization is configured as follows equation 6.

$$Q_{ab} = Q_{minb} + S(0,1) \times (Q_{maxb} - Q_{minb}) \quad (6)$$

Where are lower and upper bounds in b th direction for Q_a and S(0,1) implies random values in the interval [0,1]. Initialization Stage:

The Bernoulli procedure is employed in the first step of the SMO technique to randomly seed a population of N spider monkeys (SM) as equation 7.

$$SMO_{u,v} = \begin{cases} 1, a < prob \\ 0, otherwise \end{cases} \quad (7)$$

Where SMO(u,v) is the v^{th} dimension of the u^{th} spider monkey, a random integer distributed evenly over the interval [0,1], and prob denotes probabilities with a 0,5 value. An arbitrary produced adequacy solution SMO_u (for minimization challenges) is calculated as follows equation 8:

$$fitness_u = \begin{cases} 1 + |f_u|, F_u \leq 0, \\ \frac{1}{1 + F_u}, F_u \geq 0 \end{cases} \quad (8)$$

Where fitness u represents considered issue's fitness functions LL Stage:

In the second stage, the answer is modified based on the knowledge of LL and the team members. To solve a binary optimisation issue, logical AND, XOR, and OR operators were employed. Equation 9 represents the position update equation:

$$\mathrm{SMO}_{\mathrm{u,v}} = \begin{cases} \mathrm{SMO}_{\mathrm{u,v}} \oplus \left(\left(\mathrm{b} \otimes \left(\mathrm{II}_{\mathrm{k,v}} \oplus \mathrm{SMO}_{\mathrm{u,v}}\right)\right) + \left(\mathrm{b} \otimes \left(\mathrm{gl}_{\mathrm{v}} \oplus \mathrm{SMO}_{\mathrm{u,v}}\right)\right)\right) \\ \qquad , \mathrm{rand} \geq \mathrm{pr} \\ \text{use equation 1} \qquad \text{otherwise} \end{cases} \quad (9)$$

where SMO(u,v) and SMO(u,v) is the uth SMO's previous and previous position in the vth dimension, II(k,v) represents the kth groups' LL in vth dimensions, while d and b are binary random values in the interval [0,1] and $\otimes, \oplus, +$ are logical AND, ORand XOR, operators individually, while pr specifies the perturbation rate GL Stage:

https://doi.org/10.56294/sctconf2024650

In this stage, each SM updates its position or velocity update equation based on the data that is available to the other membersand group leader. Positions are changed based on the probability indicated by equation 10:

$$P_u = 0.9 \times \frac{fitness_u}{maximum\_fitness} + 0.1 \quad (10)$$

where P_u signifies the probability, fitness u signifies the fitness of uth SM and maximum fitness signifies group's level of greatest fitness. Equation 11 represents the positional update equations of this stage:

$$SMOn_{u,v} = SMO_{u,v} \oplus \left(\left(b \otimes \left(gl_v \oplus SMO_{u,v}\right)\right) + \left(d \otimes \left(SMO_{r,v} \oplus SMO_{u,v}v\right)\right)\right) \quad (11)$$

where gl_v signifies GL in v^{th} dimensions LL Learning Stage:

Each participant updates their position throughout this phase, and the person who performs the best is selected to serve as the local authority. This procedure will keep going until the local leader no longer sends forth updates. When a certain amount of updates pass without the LL being updated, the LL number is incremented by 1 GL Learning Stage:

The LL's status as the best group is reflected in the GL's new location. When the world leader ceases updating, this process will continue. If, after a predetermined number of updates, the GL fails to update, the GL number is raised by one LL Decision Stage:

The positions of all group members are adjusted as follows if the counts of LL above a certain threshold, LL.

$$SMO_{u,v} = \begin{cases} SMO_{u,v} \oplus \left(\left(b \otimes \left(II_{k,v} \oplus SMO_{u,v}\right)\right) + \left(b \otimes \left(gl_v \oplus SMO_{u,v}\right)\right)\right), \\ rand \geq pr \\ \square \\ use\ equation\ 1, \quad otherwise \end{cases} \quad (12)$$

Global Leader Decision Stage

While the final step of the SMO approach, if there are more global leaders than a certain amount, the GLL, the bigger set is divided into a minor group. The LL's status is updated and the GL combines to form a single team when the maximum number of groups has been established.

Data Transmission using Hybrid Cryptography and End to End Security Model

The suggested method employs the RSAandAES techniques. Plaintext is separated into two blocks here. AES is used to encrypt the block's first section, and RSA is used as the second one. Phase 1 generates ciphertext1 and ciphertext2 on the sender side, which are subsequently transferred to the receiver through a wireless channel. Phase 2 decrypts the data and retrieves the original text.[16] The recommended method is used in two steps: Two procedures are involved in the first step: encryption and plaintext splitting. In the second phase, plaintext 1,2 is converted to plaintext and two decryption operations are performed. Figure 1 depicts the overall structure of the suggested technique.

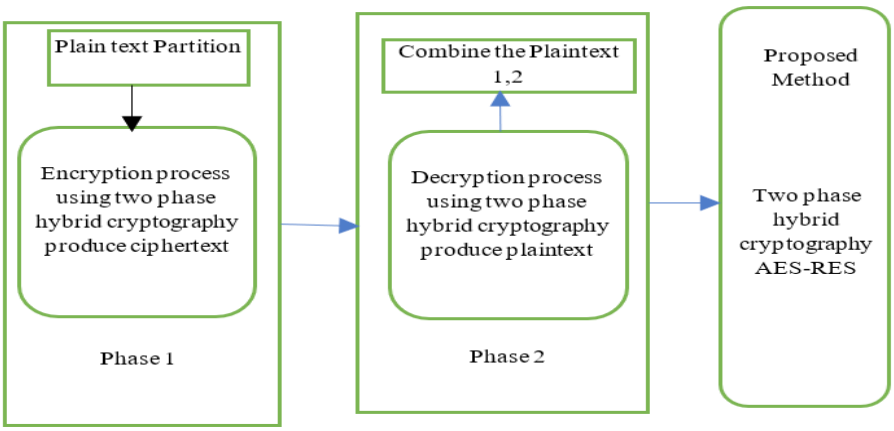

Figure 1. General Layout of the Proposed Method

https://doi.org/10.56294/sctconf2024650

Phase 1: Encryptions

The plain text has been separated into two sections: plaintext 1 and plaintext 2. Figure 5 depicts the first part of the procedure. Using AES, plain text 1 is turned into ciphertext 1.AES uses a strong secret key for decryptionand encryption.[17] Figure 2 depicts the first part of the method. Plaintext 2 is encrypted with RSA to create ciphertext 2.

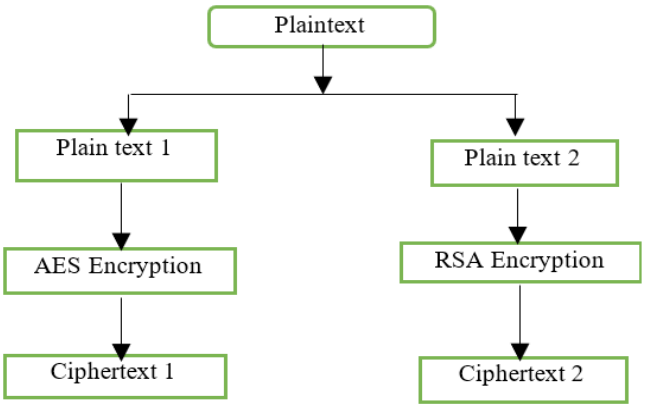

Figure 2. Phase 1 Encryption Phase

Phase 1- AES Encryption Process

The AES method is separated into three parts: encryption, decryption, and key generation. A plaintext is subjected to four various types of modifications. These are sub bytes, mix columns, add round keyand shift rows.

Input: Substitution Box (S-Box), Plaintext1 (PT1), Key

Output: Ciphertext1 (CYT1)

Step 1- sub bytes: Plaintext is divided into states. Each bytes of the state are replaced using S-Box.

Plaintext (PT1) → states (s1, s2, s3, s4...s16)

Step 2- Shift Rows: Shift rows have shifted the row of the states to the left side.

States (s) (Left Shift) → states (s')

Step 3- Mix columns: Mix column is a function, and it transfers the state column by column. It can multiply a state with a constant matrix.

States (s) Mix column → States (s')

Step 4 – Add Round Key: Add round key with a state. Make a plain text into unreadable format.

States (s) (Add round Key) → Ciphertext1 (CYT1)Phase 1- RSA Encryption Process

Input: Plaintext 1 (PT2), two prime numbers t1, t2, RSA Public Key {n,e}

Output: Ciphertext2 (CYT2)

Step 1: Select two Prime numbers t1, t2,

compute n=t1*t2

pi (n)= (t1-1) *(t2-1)

Step 2 Encryption: Ciphertext2 (CYT2) → Plaintext 2 (PT2)^e mod n

Phase 2: Decryption Process

Phase 2: Decryption Algorithm (Receiver side Process)

Input: ciphertext1 (CYT1), Ciphertext2 (CYT2), AES, RSA

Output: Plaintext (P), Plaintext1 (PT1), Plaintext2 (PT2)

Step 1: AES decryption Ciphertext1 (CYT1) → Plaintext1 (PT1)

Step 2: RSA decryption Ciphertext2 (CYT2) → Plaintext2 (PT2)

Step 3: Combined the Plaintext1 (PT1), Plaintext2 (PT2) → Plaintext (P)The AES and RSA techniques are used in phase 2 decryption methods. Ultimately, plaintext1 and plaintext2 are produced. On the receiver side, combine the two plaintexts. Figure 3 depicts the decryption procedure.

https://doi.org/10.56294/sctconf2024650

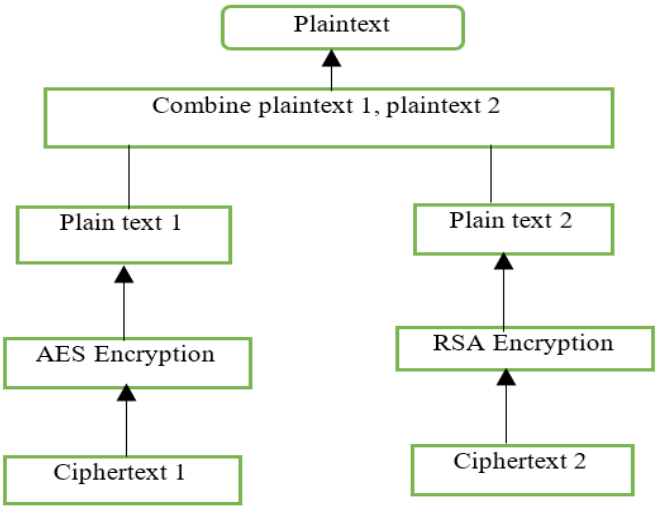

Figure 3. Phase 2 Decryption Process

Phase 2- AES decryption Process

Input: Ciphertext1 (CYT1), substitution Box (s-Box)

Output: Plaintext1 (PT1)

Step 1- Rev (Sub bytes): Plaintext is divided into states. Each byte of the state is replaced using S-Box.

Plaintext1 (PT1) → states (s1, s2, s3, s4…. S16)

Step 2- Rev (Shift Rows): Shift rows have shifted the row of the states to the left side.

states (s) (Left Shift) → states (s')

Step 3- Rev (Mix Columns): Mix Columns is a function, and it transfers the state column by column. It can multiply a state with a constant matrix.

states (s) (Mix column) → states (s')

Step 4- Rev (Add Round Key): Add round key with a state. Make a plaintext into unreadable format.

states (s) (Add Round Key) → Ciphertext1 (CYT1).Phase 2-RSA decryption Process

1. Input: Ciphertext2 (CYT2), two prime numbers t1, t2, RSA Public Key {n,e}, private key {d}
2. Output: Plaintext1 (PT2)
3. Step 1: compute ed =1 mod (t1-1) (t2-1)
4. Step 2: Decryption: Plaintext1 (PT2) → ciphertext2 (CYT2)^e mod n

RESULTS AND DISCUSSION

The outcomes of the suggested SMOFCM are discussed. The answers were developed using MATLAB. Several constraints are used to assess the effectiveness of the proposed SMOFCM, including throughput, energy consumption, and network lifetime. The suggested structure is compared to accepted methods[22] using K-means,[18] DRESEP,[19] and SMOTECP.[20,21] The simulation parameters of the recommended SMOFCM architecture are shown in table 1.

Table 1.SMOFCM Framework's Parameters used in Simulations

Simulations	Parameters
Node Counts	100
Network Area Sizes	100m × 100m
Locations of BS	(50,50)
Packet sizes	4000 bits
CH Counts	10
Simulation times	400 s
Initial Energies	50

Energy Consumption

The term "energy consumption" refers to the entire energy consumption of a system when transmitting a

https://doi.org/10.56294/sctconf2024650

data packet network life time:

The lifetime of a network is the amount of time it is fully operational. As they travel over the network, route requests are determined at each node.

Throughput

Throughput implies data packets counts that successfully arrive at BS.

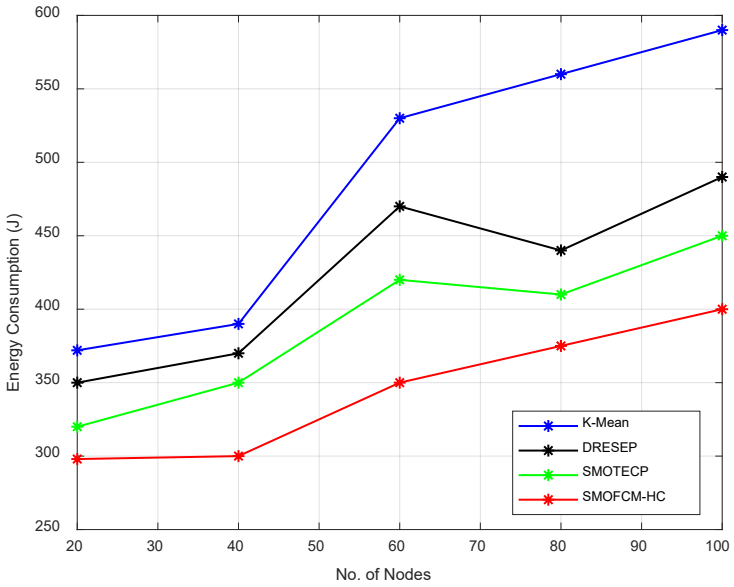

Figure 4. Performance Analysis of Energy Consumption

Figure 4 compares the recommended SMOFEM's energy consumption to that of the prior systems shown in figure 2 (DRESEP,K-MEANS and SMOTECP), and the latter approach provides a longer network lifespan. Time in the simulation is below 20, 40, 60, 80, and 100.

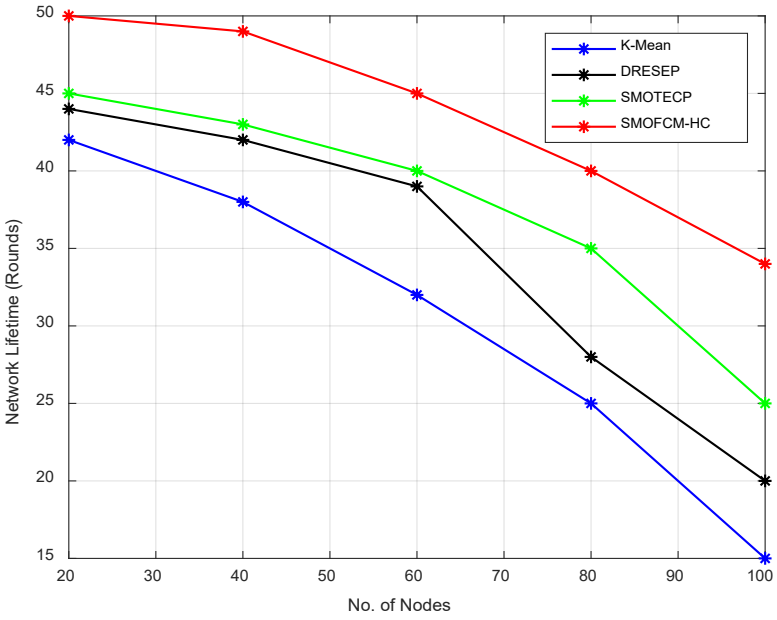

Figure 5. Performance Analysis of Network Lifetime

Figure 5 shows the network lifetime with various node numbers. The recommended SMOFCM-HC approach achieves the highest lifespan up to 100 rounds, whereas the K-Means approach achieves the lowest lifetime up to 100 rounds.

https://doi.org/10.56294/sctconf2024650

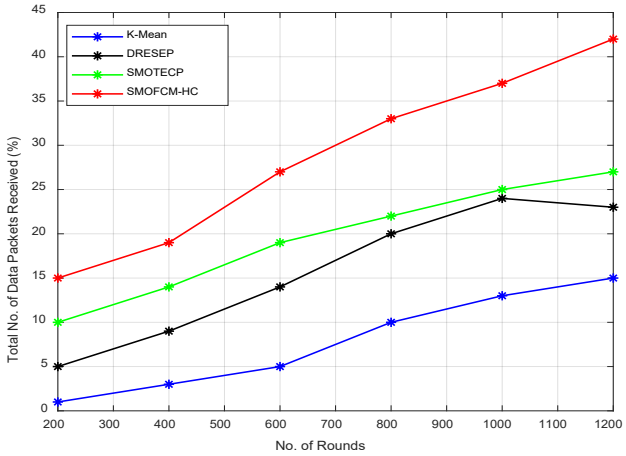

Figure 6. Performance Analysis of Throughput

Figure 6 displays the comparison between the simulation results and the conventional techniques. K-Means only received the lowest quality data packets. A considerable number of data packets have been obtained by recommended approach at the BS when compared to K-MEANS, DRESEP, SMOTECP, and SMOFCM-HC.

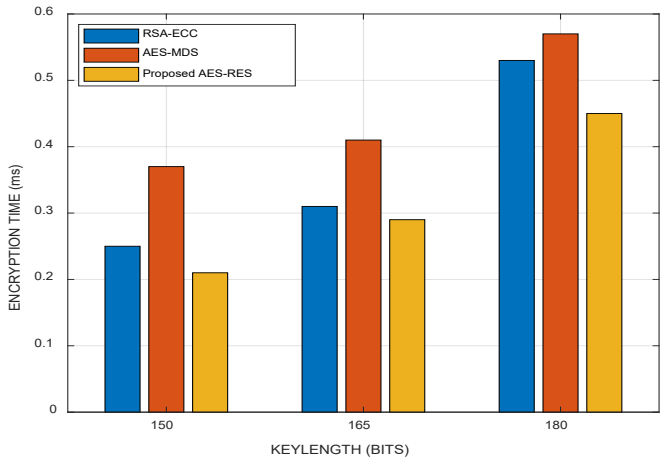

Figure 7. Performance Result of Encryption Time

According to figure 7, the length of time required for encryption increases with key size. The suggested method AES-RSA separates the plaintext into partitions, which speeds up the encryption procedure in comparison to RSA-ECC and AES-MD5.

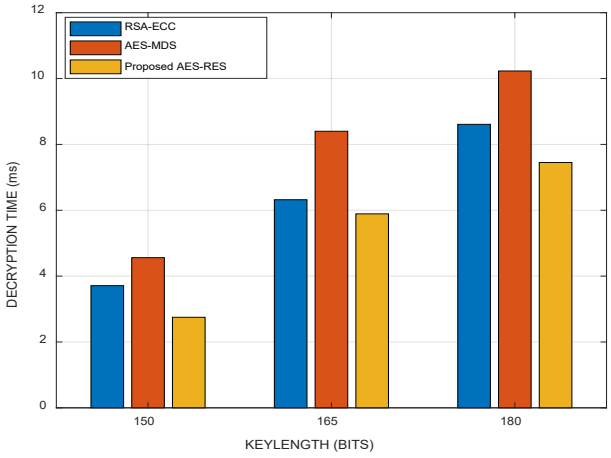

Figure 8. Performance Analysis of Decryption Time

https://doi.org/10.56294/sctconf2024650

Decryption time increases with key size, as shown figure 8. The suggested system AES-RSA separates the ciphertext into partitions, which speeds up the decryption process compared to RSA-ECC and AES-MD5.

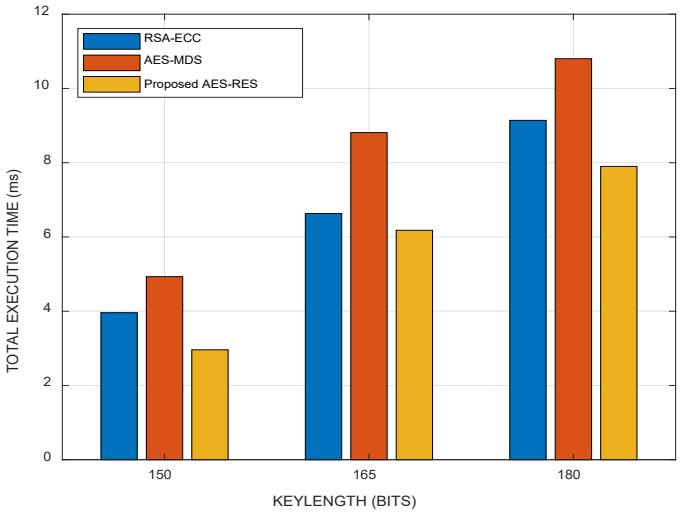

Figure 9. Performance Analysis of Total Execution Time

Figure 9 Depending on the key and text sizes, the overall execution time varies. Here, RSA-ECC and AES-MD5 take longer to run than the suggested system.

CONCLUSION

This work develops a novel SMOFCM technique to increase network lifetime and reduce energy consumption. The Cluster Head (CH) is chosen by optimization techniques, and the fuzzy C-Means clustering framework is mostly used with the suggested strategy to achieve cluster formation. An approach based on hybrid cryptography provides secure data transfer in WSN. One key is tracked for decryption and encryption using symmetric-key cryptography. Thus, it has a quick computation rate. Information can be shared very securely with an asymmetric key. Both can offer increased defence against assaults on wireless networks. This paper introduces a new two-phase cryptography method that combines symmetric and asymmetric techniques. The findingsdemonstrate that the recommended technique outperforms than the conventional strategies, lengthening network lifetime and using less energy. The safe data transmission in WSN is improved by the hybrid symmetric and asymmetric cryptographic procedure.

REFERENCES

1. G. Khan, S. Basharat and M. U. Riaz, “Analysis of asymmetric cryptography in information security based on computational study to ensure confidentiality during information exchange,” International Journal of Scientific & Engineering Research, vol.9, no.11, pp.992-999, 2018.

2. H. Jabbar and I. S. Alshawi, “Spider monkey optimization routing protocol for wireless sensor networks,” International Journal of Electrical & Computer Engineering, vol.11, no.3,pp.2432-2442, 2021.

3. Mahboub and M. Arioua, “Energy-efficient hybrid k-means algorithm for clustered wireless sensor networks,” International Journal of Electrical and Computer Engineering, vol.7, no.4, pp.2054-2060, 2017.

4. S. Tushar and A. Mishra, “Cryptographic Algorithm for Enhancing Data Security: A Theoretical Approach,” International Journal of Engineering Research & Technology, vol.10, no.03, pp.274-277, 2021.

5. Amado DPA, Diaz FAC, Pantoja R del PC, Sanchez LMB. Benefits of Artificial Intelligence and its Innovation in Organizations. AG Multidisciplinar 2023;1:15-15. https://doi.org/10.62486/agmu202315.

6. Bhushan, C. Sahoo, P. Sinha and A. Khamparia, “Unification of Blockchain and Internet of Things (BIoT): requirements, working model, challenges and future directions,” Wireless Networks, vol.27, no.1, pp.55- 90, 2021.

7. Batista-Mariño Y, Gutiérrez-Cristo HG, Díaz-Vidal M, Peña-Marrero Y, Mulet-Labrada S, Díaz LE-R. Behavior of stomatological emergencies of dental origin. Mario Pozo Ochoa Stomatology Clinic. 2022-2023. AG Odontologia 2023;1:6-6. https://doi.org/10.62486/agodonto20236.

8. Caero L, Libertelli J. Relationship between Vigorexia, steroid use, and recreational bodybuilding practice and the effects of the closure of training centers due to the Covid-19 pandemic in young people in Argentina. AG Salud 2023;1:18-18. https://doi.org/10.62486/agsalud202318.

9. Cavalcante L de FB. Feminicide from the perspective of the cultural mediation of information. Advanced Notes in Information Science 2023;5:24-48. https://doi.org/10.47909/978-9916-9906-9-8.72.

10. Chalan SAL, Hinojosa BLA, Claudio BAM, Mendoza OAV. Quality of service and customer satisfaction in the beauty industry in the district of Los Olivos. SCT Proceedings in Interdisciplinary Insights and Innovations 2023;1:5-5. https://doi.org/10.56294/piii20235.

11. Chávez JJB, Trujillo REO, Hinojosa BLA, Claudio BAM, Mendoza OAV. Influencer marketing and the buying decision of generation «Z» consumers in beauty and personal care companies. SCT Proceedings in Interdisciplinary Insights and Innovations 2023;1:7-7. https://doi.org/10.56294/piii20237.

12. Paulraj, R. Lavanya, T. Jayasudha, M. I. Niranjana, T. Daniyaand F. D. Shadrach, "Blockchain-based Wireless Sensor Network Security Through Authentication and Cluster Head Selection," In 2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS, 2023, pp. 1-5.

13. Samiayya, S. Radhika and A. Chandrasekar, "An optimal model for enhancing network lifetime and cluster head selection using hybrid snake whale optimization," Peer-to-Peer Networking and Applications, vol.16, no.4, pp.1959-1974, 2023.

14. Diaz DPM. Staff turnover in companies. AG Managment 2023;1:16-16. https://doi.org/10.62486/agma202316.

15. Espinosa JCG, Sánchez LML, Pereira MAF. Benefits of Artificial Intelligence in human talent management. AG Multidisciplinar 2023;1:14-14. https://doi.org/10.62486/agmu202314.

16. Figueredo-Rigores A, Blanco-Romero L, Llevat-Romero D. Systemic view of periodontal diseases. AG Odontologia 2023;1:14-14. https://doi.org/10.62486/agodonto202314.

17. Gonzalez-Argote J, Castillo-González W. Productivity and Impact of the Scientific Production on Human-Computer Interaction in Scopus from 2018 to 2022. AG Multidisciplinar 2023;1:10-10. https://doi.org/10.62486/agmu202310.

18. Hernández-Flórez N. Breaking stereotypes: "a philosophical reflection on women criminals from a gender perspective". AG Salud 2023;1:17-17. https://doi.org/10.62486/agsalud202317.

19. Hinojosa BLA, Mendoza OAV. Perceptions on the use of Digital Marketing of the micro-entrepreneurs of the textile sector of the Blue Gallery in the emporium of Gamarra. SCT Proceedings in Interdisciplinary Insights and Innovations 2023;1:9-9. https://doi.org/10.56294/piii20239.

20. J. C. Bezdek, R. Ehrlich and W. Full, "FCM: The fuzzy c-means clustering algorithm," Computers & geosciences, vol.10, no.2-3, pp.191-203, 1984.

21. J. Uthayakumar, T. Vengattaraman and P. Dhavachelvan, "A new lossless neighborhood indexing sequence (NIS) algorithm for data compression in wireless sensor networks," Ad Hoc Networks, vol.83, pp. 149- 157, 2019.

22. K. Vanitha, K. Anitha, A. M. Z. Rahaman and M. M. Musthafa, "Analysis of Cryptographic Techniques in Network Security," Journal of Applied Science and Computations, vol.5, no.8, pp.155-163, 2018.

23. Lamorú-Pardo AM, Álvarez-Romero Y, Rubio-Díaz D, González-Alvarez A, Pérez-Roque L, Vargas-Labrada LS. Dental caries, nutritional status and oral hygiene in schoolchildren, La Demajagua, 2022. AG Odontologia 2023;1:8-8. https://doi.org/10.62486/agodonto20238.

24. Ledesma-Céspedes N, Leyva-Samue L, Barrios-Ledesma L. Use of radiographs in endodontic treatments in pregnant women. AG Odontologia 2023;1:3-3. https://doi.org/10.62486/agodonto20233.

25. Lopez ACA. Contributions of John Calvin to education. A systematic review. AG Multidisciplinar 2023;1:11-11. https://doi.org/10.62486/agmu202311.

26. M. Al-Hawawreh, I. Elgendi and K. Munasinghe, "An Online Model to Minimize Energy Consumption of IoT sensors in Smart Cities," IEEE Sensors Journal, vol.22, no.20, pp.19524-19532, 2022.

27. M. P. Gharat and D. Motawani, "Overview on Symmetric Key Encryption Algorithms," International Journal of Engineering Research and Applications, vol.4, no.9, pp.123-126, 2014.

28. Marcillí MI, Fernández AP, Marsillí YI, Drullet DI, Isalgué RF. Older adult victims of violence. Satisfaction with health services in primary care. SCT Proceedings in Interdisciplinary Insights and Innovations 2023;1:12-12. https://doi.org/10.56294/piii202312.

29. Marcillí MI, Fernández AP, Marsillí YI, Drullet DI, Isalgué VMF. Characterization of legal drug use in older adult caregivers who are victims of violence. SCT Proceedings in Interdisciplinary Insights and Innovations 2023;1:13-13. https://doi.org/10.56294/piii202313.

30. Moraes IB. Critical Analysis of Health Indicators in Primary Health Care: A Brazilian Perspective. AG Salud 2023;1:28-28. https://doi.org/10.62486/agsalud202328.

31. N. Mittal and U. Singh, "Distance-based residual energy-efficient stable election protocol for WSNs," Arabian Journal for Science and Engineering, vol.40, pp. 1637-1646, 2015.

32. N. Mittal, U. Singh, R. Salgotra and B. S. Sohi, "A boolean spider monkey optimization-based energy efficient clustering approach for WSNs,"Wireless Networks, vol.24, pp.2093-2109, 2018.

33. N. Vidhya, V. Seethalakshmi, R. Monisha, J. Dhanasekar, V. Gurunathan and C. Rajanandhini, "Coherent Data Transmission Using Multiplexing for a DWDM Communication System," In 2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon), 2022, pp. 1-4.

34. Ogolodom MP, Ochong AD, Egop EB, Jeremiah CU, Madume AK, Nyenke CU, et al. Knowledge and perception of healthcare workers towards the adoption of artificial intelligence in healthcare service delivery in Nigeria. AG Salud 2023;1:16-16. https://doi.org/10.62486/agsalud202316.

35. Peñaloza JEG, Bermúdez L marcela A, Calderón YMA. Perception of representativeness of the Assembly of Huila 2020-2023. AG Multidisciplinar 2023;1:13-13. https://doi.org/10.62486/agmu202313.

36. Pérez DQ, Palomo IQ, Santana YL, Rodríguez AC, Piñera YP. Predictive value of the neutrophil-lymphocyte index as a predictor of severity and death in patients treated for COVID-19. SCT Proceedings in Interdisciplinary Insights and Innovations 2023;1:14-14. https://doi.org/10.56294/piii202314.

37. Prado JMK do, Sena PMB. Information science based on FEBAB's census of Brazilian library science: postgraduate data. Advanced Notes in Information Science 2023;5:1-23. https://doi.org/10.47909/978-9916-9906-9-8.73.

38. Pupo-Martínez Y, Dalmau-Ramírez E, Meriño-Collazo L, Céspedes-Proenza I, Cruz-Sánchez A, Blanco-Romero L. Occlusal changes in primary dentition after treatment of dental interferences. AG Odontologia 2023;1:10-10. https://doi.org/10.62486/agodonto202310.

39. Quiroz FJR, Oncoy AWE. Resilience and life satisfaction in migrant university students residing in Lima. AG Salud 2023;1:9-9. https://doi.org/10.62486/agsalud20239.

40. Roa BAV, Ortiz MAC, Cano CAG. Analysis of the simple tax regime in Colombia, case of night traders in the city of Florencia, Caquetá. AG Managment 2023;1:14-14. https://doi.org/10.62486/agma202314.

41. Rodríguez AL. Analysis of associative entrepreneurship as a territorial strategy in the municipality of

Mesetas, Meta. AG Managment 2023;1:15-15. https://doi.org/10.62486/agma202315.

42. Rodríguez LPM, Sánchez PAS. Social appropriation of knowledge applying the knowledge management methodology. Case study: San Miguel de Sema, Boyacá. AG Managment 2023;1:13-13. https://doi.org/10.62486/agma202313.

43. S. Kaviarasan and R. Srinivasan, "A Novel Spider Monkey Optimized Fuzzy C-Means Algorithm (SMOFCM) for Energy-Based Cluster-Head Selection in WSNs," International Journal of Electrical and Electronics Research (IJEER), vol.11, no.1, pp.169-175, 2023.

44. S. Mody, S. Mirkar, R. Ghag and P. Kotecha, "Cluster Head Selection Algorithm for Wireless Sensor Networks Using Machine Learning," In 2021 International Conference on Computational Performance Evaluation (ComPE), 2021, pp. 445-450.

45. S. Sultana, G. Ghinita, E. Bertino and M. Shehab, "A Lightweight Secure Scheme for Detecting Provenance Forgery and Packet Drop Attacks in Wireless Sensor Networks," IEEE Transactions On Depedable And Secure Computing, vol. 6, no. 1, pp. 1-14, 2015.

46. S. Urooj, S. Lata, S. Ahmad, S. Mehfuz and S. Kalathil, "Cryptographic Data Security for Reliable Wireless Sensor Network," Alexandria Engineering Journal, vol.72, pp.37-50, 2023.

47. Serra S, Revez J. As bibliotecas públicas na inclusão social de migrantes forçados na Área Metropolitana de Lisboa. Advanced Notes in Information Science 2023;5:49-99. https://doi.org/10.47909/978-9916-9906-9-8.50.

48. Solano AVC, Arboleda LDC, García CCC, Dominguez CDC. Benefits of artificial intelligence in companies. AG Managment 2023;1:17-17. https://doi.org/10.62486/agma202317.

49. T. Alam, "Cloud-based IoT applications and their roles in smart cities," Smart Cities, vol.4, no.3, pp.1196-1219, 2021.

50. T. Sampradeeprajand V. A. Devi, "A Hybrid Cryptography and End-to-end Security Model for Wireless Sensor Networks," Research Square, pp.1-23, 2022.

51. V. Narayan, A. K. Danieland P. Chaturvedi, "FGWOA: An efficient heuristic for cluster head selection in WSN using fuzzy based grey wolf optimization algorithm," Research Square, pp.1-16, 2022.

FINANCING

There is no funding for this work.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

AUTHORSHIP CONTRIBUTION

Conceptualization: Yuvaraja M, Sureshkumar S, James SJ, Thillaikkarasi S.
Research: Yuvaraja M, Sureshkumar S, James SJ, Thillaikkarasi S.
Methodology: Yuvaraja M, Sureshkumar S, James SJ, Thillaikkarasi S.
Project management: Yuvaraja M, Sureshkumar S, James SJ, Thillaikkarasi S.
Original drafting-drafting: Yuvaraja M, Sureshkumar S, James SJ, Thillaikkarasi S.
Writing-revising and editing: Yuvaraja M, Sureshkumar S, James SJ, Thillaikkarasi S.