Enhancing wireless sensor network security with optimized cluster head selection and hybrid public-key encryption

Chaya Puttaswamy[1], Nandini Prasad Kanakapura Shivaprasad[2]
[1]Department of Information Science and Engineering, GSSS Institute of Engineering and Technology for Women, Mysore, Affiliated to Visvesvaraya Technological University, Belagavi, India
[2]Department of Information Science and Engineering, Dayananda Sagar Academy of Technology and Management, Bangalore, Affiliated to Visvesvaraya Technological University, Belagavi, India

Article Info

Article history:

Received Jan 25, 2024
Revised Feb 26, 2024
Accepted Feb 27, 2024

Keywords:

Energy and security efficiency
Fuzzy logic
Intelligent decision logic
Lightweight hybrid encryption
Wireless sensor network

ABSTRACT

This paper introduces an integrated methodology that enhances both the efficiency and security of wireless sensor networks (WSNs) against various active attacks. A two-fold strategy is proposed that incorporates an advanced cluster head (CH) selection and a customized, lightweight encryption protocol. The CH selection process is optimized through a multi-phase approach using fuzzy logic, local and global network qualifiers, and a trust index to ensure the election of CHs that are not only energy-efficient but also reliable. To complement the robust CH selection, the study introduces a hybrid yet lightweight encryption scheme customized Rivest-Shamir-Adleman (c-RSA) and customized advanced encryption standard (c-AES) algorithms. This scheme is customized for WSNs with limited computational resources, maintaining strong encryption standards while significantly reducing energy consumption and computational overhead. Experimental results demonstrate that the proposed system substantially enhances network performance, exhibiting a 34.15% improvement in energy efficiency and a 30.95% increase in reliability over existing methods such as LEACH and its modified versions. This comprehensive approach underscores the potential for a synergistic design in WSNs that does not compromise on security while optimizing operational efficiency.

Corresponding Author:

Chaya Puttaswamy
Department of Information Science and Engineering, GSSS Institute of Engineering and Technology for Women
Mysore-570016, India
Email: chayaneetha@gmail.com

1. INTRODUCTION

In the constantly evolving world of modern technology, wireless sensor networks (WSNs) play a key role in enabling the internet of things (IoT) ecosystem [1]. A WSN consists of many small, low-power sensor nodes collaborating to gather, process, and communicate data from their deployed environment [2]. This technology has many applications, including environmental monitoring, smart healthcare, smart cities, precision agriculture, and industrial automation. The basic idea of WSNs is to distribute sensing and communication capabilities to enable real-time data collection and decision-making [3]. While WSNs have the potential to revolutionize industries and improve our daily experiences, designing and operating these networks pose several major challenges. One of the critical issues is energy efficiency because, in WSN, sensor nodes are usually powered by non-rechargeable and non-replaceable batteries. This means saving energy is crucial to extending the network's lifetime, thereby ensuring sustainable and autonomous operation

[4]. Besides energy efficiency, security ranks crucial in WSNs as they are increasingly used in critical infrastructures and other sensitive applications. WSNs are vulnerable to various security threats, such as data interception, tampering, and node leakage [5], [6]. These threats can pose significant risks to the integrity of collected data, unauthorized access, and compromised network operations. Therefore, achieving a balance between energy efficiency and security becomes crucial in the design of wireless sensor networks. In literature, several schemes have already been proposed to address the energy efficiency and security challenges in WSNs, but they often fail to provide a comprehensive and integrated solution [7], [8]. Many of these schemes are based on certain assumptions and specific design considerations, which may not be able to adapt to the dynamic and unpredictable nature of WSN environments. In addition, some approaches can place too much of a computational burden on the resource-limited sensor nodes, resulting in energy waste and degraded network performance [9]. In the security context, traditional encryption methods cannot be directly introduced because they add much overhead and exacerbate the energy consumption problem. In the current research scenario, the need for more adaptive, resilient wireless sensor networks has led to the development of new solutions. In this regard, there is growing interest in adopting artificial intelligence (AI) based approaches to improve the performance of wireless sensor networks, such as energy efficiency, packet routing, and security [10].

However, there are also a few similar studies in recent literature to achieve efficiency and sufficient safety properties. Ahmed *et al.* [11] emphasize the need for enhanced security and optimization in WSN. The authors have presented a multi-tiered trust evaluation system, distinguishing nodes' trustworthiness at varied levels and aiding in recognizing and isolating potential malicious nodes. This study also integrates a customized ant colony optimization (ACO) technique to optimize routing. Gulganwa and Jain [12] have used a weighted clustering scheme to enhance the data aggregation process in WSN and then implemented a support vector machine (SVM) and multi-layer perceptron (MLP) artificial neural network (ANN) based intrusion detection system (IDS) to resist potential attacks. The experimental outcome shows 90% detection accuracy for intrusion detection, followed by enhanced throughput and reduced delay. Haseeb *et al.* [13] address the challenge of resource limitations and security concerns in IoT-based WSNs for smart agriculture. It involves a multi-criteria decision function-based clustering scheme, and packet transmission security is ensured using the recurrence of the linear congruential generator. The experimental outcome suggests an average improvement of approximately 13% in throughput and 16% in energy consumption. The study [14] adopted a fuzzy logic method, an application of AI to generate high-quality clusters, utilizing a criterion that improves inter-cluster and intra-cluster distances while reducing clustering errors. The presented scheme utilizes various criteria, including residual energy and distance metrics. The method exhibits high reliability, low error rate, independence of key cluster heads (CHs), scalability, and strong performance in large-scale networks. Niu *et al.* [15] suggest a blockchain security system to counter the often reported assault, such as a targeted attack on plaintext that results in the disclosure of the secret key. In Mangia *et al.* [16], [17] blockchain has been utilized to secure the data obtained by compressed sensing in IoT and is designed to defend against man-in-the-middle attacks. An approach of lightweight authentication for low-cost sensor devices is introduced by Khan *et al.* [18] using a session key establishment procedure. According to Al-Asli *et al.* [19], symmetric encryption keys significantly increase device security. Re-encryption enables resistance to various threats over multiple equipment connected in an IoT. Also, there is an increasing demand to utilize certificateless techniques. However, multi-party usage is not always done with a certificate. Zhang *et al.* [20] presented an extended security mechanism used to strengthen the authentication procedure utilizing a certificateless technique. This verification, however, only happens once and might be less reliable if exposed to a dynamic assault environment. The existing research method by Zhao *et al.* [21] used identity-based encryption combined with a physically unclonable function. This method performs encryption twice over the IoT environment using quadratic form residues. Al-Naeem [22] attempted to predict the re-occurrences of spoofed acknowledgement packets sent to deflate a target network node by a distributed denial-of-service (DDoS) attack. The prediction of DDoS attacks is done based on the variability analysis of the transmission pattern. Liu and Li [23] applied a mechanism of diffusion least-mean squares to determine a threshold as a reliable reference point to detect the trust neighbors of each node. The strategy for node identification based on time synchronization and link information is presented by Huan *et al.* [24]. This study has also utilized a neural network to enable centralized and distributed node identification for single and multi-hop communication scenarios. Nurellari *et al.* [25] investigated the behavior of the compromised nodes towards the data fusion process. The authors applied the fusion rule to mitigate attacks in WSN. Dautov and Tsouri [26] demonstrated that negative correlation can be exploited and poses a significant threat to sensors that use core extraction techniques that rely on the physical layer and channel-state information.

Hence it can be seen that numerous studies have explored the joint problem of energy efficiency and robust security in WSNs. However, achieving a satisfactory balance between these two factors remains an active area of ongoing research. In WSNs, the efficient selection of CHs is particularly challenging due to energy constraints, dynamic network conditions, and the need to balance multiple objectives such as energy efficiency, network throughput, and reliability. Traditional methods for CH selection, which often dependent on randomized or static algorithms, lead to suboptimal outcomes characterized by uneven energy consumption across nodes [14]. This imbalance accelerates energy depletion in certain nodes, leading to network segmentation and a reduction in the network's lifespan. Alongside, the critical need to enhance security within WSNs against both active and passive threats is highlighted by the vulnerability of these networks to various attacks, compromising data integrity, confidentiality and reliability of the entire network [11], [12]. The significant research gaps that the proposed study aims to address are as follows:

- Existing strategies typically address efficiency and security independently, resulting in compromised network performance and increased vulnerability to attacks [11], [12]. An integrated approach that synergizes energy efficiency with robust security measures to enhance network resilience is found to be absent.
- The lack of security considerations in the CH selection process exposes WSNs to a spectrum of attacks, from node impersonation to sinkhole attacks [15]–[17]. There is an urgent need for a CH selection algorithm that inherently integrates security, selecting CHs for their energy efficiency, connectivity, and their robustness against security threats.
- While fuzzy logic has been harnessed for CH selection, its application has been limited, focusing predominantly on factors like residual energy and proximity to the base station [14]. The proposed study extends the application of fuzzy logic in CH selection, incorporating a wider array of factors, including node centrality, connectivity, and security metrics, for a more effective selection process.
- The challenge of deploying computationally intensive encryption methods in resource-constrained WSN environments is well-reported in literature [18]–[20]. There exists a critical need for robust and lightweight encryption algorithms that do not compromise on security while being efficient enough for WSN applications.

The proposed solution is designed to operate within the unique constraints of WSN environments, focusing primarily on the CH and base station (BS) levels to optimize resource usage. By leveraging enhanced fuzzy logic for CH selection and introducing a lightweight, hybrid encryption model combining modified advanced encryption standard (AES) and Rivest-Shamir-Adleman (RSA), the proposed methodology is custom-made to address the identified gaps [21], [22]. This method ensures resource-conscious security and efficiency improvements, responding directly to the challenges outlined by Ahmed *et al.* [11], and the optimization needs identified in studies by Haseeb *et al.* [13] and Niu *et al.* [15]. The contribution of this paper revolves around addressing these gaps, aiming to advance the state-of-the-art in WSN design for enhanced efficiency, security, and overall network resilience. The proposed study introduces a comprehensive methodology for enhancing the security and efficiency of WSNs through a novel integration of fuzzy logic-based CH selection and lightweight public key encryption for secure data transmission phase. By addressing the challenges posed by the unpredictable nature of WSNs, the proposed work in this paper has the potential to create an adaptive and reliable environment for secure communication with a longer network lifespan. The significant contributions of this research work highlighted as follows:

- The study introduces a multi-phase CH selection process that uniquely combines local and global qualifiers with a trust index, employing fuzzy logic to assess the suitability of nodes for the CH role. This ensures that selected CHs are not only operationally capable but also strategically positioned and reliable.
- The study incorporates a concept resource sharing scheme where the BS maintains and shares a super matrix with comprehensive network data among all nodes. This ensures informed decision-making across the network, enhancing the transparency and efficiency of the CH selection process.
- The study introduces a dynamic approach to managing CHs, where CHs nearing energy depletion are proactively replaced. This strategy not only conserves energy but also maintains optimal network operation without the need for cluster redesign, contributing to the sustainability and longevity of WSNs.
- The study proposes a lightweight public key encryption mechanism specifically designed for WSNs, balancing the need for robust data security with the imperative of minimal computational overhead. This ensures secure data transmission across the network while preserving node energy resources.

Hence, the proposed study offers a comprehensive framework for addressing vulnerabilities, resource limitations, and operational inefficiencies in WSNs. By tackling these challenges, it also provides a scope for a more resilient IoT ecosystem. This framework represents a significant approach in ensuring adequate balance between higher energy savings and security robustness for WSNs in dynamic and resource-constrained environments.

2. METHOD

The study adopts analytical research methodology in the design of the proposed system to ensure higher energy-efficiency and secure data transmission in WSN. The entire modelling of the proposed system is carried out in three phases viz. i) network modelling, ii) two-phase clustering and iii) lightweight hybrid encryption mechanism.

2.1. Network model

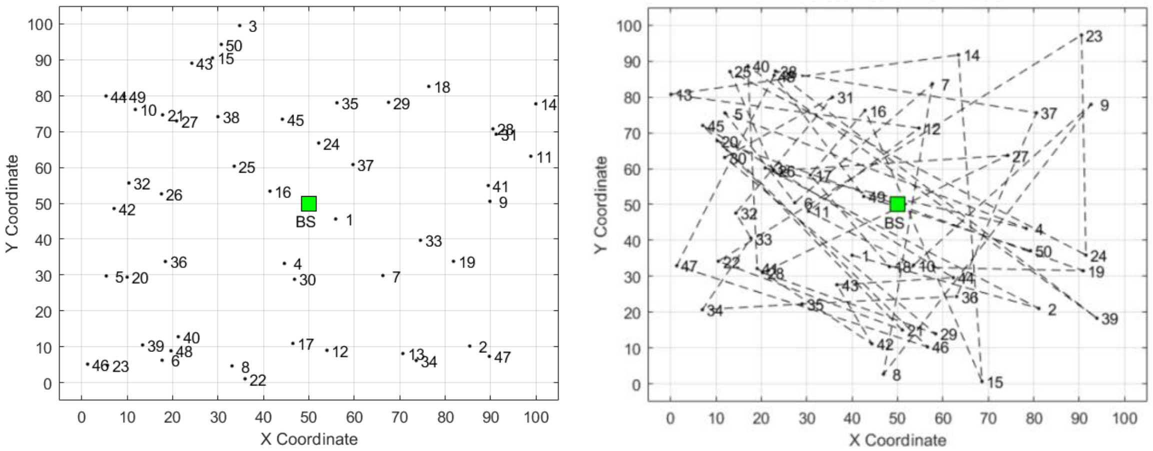
The proposed network modelling simulates WSN considering scenario of practical IoT application, where sensors nodes are often deployed randomly and in uniformly distributed manner. Once the sensor nodes are deployed, they need to establish adjacency with each other. This means that each sensor node needs to identify its neighboring nodes. The node deployment process considers$N$ sensor nodes distributed randomly within a simulation area$A$, following a uniform distribution pattern. The position of each node i, determined by its coordinates (x_i, y_i), where $\mathrm{x_i} \sim \mathrm{U}(0, \mathrm{A_x})$ and $\mathrm{y_i} \sim \mathrm{U}\big(0, \mathrm{A_y}\big)$, indicating ndicating a uniform distribution between 0 and the maximum dimensions $\mathrm{A_x}$ and $\mathrm{A_y}$ of the deployment area. The placement of the BS is strategically placed using predefined coordinates (BS_x, BS_y), as the local data access point for data gathering and communication.

The next step in the network modelling is subjected to node adjacency establishment process where each node n_i has a defined transmission range TR_{n_i}. A node n_j is considered adjacent to n_i if the Euclidean distance $d(n_i, n_j)$ between them is less than or equal to TR_{n_i}. Mathematically, adjacency is defined as $\mathrm{n_j} \in \mathrm{A_{n_i}} \Leftrightarrow \mathrm{d(n_i, n_j)} \leq \mathrm{TR_{n_i}}$, where A_{n_i} denotes the set of nodes adjacent to n_i. Afterwards, sensor nodes periodically broadcast Hello messages to announce their presence to adjacent nodes within their transmission range. Upon receiving these messages, nodes update their adjacency lists, thereby establishing communication links.

However, the open nature of the shared medium of WSN always possesses a potential risk of data collisions, especially when multiple nodes trying to communicate simultaneously. Therefore, to mitigate this, the study uses the carrier sense multiple access (CSMA) technique in which nodes sense the medium before transmitting. If the medium is busy (i.e., another node is transmitting), the node will wait and attempt transmission later. Mathematically, this can be given as (1):

$$T(n_i) = \begin{cases} 1 \; if medium \; is \; free \\ 0 \; if medium \; is \; busy \end{cases} \tag{1}$$

where, $T(n_i)$ denotes the transmission status of node n_i and if $T(n_i) = 1$, this means that the node n_i will transmit the message, otherwise, it will wait. The schematic illustration of the network modeling is shown in Figure 1, where Figure 1(a) node deployment and Figure 1(b) connectivity among nodes based on adjacency establishment.



(a)

(b)

Figure 1. Illustrates simulation of network set-up for (a) node deployment and (b) connectivity

2.2. Multi-phase clustering scheme

The proposed study introduces a multi-phase clustering scheme designed to optimize the selection of CHs in WSNs. The proposed scheme utilizing a fuzzy logic algorithm that evaluates sensor nodes to become CHs based on a combination of local and global qualifiers, alongside trust indices, aiming to select

CHs that are energy-efficient, strategically positioned, and reliable. The methodology operates under the following design considerations:

- The study considers a non-compromised state of nodes at deployment and assumes the BS as a trusted, resource-rich entity responsible for maintaining records of node data and security key management.
- Nodes and the BS are synchronized in terms of time and communication cycles.
- The BS maintains a comprehensive super matrix M that records detailed information about each node, including local qualifiers (remaining energy and adjacent nodes) and global qualifiers (node centrality, node proximity, and distance between CHs), alongside a trust index.
- Nodes communicate their status periodically to the BS, which updates the super matrix M, which plays a crucial role for informed decision-making regarding CH selection and network management.
- The BS calculates the trust index for the initial CH candidates, focusing on remaining energy and communication frequency to identify potential security risks. Weights for these qualifiers are assigned based on their relevance to distinguishing between normal and attacker nodes.

2.2.1. Initial CH pool formation

This phase initiates the process of selecting CH within WSN, utilizing fuzzy logic to assess the suitability of each node to serve as a CH based on local qualifiers. This assessment results in the formation of an initial pool of CH candidates ensuring that only nodes with adequate energy levels and connectivity are chosen as CH, which is crucial for efficient data aggregation and transmission. The study considers local qualifiers LQ such as remaining energy E_i and the number of adjacent nodes A_i into the fuzzy logic assessment using the function $f(\cdot)$ given as (2):

$$CH_{initial} \leftarrow LQ(n_i) = f(E_i, A_i) \tag{2}$$

where, $CH_{initial}$ represents the initial pool of CH candidates derived from this assessment and the function $f(\cdot)$ applies a fuzzy logic algorithm for evaluating the nodes. Higher scores on these local qualifiers increase a node's likelihood of being selected as a CH. The fuzzy logic evaluation assigns decision scores to nodes based on their performance against the established criteria, ranging from "significant" for nodes with outstanding energy reserves and connectivity to "dominant" and "moderately large", reflecting varying degrees of suitability. The decision matrix, populated with these scores alongside corresponding control rules such as low, medium, and high, facilitates a structured selection of initial CH candidates.

2.2.2. Optimal CH selection

This phase of the clustering operation focuses on identifying additional potential cluster heads (CHs) from the initial CH Pool established in the previous phase, using global qualifiers. It is important to note that not all nodes are assessed at this stage; rather, only the identified potential CHs undergo further scrutiny through global qualifiers and integration of a trust index. This ensures that the chosen CHs are not only operationally efficient but also strategically aligned and trustworthy.

a) Assessment of global qualifiers: initially selected $CH_{initial}$ qualifying from the initial phase undergo further evaluation using fuzzy logic, incorporating global qualifiers GQ. These qualifiers assess the centrality of the nodes C_i, their proximity to the BS P_i, and the inter-CH distance D_{ij} between potential CHs n_i and n_j. Mathematically, this process is described as (3):

$$CH_{Candidates} \leftarrow GQ(CH_{initial}) = g(C_i, P_i, D_{ij}) \tag{3}$$

This comprehensive assessment ensures the selection of candidate CHs that exhibit superior scores across $GQ \in \{C_i, P_i, D_{ij}\}$ are more likely to be selected as sub-optimal CHs, prioritizing those that demonstrate strategic advantage and network reliability.

b) Trust index: Simultaneously, the BS computes a trust index Ti for each candidate $CH_{Candidates}$ assessing their historical reliability and security profile based on energy consumption patterns and communication frequencies. The trust index is formulated as (4):

$$T_i = w_E \times E_i + w_F \times F_i \tag{4}$$

where T_i is the trust index for each CHs, E_i and F_i represent energy levels and communication frequency, respectively, with w_E, w_F as their associated weights, reflecting the criteria's significance in identifying secure nodes.

c) Composite score computation: The final selection of a CHs is determined by computing composite score CS that integrates the local and global qualifiers with the trust index, weighted by their respective importance α, β, γ, numerically given as (5):

$$CS(CH_{Candidates}) = (\alpha \times LQ(n_i)) + \beta \times GQ(n_i) + (\gamma \times T_i) \quad (5)$$

d) Optimal CH selection: A node $n_i \in CH_{Candidates}$ is selected as a CH if $CS(n_i)$ exceeds a predefined threshold θ, which is optimized through simulations to ensure network robustness and efficiency, given as (6):

$$CH_{optimal} \leftarrow \{n_i | CS(n_i) > \theta\} \quad (6)$$

e) Declaration and network update: The BS announces the optimal CHs to the network. These CHs assume their roles in coordinating data aggregation from their clusters and managing data transmission to the BS.

f) CH replacement: The BS also monitors the energy levels of active CHs and initiates the selection of new CHs when current ones deplete a significant portion of their energy, optimizing network longevity and efficiency. In this regard, CHs transition back to regular nodes upon depleting 70% of their energy, at which point the BS initiates a selection process for new CHs within the same cluster, thereby conserving energy and maintaining optimal network operation.

It is important to understand the role of nodes, and BS in the clustering phase. Initially, sensor nodes evaluate their potential as CHs based on energy and connectivity, ensuring a fair chance for all to contribute to network efficiency. The BS serve as centralized entity which maintains a super matrix that holds detailed information on both local and global qualifiers alongside trust indices for all nodes. The fuzzy logic is applied centrally at the BS, which uses this super matrix enables the BS to conduct thorough evaluations of CH candidates, combining objective metrics with trust indices to identify the most fitting nodes for the CH role. The centralized approach benefits from having a complete view of the network, allowing for more informed and strategic CH selection decisions. Moreover, the system adopts a resource-sharing mechanism, modernizing data processing and enhancing energy conservation across the network. This scheme centralizes the storage and processing of critical information at the BS, thereby reducing the operational burden on individual nodes. When nodes need specific information for decision-making or operational tasks, they request it from the BS, ensuring on-demand access to up-to-date and comprehensive data. This strategy significantly lowers the energy and computational demands on individual nodes, allowing them to concentrate on their primary sensing and communication tasks.

2.3. Proposed hybrid lightweight encryption

The study proposes a hybrid, yet lightweight encryption scheme designed for resource-constrained environments to protect sensory data from unauthorized access, ensuring confidentiality and integrity. The proposed study considers two popular encryption techniques, AES known for its encryption efficiency and RSA, recognized for secure key exchanges and presents customization in their design to address their high computational demands. This study further hybridizes the proposed customized RSA (c-RSA) and AES (c-AES) to facilitate secure key exchanges and data encryption efficiently, thus maintaining the algorithms' security strengths while significantly reducing their energy and computational overhead.

2.3.1. Implementation design of customized AES

The proposed customized AES (c-AES) simplifies the original AES by omitting the computationally intensive MixColumns step and introducing a permutation step. This modification maintains AES's cryptographic efficacy, ensuring data security while substantially reducing energy and computational demands. c-AES remains compatible with AES's 128-bit block and key sizes, optimizing encryption workflow without compromising security standards. Algorithm 1 outlines the implementation of c-AES, utilizing a plaintext block P of 128 bits and an encryption key K of 128 bits to produce a ciphertext block C of 128 bits. The introduction of a permutation step facilitates efficient data diffusion and cipher security, eliminating the complexity of MixColumns. The initial combination of plaintext with the first-round key (RK_0) through XOR operation, SubBytes, and ShiftRows steps are retained from the original AES. The permutation step applies a predefined matrix Mp to the state, rearranging the bytes in a manner that contributes to the security of the cipher without the need for the complex polynomial operations of MixColumns. This step is carefully designed to balance security with computational efficiency.

The final round of c-AES mirrors that of the original AES, focusing on SubBytes, ShiftRows, and the final AddRoundKey step. The simplification in c-AES primarily affects the intermediate rounds, with the final round ensuring that the encryption process concludes with a strong diffusion of the plaintext and key material. This customization makes c-AES particularly suited for applications where the security of data transmission must not compromise the operational longevity and efficiency of the network.

Algorithm 1. Design and Implementation of c-AES

```
Input: Plaintext block $P$ of 128 bits, Encryption key K of 128 bits
Output: Ciphertext block $C$ of 128 bits.
Start
 1. Generate $N_r + 1$ round keys $RK_i$ fromencryption key $K$, where $N_r$=10 for a 128-bit key. Use
    the AES key schedule, incorporating Rijndael's S-box for byte substitution and the
    round constant $Rcon[i]$ for each round$i$, where $i = 0, \cdots N_r$.
 2. Combine the plaintext block $P$ with the first-round key $RK_0$ using the XOR operation:
    $State\ =\ P\ \oplus RK_0$
 3. For round $i = 1$ to $N_r - 1$
 4. SubBytes: For each byte $b_{xy}$ in State, replace it with $S(b_{xy})$
    $State_{xy} = S(b_{xy})$, where $S$ is defined by AES S-box.
 5. ShiftRows: Perform cyclic left shift on row $r$ by r positions
    $State_{r,c} =\ State_{r,(c+r)\ mod\ 4}, r = 0, \cdots, 3$.
 6. Permutation Step: Apply a permutation $P_f$ on $State$.
    Let $P_f$ be represented by a permutation matrix $M_p$such that:
    $State' = M_p \times State$, where $State'$ is the permuted state
 7. AddRoundKey: XOR the state with the round key $RK_i$:$State = Stat \oplus RK_i$
 8. Final Round ($i$ = $N_r$):
 9.    Execute the SubBytes and ShiftRows steps as described above.
 10.   Perform the Final AddRoundKey step by XORing the state with the last round key $RK_{Nr}$
 11. $State = Stat \oplus RK_{Nr}$
 12. End
 13. The state after the final round is the ciphertext (C):$C = State$
End
```

2.3.2. Customized RSA

The security of RSA is fundamentally based on the computational difficulty of factoring large integers. The RSA customization proposes adopts tri-prime approach that include an additional prime number $s_n$in the key generation process, where each prime is smaller in size compared to the two larger primes used in traditional RSA. For example, instead of two 1,024-bit primes, three 684-bit primes can be used, since 3×684 ≈ 2048. This customization aims to enhance the speed of key generation, decryption and increase the difficulty of analyzing the modulus. The implementation procedure of proposed customized RSA (c-RSA) is described in Algorithm 2. The inclusion of a third prime number increases the complexity of factorization, providing an additional layer of security. Through Chinese remainder theorem (CRT), decryption operations become more efficient, a substantial advantage for devices with limited computational resources.

Algorithm 2. Design and implementation of c-RSA

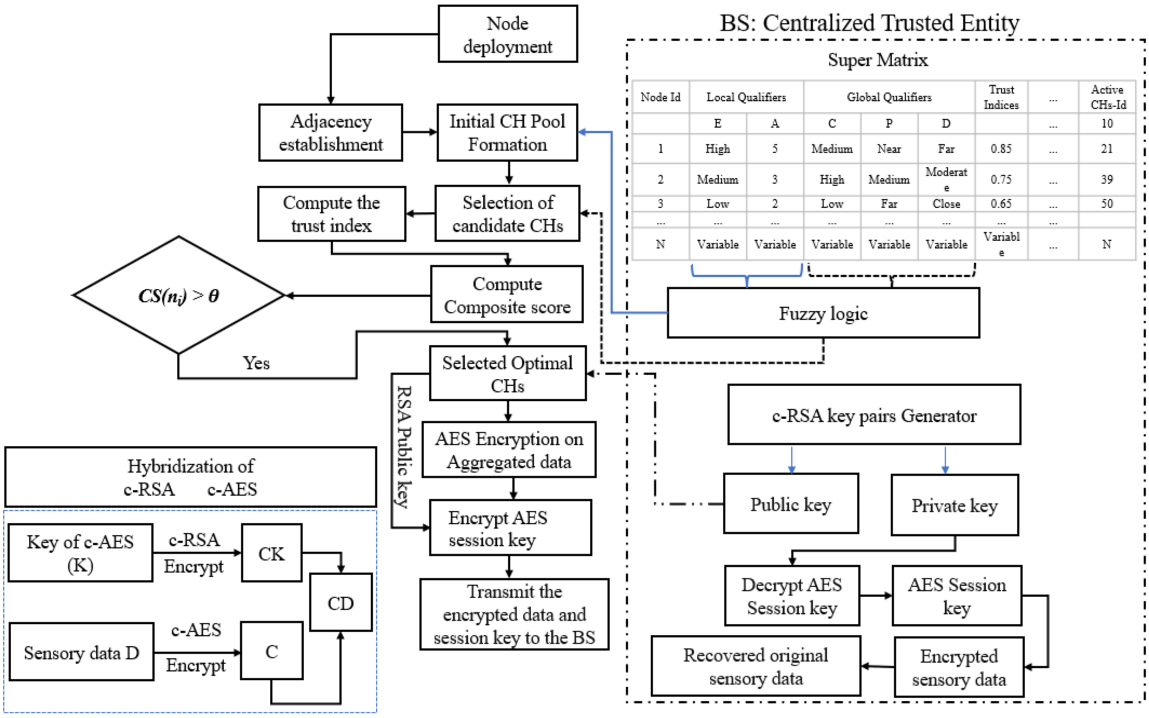
```
 1. Key Generation
    Select three large primes $p$, $q$, and $r$, significantly increasing the difficulty of
    factorization.
       Compute $N = p \times q \times r$, which remain the modulus for both keys
       Compute the modified totient function $\varphi(N) = (p-1) \times (q-1) \times (r-1)$
       An encryption exponent $e$ is chosen such that $11 < e < \varphi(N)$ and $\gcd(e, \varphi(N)) = 1$
       The decryption exponent $d$ is determined where $e \times d \equiv 1 \bmod \varphi(N)$
       The public key remains $(e, N)$, while the private key become more complex, incorporating
    CRT optimizations for efficiency.
 2. Encryption:
    Similar to traditional RSA, with $C = M^e \bmod N$, taking advantage of increased modulus
    size for security.
 3. Decryption:
    Utilize CRT with the three primes to facilitate efficient decryption, reducing the
    computational burden: Compute

       $M_P = C^{dmod(p-1)} modp$
       $M_q = C^{dmod\ (q-1)} modq$
       $M_r = C^{dmod\ (r-1)} modr$

Reconstruct M from $M_P$, $M_q$ and $M_r$ using the CRT
```

2.3.2. Secure data transmission

In order to secure transmission of data packet, the study performs hybridization of the proposed-RSA and c-AES encryption, where c-AES encryption is designed to encrypt the data using session key and c-RSA is used to encrypt the c-AES session key. This encryption mechanism is deployed at CHs to encrypted data and encrypt secret key then both are transmitted to the BS. The BS then decrypt the session key using their c-RSA private key and then decrypt the data using the retrieved c-AES session key. The implementation of hybrid yet lightweight encryption for secure data transmission is described as follows:

a) Key generation and secure distribution: The process initiates with the generation of c-RSA key pairs for each CH ensuring each has a public key for encrypting messages and a private key for decrypting them. The BS generates cryptographic keys using the c-RSA for each CH.
b) Key distribution: The BS sends the c-RSA public keys to the CHs in secure manner immediate after CHs are selected. This ensures that each CH has a unique public key for encrypting data intended for the BS, and the BS has the corresponding private keys to decrypt the data received from the CHs.
c) Data aggregation and encryption: Sensor nodes transmit their collected data to their respective CHs without encryption, relying on the secure selection process of CHs based on fuzzy logic and trust indices to ensure data integrity up to this point. The CH aggregates data from its sensor nodes. It then encrypts this aggregated data using the c-AES to generate a session key unique for this particular data packet, ensuring confidentiality. A unique session key, generated specifically for this encryption, guarantees the confidentiality of the data.
d) Session key security: The session key itself is then encrypted with the c-RSA public key of the next intended recipient, which could be another CH if multi-path routing or the BS if direct communication. This layered encryption approach ensures that the session key can be securely transmitted along with the encrypted data.
e) Packet forwarding: The encrypted packet, now containing both the c-AES encrypted data and the c-RSA encrypted session key, is forwarded towards the BS. This forwarding process is designed to be efficient, ensuring timely and secure delivery of data to the BS. The study implements shortest-path finding routing algorithm.
f) Final decryption at the BS: The ultimate decryption occurs at the BS, the network's trusted authority with the computational capability to efficiently decrypt incoming packets. The BS uses its private c-RSA key to decrypt the session key and then applies this session key to decrypt the c-AES encrypted data, successfully retrieving the original data packet.

The proposed encryption scheme leverages the strengths of both c-RSA for secure key exchange and c-AES for efficient data encryption. This balanced approach addresses the security needs of WSNs without imposing higher computational costs. Additionally, Figure 2 illustrates the flowchart of the entire methodology, providing a visual interpretation of the optimal CH selection and secure data transmission.



Node Id	Local Qualifiers		Global Qualifiers			Trust Indices	...	Active CHs-Id
	E	A	C	P	D		...	10
1	High	5	Medium	Near	Far	0.85	...	21
2	Medium	3	High	Medium	Moderate	0.75	...	39
3	Low	2	Low	Far	Close	0.65	...	50
...	...	...	...	...	...	...	...	
N	Variable	Variable	Variable	Variable	Variable	Variable	...	N

Figure 2. Illustrates high-level flow diagram of the proposed methodology

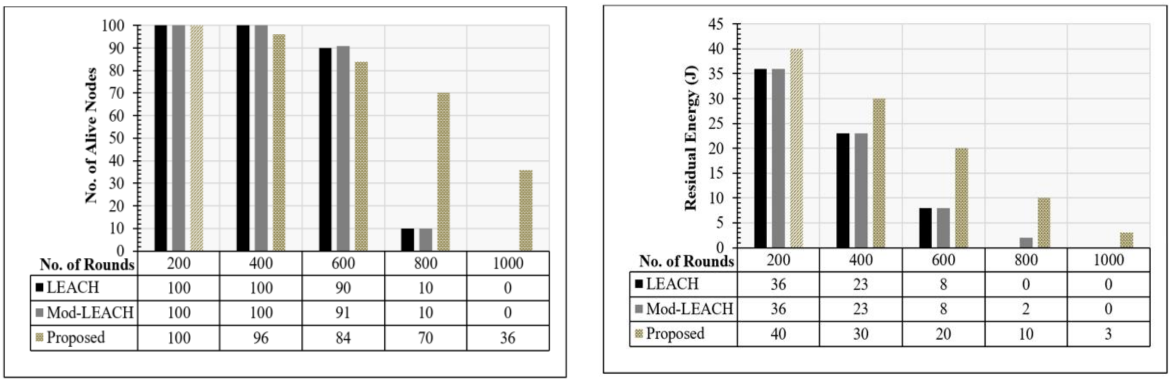
3. RESULTS AND DISCUSSION

This section discusses the outcome and performance analysis of the proposed system. The development and design of the proposed system are carried out on a numerical computing tool (MATLAB). The scope and effectiveness of the proposed system are justified based on the comparative analysis with the existing technique, namely the LEACH and modLEACH modified version of original LEACH. The overall analysis is carried out in two different comparative assessments viz: i) analysis under active attack and ii) analysis under active attack. Table 1 shows the simulation parameters used in the proposed system implementation.

The performance analysis shown in Figure 3 is carried out regarding assessing energy-efficiency of the proposed scheme. Figure 3(a) shows analysis for remaining alive nodes the trend that the proposed outperforms the other techniques. A performance graph shows that for the proposed system all nodes died at 1,100th communication round, whereas in the case of the LEACH all nodes were dead at 820th round. Similar performance can be also seen for the ModLEACH in which all nodes died at 840th round. The closer analysis reveals that the proposed system offers approximately double the lifetime than LEACH, and ModLEACH. This analysis also reveals that the proposed scheme ensures stability in the network from the time period of the death of the first node to the remaining alive nodes. While Figure 3(b) presents analysis regarding remaining energy of nodes over progressive communication rounds that includes cost measures associated with security function and data transmission. The graph trend exhibits a linear trend of energy consumption by proposed and existing technique. However, a better performance trend is shown by the proposed scheme where nodes hold energy for long run compared to the existing techniques. The proposed technique shows an average value of 13.4 joules of remaining energy over 1,200 communication rounds, whereas the existing LEACH technique shows an average value of 2.6 joules of remaining energy, while 3.3 joules of average residual energy over 1,100 communication rounds for Mod_Leach.

Table 1. Simulation parameters

Parameters	Values
Wireless sensor nodes	300
Simulation area	100 m^2
Deployment strategy	Random
Initial energy (i_e)	50 Joule
Transmission energy	50 nj/bit
Receptance energy	50 nj/bit
Data aggregation energy	50 nj/bit/signal
Simulation round	2,500
Packet size	4k bit
Control packet size	16 bit
Cluster percentage	20%
Attack percentage	5%



No. of Rounds	200	400	600	800	1000
■ LEACH	100	100	90	10	0
■ Mod-LEACH	100	100	91	10	0
▨ Proposed	100	96	84	70	36

(a)

No. of Rounds	200	400	600	800	1000
■ LEACH	36	23	8	0	0
■ Mod-LEACH	36	23	8	2	0
▨ Proposed	40	30	20	10	3

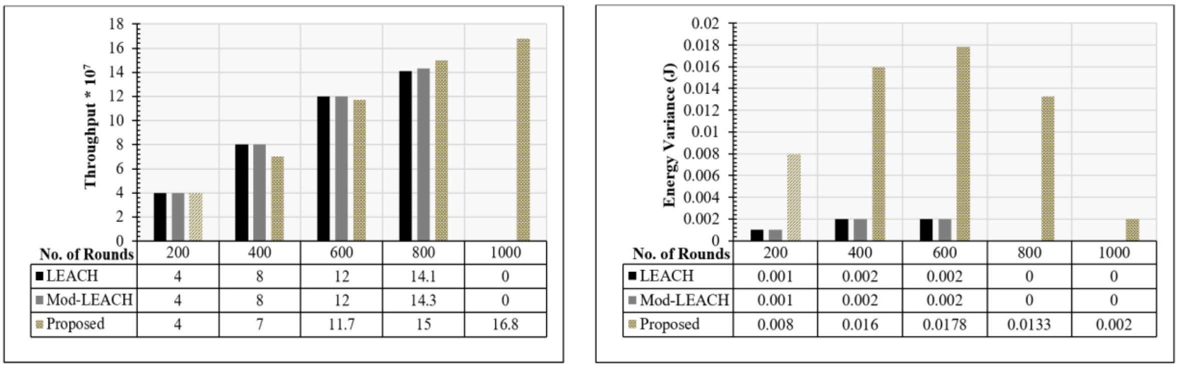
(b)

Figure 3. Analysis of system with respect energy efficiency with sub-figure (a) evaluates remaining alive nodes and sub-figure and (b) evaluates remaining energy

The study also performs analysis of the proposed scheme concerning network performance as shown in Figure 4. The performance analysis regarding throughput is shown in Figure 4(a) which demonstrates better throughput trend exhibited by the proposed technique compared to others. The average through of the proposed technique is 2.14, whereas LEACH and Mod_Leach achieved 0.41 and 0.66, respectively. The analysis shows the proposed system offers better transmission performance thereby delivering higher data packets to the base station. Figure 4(b) shows analysis of the proposed system performance regarding variance in energy usage of nodes evaluated based on simulation analysis with 100 sensor nodes and 1,200 communication rounds. The graph trend illustrates that the energy variance at the initial communication round was zero, which signifies that the energy distribution at the beginning of the communication is uniform.

It can be seen that over the progressive communication round for the communication or data transmission, the graph curves indicating the proposed technique always remain under the curves compared to the existing technique. In addition, the proposed technique's energy usage pattern was reduced to the lower zero towards communication rounds 1,100. Therefore, the performance indicates that the proposed technique maintains an effective load balancing in the network.

Figure 5 presents a comprehensive analysis of the encryption and decryption times for the proposed c-AES) and c-RSA) algorithms. In Figure 5(a) the performance of proposed c-AES in comparison with the original AES (o-AES) is assessed for time taken for encryption operations against varying file sizes, ranging from 10 bytes to 8 kilobytes. The c-AES demonstrates a consistently lower encryption time across all file sizes when compared to standard AES, indicating a significant improvement in efficiency. This suggests that c-AES is particularly effective for larger data sizes, a critical advantage in WSNs where the computational overhead must be minimized. In Figure 5(b) the performance of the proposed c-RSA algorithm is compared against original RSA (o-RSA) across various key sizes from 170 to 684 bits. It is evident that c-RSA encryption times are consistently lower than those of o-RSA, highlighting the effectiveness of the tri-prime factorization and CRT optimizations used in c-RSA. The decryption time, a critical operation in the context of WSNs, also shows a significant improvement for c-RSA over o-RSA.

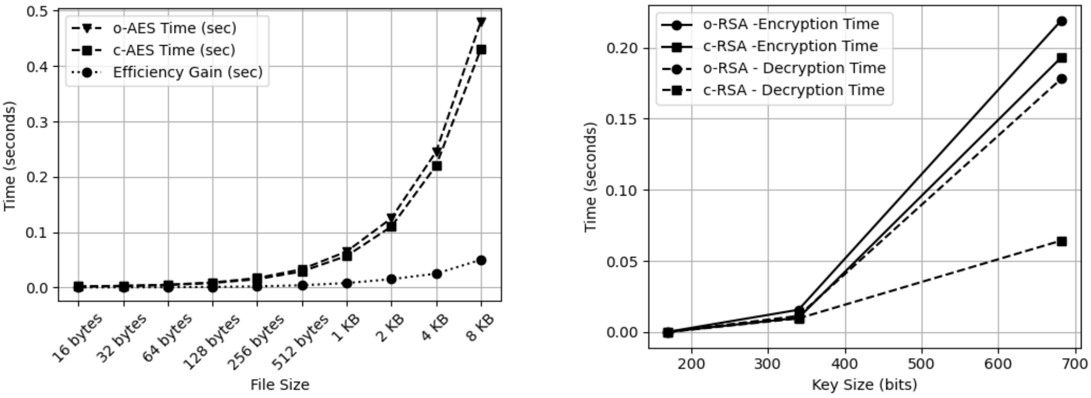


No. of Rounds	200	400	600	800	1000
■ LEACH	4	8	12	14.1	0
■ Mod-LEACH	4	8	12	14.3	0
▨ Proposed	4	7	11.7	15	16.8

No. of Rounds	200	400	600	800	1000
■ LEACH	0.001	0.002	0.002	0	0
■ Mod-LEACH	0.001	0.002	0.002	0	0
▨ Proposed	0.008	0.016	0.0178	0.0133	0.002

(a) (b)

Figure 4 Analysis of system with respect to network performance where sub-figure (a) assesses throughput and sub-figure (b) assess energy variance



(a) (b)

Figure 5 Analysis of proposed lightweight encryption in terms of encryption and decryption time where sub-figure (a) shows analysis for proposed c-AES and sub-figure (b) shows analysis for proposed c-RSA

4. CONCLUSION

This paper has introduced a comprehensive strategy aimed at enhancing energy efficiency and ensuring adequate data security in WSNs against various active attacks, including but not limited to spoofing, Sybil, selective forwarding, and replay attacks. The major contribution is the integration of an advanced CH selection mechanism integrated with a hybrid and lightweight encryption techniques. The proposed CH selection algorithm accurately evaluates both local and global parameters to identify CHs that are not only energy-efficient but also superior in connectivity and strategic positioning within the network. The second major contribution of this paper is the introduction of customization in original AES and RSA encryption algorithm taking benefits of symmetric and asymmetric cryptographic methods. This defensive layer is specifically engineered to be computationally light within the resource constraints inherent to WSN environments. The study outcomes demonstrate effectiveness of the proposed system over well-known protocols such as LEACH and ModLEACH. The proposed system distinguishes itself through several advantageous features its dynamic and adaptive nature, comprehensive consideration of multifaceted factors for CH selection, and robustness in handling network variability and potential threats. In future, the scope of the proposed system will be extended towards implementing an effective intrusion detection system using optimized deep learning models.

REFERENCES

[1] K. Gulati, R. S. Kumar Boddu, D. Kapila, S. L. Bangare, N. Chandnani, and G. Saravanan, “A review paper on wireless sensor network techniques in internet of things (IoT),” *Materials Today: Proceedings*, vol. 51, pp. 161–165, 2022, doi: 10.1016/j.matpr.2021.05.067.

[2] P. K. Singh and A. Sharma, “An intelligent WSN-UAV-based IoT framework for precision agriculture application,” *Computers and Electrical Engineering*, vol. 100, May 2022, doi: 10.1016/j.compeleceng.2022.107912.

[3] A. Shahraki, A. Taherkordi, O. Haugen, and F. Eliassen, “A survey and future directions on clustering: from WSNs to IoT and modern networking paradigms,” *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 2242–2274, Jun. 2021, doi: 10.1109/TNSM.2020.3035315.

[4] L. Kaur and R. Kaur, “A survey on energy efficient routing techniques in WSNs focusing IoT applications and enhancing fog computing paradigm,” *Global Transitions Proceedings*, vol. 2, no. 2, pp. 520–529, Nov. 2021, doi: 10.1016/j.gltp.2021.08.001.

[5] D. S. Ibrahim, A. F. Mahdi, and Q. M. Yas, “Challenges and issues for wireless sensor networks: a survey,” *Journal of Global Scientific Research*, vol. 6, no. 2, pp. 1079–10927, 2021.

[6] M. Keerthika and D. Shanmugapriya, “Wireless sensor networks: active and passive attacks-vulnerabilities and countermeasures,” *Global Transitions Proceedings*, vol. 2, no. 2, pp. 362–367, Nov. 2021, doi: 10.1016/j.gltp.2021.08.045.

[7] V. Sharma and D. P. Bhatt, “A review on recent trends in secure and energy efficient routing approaches in wireless sensor networks,” *IOP Conference Series: Materials Science and Engineering*, vol. 1099, no. 1, Mar. 2021, doi: 10.1088/1757-899X/1099/1/012044.

[8] A. Kuthe and A. K. Sharma, “Review paper on design and optimization of energy efficient wireless sensor network model for complex networks,” in *2021 5th International Conference on Information Systems and Computer Networks (ISCON)*, Oct. 2021, pp. 1–3, doi: 10.1109/ISCON52037.2021.9702421.

[9] W. Osamy, A. M. Khedr, A. Salim, A. I. AlAli, and A. A. El-Sawy, “Recent studies utilizing artificial intelligence techniques for solving data collection, aggregation and dissemination challenges in wireless sensor networks: a review,” *Electronics*, vol. 11, no. 3, Jan. 2022, doi: 10.3390/electronics11030313.

[10] A. Dwivedi, A. Sharma, and P. Mehra, “Energy-aware routing protocols for wireless sensor network based on fuzzy logic: A 10-years analytical review,” *EAI Endorsed Transactions on Energy Web*, Jul. 2018, doi: 10.4108/eai.6-10-2020.166548.

[11] A. J. Ahmed, A. H. Abbas, and S. AbdulJabbar Rashid, “Multi level trust calculation with improved ant colony optimization for improving quality of service in wireless sensor network,” *IAES International Journal of Artificial Intelligence (IJ-AI)*, vol. 12, no. 3, Sep. 2023, doi: 10.11591/ijai.v12.i3.pp1224-1237.

[12] P. Gulganwa and S. Jain, “EES-WCA: energy efficient and secure weighted clustering for WSN using machine learning approach,” *International Journal of Information Technology*, vol. 14, no. 1, pp. 135–144, Feb. 2022, doi: 10.1007/s41870-021-00744-5.

[13] K. Haseeb, I. Ud Din, A. Almogren, and N. Islam, “An energy efficient and secure IoT-based WSN framework: an application to smart agriculture,” *Sensors*, vol. 20, no. 7, Apr. 2020, doi: 10.3390/s20072081.

[14] A. A. Baradaran and K. Navi, “HQCA-WSN: high-quality clustering algorithm and optimal cluster head selection using fuzzy logic in wireless sensor networks,” *Fuzzy Sets and Systems*, vol. 389, pp. 114–144, Jun. 2020, doi: 10.1016/j.fss.2019.11.015.

[15] Y. Niu, J. Zhang, A. Wang, and C. Chen, “An efficient collision power attack on AES encryption in edge computing,” *IEEE Access*, vol. 7, pp. 18734–18748, 2019, doi: 10.1109/ACCESS.2019.2896256.

[16] M. Mangia, F. Pareschi, R. Rovatti, and G. Setti, “Low-cost security of IoT sensor nodes with rakeness-based compressed sensing: Statistical and known-plaintext attacks,” *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 2, pp. 327–340, Feb. 2018, doi: 10.1109/TIFS.2017.2749982.

[17] M. Mangia, A. Marchioni, F. Pareschi, R. Rovatti, and G. Setti, “Chained compressed sensing: a blockchain-inspired approach for low-cost security in IoT sensing,” *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6465–6475, Aug. 2019, doi: 10.1109/JIOT.2019.2910402.

[18] S. Khan, A. I. Alzahrani, O. Alfarraj, N. Alalwan, and A. H. Al-Bayatti, “Resource efficient authentication and session key establishment procedure for low-resource IoT devices,” *IEEE Access*, vol. 7, pp. 170615–170628, 2019, doi: 10.1109/ACCESS.2019.2955604.

[19] M. Al-Asli, M. E. S. Elrabaa, and M. Abu-Amara, “FPGA-based symmetric re-encryption scheme to secure data processing for cloud-integrated internet of things,” *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 446–457, Feb. 2019, doi: 10.1109/JIOT.2018.2864513.

[20] Y. Zhang, F. Ren, A. Wu, T. Zhang, J. Cao, and D. Zheng, "Certificateless multi-party authenticated encryption for NB-IoT terminals in 5G networks," *IEEE Access*, vol. 7, pp. 114721–114730, 2019, doi: 10.1109/ACCESS.2019.2936123.

[21] B. Zhao, P. Zhao, and P. Fan, "ePUF: a lightweight double identity verification in IoT," *Tsinghua Science and Technology*, vol. 25, no. 5, pp. 625–635, Oct. 2020, doi: 10.26599/TST.2019.9010072.

[22] M. A. Al-Naeem, "Prediction of re-occurrences of spoofed ACK packets sent to deflate a target wireless sensor network node by DDOS," *IEEE Access*, vol. 9, pp. 87070–87078, 2021, doi: 10.1109/ACCESS.2021.3089683.

[23] Y. Liu and C. Li, "Secure distributed estimation over wireless sensor networks under attacks," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 54, no. 4, pp. 1815–1831, Aug. 2018, doi: 10.1109/TAES.2018.2803578.

[24] X. Huan, K. S. Kim, and J. Zhang, "NISA: node identification and spoofing attack detection based on clock features and radio information for wireless sensor networks," *IEEE Transactions on Communications*, vol. 69, no. 7, pp. 4691–4703, Jul. 2021, doi: 10.1109/TCOMM.2021.3071448.

[25] E. Nurellari, D. McLernon, and M. Ghogho, "A secure optimum distributed detection scheme in under-attack wireless sensor networks," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 4, no. 2, pp. 325–337, Jun. 2018, doi: 10.1109/TSIPN.2017.2697724.

[26] R. Dautov and G. R. Tsouri, "Effects of passive negative correlation attack on sensors utilizing physical key extraction in indoor wireless body area networks," *IEEE Sensors Letters*, vol. 3, no. 7, pp. 1–4, Jul. 2019, doi: 10.1109/LSENS.2019.2921004.

BIOGRAPHIES OF AUTHORS

Chaya Puttaswamy received the B.E degree in information science and engineering from Coorg Institute of Engineering, Ponnampet, Karnataka, India, in 2004, and the M.Tech. Degree in software engineering from SJCE, Mysore, Karnataka, India in 2011. She is currently working as assistant professor in Department of Information Science and Engineering, GSSS Institute of Engineering and Technology for Women, Mysore, and Research Scholar at VTU, Belagavi, Karnataka, India. Her research interests include wireless sensor networks and communication networks. She has 16 years of teaching experience and published research articles in international journals, international conferences, and national conferences. She can be contacted at email: chayaneetha@gmail.com.

Nandini Prasad Kanakapura Shivaprasad received the B.E. degree in computer science and engineering from PESIT, in 2001, M.Tech. degree in computer science and engineering from VTU, Belagavi, India, in 2005, and the Ph.D. degree in engineering from UBDT, Kuvempu University in 2014 and Postdoc Fellowship (London) in 2023. Presently, she is the dean of foreign affairs, and HOD ISE at Dayananda Sagar Academy of Technology and Management (DSATM), Bangalore. She received the Best Paper Awards at various conferences and also received the "Bharat Jyothi Award" from India International Friendship Society, New Delhi, in August 2012. She has received appreciation certificates from NPTEL and ARPIT. She was appointed as a CSI editorial board member in 2017, a AICTE expert member for AICTE Expert Committee in 2017 and 2016 for AICTE Expert Committee and is a member of Indian Society for Technical Education (ISTE), Institute for Smart Structures and Systems (ISSS), CSTA, and Cryptology Research Society of India (CRSI). She has served as a reviewer for IEEE, Springer, and Elsevier Conferences and for the Journal of Computational and Theoretical Nanoscience, September 2018, and had obtained various funds from AICTE, India. She can be contacted at email: drnandini.prasad1@gmail.com.