A Secure Data Aggregation for Clustering Routing Protocols in Heterogenous Wireless Sensor Networks

Original Scientific Paper

Basim Abood*
Department of Communication Engineering,
College of Engineering, University of Sumer,
Thi-Qar 64001, Iraq
basim.alkhafaji@uos.edu.iq

Hayder Kareem Amer
Department of Computer Technology Engineering,
College of Technical,
Imam Ja'afar Al-Sadiq University, Thi-Qar 64001, Iraq
hayder.kareem@ijsu.edu.iq

Wael Abd Alaziz
Department of Computer Information Systems,
College of Computer Science & Information Technology,
University of Sumer, Thi-Qar 64001, Iraq
w.abdalaziz@uos.edu.iq

Hussain K. Chaiel
Department of Communication Engineering,
College of Engineering, University of Sumer,
Thi-Qar 64001, Iraq
hussain.chaiel@uos.edu.iq

*Corresponding author

Abstract *– The paper presents a broadly elaborated, secure, and energy-efficient data aggregation scheme of the heterogeneous wireless sensor networks (HWSNs). This is motivated by two consistent shortcomings of existing work: (i) clustering-based routing algorithms like LEACH, SEP, and FSEP are inadequate on balancing the energy usage when there is a disparity in the node capabilities, and (ii) most ECC-based security systems create too much computation overhead to extend network lifetime. To satisfy such gaps, the given framework integrates the Spider Monkey Optimization Routing Protocol (SMORP) with a compact cryptographic implementer including the Improved Elliptic Curve Cryptography (IECC) and El Gamal Digital Signature (ELGDS) scheme. SMORP gives maximum consideration to cluster forming and multi hop forwarding and the IECC-ELGDS module that provides all the above data confidentiality, authentication and data integrity at a lower cost of computation. As compared to the previous strategies, the combination of routing optimization and elliptic-curve-based secure aggregation facilitates energy efficiency and high-security assurance in the resource-constrained nodes. MATLAB models show that the offered framework can boost network life up to 27 percent, residual energy up to 32 percent, and get a 96 percent packet-delivery ratio relative to LEACH, SEP, and FSEP. Moreover, the IECC-ELGDS module will need less time in encryption/decryption by 22-35 percent in comparison with ECC-HE, IEKC and ECDH-RSA. These findings support the idea that the SMORP-IECC-ELGDS is a viable and fast architecture to secure aggregation in the real-life HWSN deployment.*

Keywords: *Wireless sensor networks, Lifetime prolonging, Data aggregation Security, Spider Monkey Optimization, Elliptic Curve, EL Gamal Digital Signature algorithm, cryptography, Routing clustering.*

Received: October 11, 2025; Received in revised form: January 8, 2026; Accepted: January 12, 2026

1. INTRODUCTION

Typically, low cost and easy scale-up characteristics have made Wireless Sensor Networks (WSNs) a base technology in large scale environmental monitoring, automation in industrial settings and Autonomous operation in harsh environments or remote settings that do not require continuous human supervision. New applications require round-the-clock sensing, time-sensitive data streaming and unattended long-term operation, which puts intense limitations on both network lifetime and energy expenditure. The same requirements are further complicated in the heterogeneous WSNs (HWSNs) where there is differences in hardware capacity and battery resources provided by the sensor nodes, communication range, and processing power. These heterogeneous architectures facilitate more differing deployments, as well as result in drawsive mismatched energy depletion, uneven routing loads, and enhance susceptibility to communication issues [1-3]. Alongside energy constraints, security is one of the most often challenged issues in deployments of clustered WSN, as sensor nodes are frequently deployed in hostile physical conditions and they use broadcast wireless networks, similar to those used by eavesdropping, packet manipulation,

identity spoofing, replay attacks and malicious node injection. Providing multi-hop aggregation with confidentiality, authentication and integrity of the data is thus important to mission critical applications, especially where the aggregated data has a direct impact on control or situational awareness [4-6]. Nonetheless, even classical forms of public-key cryptography are computationally infeasible on the lean sensor nodes, and lightweight cryptography (elliptic-curve cryptography) and optimized digital signature designs are made use of to mitigate the impact of computation overheads and offer high levels of security assurance[7-9]. These two issues, energy efficiency and secure data aggregation, have led to more recent studies that focus on integrated solutions, which combine routing and security together, instead of focusing on them as different layers. Existing clustering-based routing schemes such as LEACH, SEP, and FSEP (introduced in [10-12]) provide strong baselines for energy-aware operation but do not incorporate end-to-end security. Similarly, modern lightweight security frameworks such as ECC-HE, IEKC, and ECDH-RSA (examined in [13-15]) respectively, improve confidentiality and authentication but do not address energy balancing or cluster-head (CH) overloading during repeated aggregation cycles. Therefore, there is a clear need for a unified framework that simultaneously ensures secure data aggregation and minimizes routing-related energy consumption across heterogeneous sensing tiers. *To address this need, this paper proposes an integrated SMORP–IECC–ELGDS framework that jointly optimizes energy-aware routing and secure ciphertext aggregation in heterogeneous wireless sensor networks.* The remainder of this paper is organized as follows. Section 2 presents the related works, covering recent advances in energy-efficient routing, lightweight cryptographic mechanisms, and integrated energy–security frameworks in heterogeneous WSNs. Section 3 describes the proposed methodology, including the enhanced SMORP-based clustering and routing process together with the integrated IECC–ELGDS security architecture for secure data aggregation. Section 4 outlines the simulation environment, the network and radio-energy models, and the performance metrics used in the evaluation. Section 5 provides a detailed discussion and analysis of the obtained results and compares the proposed framework with existing routing and security schemes. Finally, Section 6 concludes the paper and highlights prospective directions for future research.

Objectives, Contributions, and Novelty

To bridge this gap, the present work introduces a unified secure-and-energy-efficient architecture that integrates a biologically inspired optimization-based routing protocol with a lightweight hybrid cryptographic mechanism. Specifically, the study proposes a combined Spider Monkey Optimization Routing Protocol (SMORP) and Improved Elliptic Curve Cryptography with ElGamal Digital Signature (IECC–ELGDS) framework that jointly optimizes cluster formation, forwarding decisions, secure ciphertext aggregation, and authenticated delivery. The objectives of this work are threefold:

1. **Design an energy-efficient routing mechanism** capable of maintaining balanced energy consumption across heterogeneous sensor tiers through adaptive CH selection and optimized multi-hop forwarding.
2. **Develop a lightweight, secure aggregation framework** that ensures confidentiality, integrity, and authentication without imposing prohibitive computational overhead on sensor nodes.
3. **Integrate routing and security into a single operational pipeline**, eliminating the traditional separation between network-layer optimization and cryptographic protection.

The novelty of the proposed SMORP–IECC–ELGDS architecture lies in:

- The initial closely coordinated model with energy-conscious routing and hybrid lightweight security strengthening other instead of acting as separate layers.
- An aggregated workflow of ciphertexts, such that CHs are able to aggregate encrypted readings without decryption and this decreases the computational cost and removes any plaintext exposure.
- Concurrent engineering of energy metrics and security-aware communication structure is a dual-fitness routing scheme modulated by both- an element unattainable in previous SMORP-based research and ECC-based aggregation plan.
- Improved security strength based on a hybrid encryption and signature check by elliptic curves and maintains scalability with dense HWSNs.

Full MATLAB simulations indicate that the suggested framework has a substantial impact on network lifetime, distribution of residual-energy, secure aggregation overhead, and delivery reliability over the state-of-the-art routing and security baselines

2. RELATED WORKS

Recent developments in the area of heterogeneous wireless sensor networks (HWSNs) have increased the pressure on the design of routing protocols and security solutions that could meet both energy constraints and data privacy. The current research activities can be approximately divided into two directions that are complementary (i) energy-conscious clustering and routing algorithms aimed at extending network lifetime and (ii) lightweight cryptographic and authentication systems aimed at ensuring in-network data aggregation security. This part presents a selected collection of the recent literature, focusing on their methodology, performance, and limitations when used in scalable and secure HWSN implementation.

2.1. POWER-SAVING CLUSTERING AND ROUTING IN HWSNS.

In the heterogeneous wireless sensor networks (HWSNs), energy-efficient clustering and routing are still fundamental issues due to the underlying heterogeneity of the nodes, that is, they are not equal in terms of their initial energy and differing levels of computational power. Energy-conscious communication The classical clustering algorithms, including LEACH [10], SEP [11], and FSEP [12] achieved the benchmark of energy-optimal algorithms through localized data-aggregating and periodic rotation of CH. LEACH proposed a probabilistic mechanism of CH election that reduces the transmission overhead whereas SEP generalized this designation to unequal deployments by weighting probabilities of CH election by the initial battery level of each node. FSEP

also improved heterogeneity support by adding two sensor classes (L- nodes and H- nodes) which gave a better stability of the networks whose energy distribution was in multilevel. Such classical clustering protocols have been the usual benchmark models on performance comparison in current WSN studies because of its straightforwardness, reproducibility, and behavioral understanding in a heterogeneous environment. In addition, FSEP can also be of relevance in the case of HWSNs since its two level energy model is quite consistent with the heterogeneity assumptions typically utilized in large scale simulation research. Based on these classical models, optimization-based routing schemes have been proposed to overcome the constraints of these classical ones. A typical example is the Spider Monkey Optimization Routing Protocol (SMORP) proposed by Jabbar and Alshawi [16], which provides swarm-intelligence behavior to achieve the stability of CH selections, more evenly distributes the load, and delays the energy depletion SMORP consistently outperforms LEACH, SEP and FSEP on various measures; but is strictly an energy centric approach. It lacks cryptographic protection, in-network aggregation security or authentication, making it susceptible to manipulation in routing and tampering data in hostile conditions. More recently, trust-based routing as well as optimization-assisted routing strategies have been considered in order to increase reliability and resilience Muneeswari *et al*. in [17], introduced a Trust- and Energy-Aware Routing Protocol which compares the credibility of nodes to prevent malicious relays and enhance the reliability of packet delivery. Although these benefits are evident, the computation of trust is associated with much overhead when the network density is large. At the same time, Balan *et al*. in [18], came up with a Taylor-based Gravitational Search Algorithm (TBGSA) of multi-hop routing, which realized better load balancing and network lifetime. Nevertheless, it cannot be used in a hostile environment due to the lack of cryptographic or secure aggregation measures. Similarly, direction-aware multicast routing scheme was suggested by Lekshmi and Suji Pramila [19], to serve a vehicular sensor network with focus on stability in fast mobility. Though this model works in dynamic situations, it is not applicable to static HWSNs as well as confidentiality or authentication are not considered. More developments in optimization of clustering have also been reported based on metaheuristic methods. To get a more homogenous distribution of the residual-energy and minimize irrelevant re-clustering, Reddy *et al*. proposed a better way to get a better Grey Wolf Optimization (IGWO) that results in better distributions [20]. The approach that Jibreel *et al*. came up with is HMGEAR, which is a heterogeneous gateway-assisted routing protocol; it addresses the energy holes surrounding the base station, involving the combination of multi-hop and adaptive head in its selection [21]. Tabatabaei also illustrated the approach whereby optimization of bacterial foraging along with the mobile sink can minimize routing bottlenecks and increase the the network lifetime [22]. These strategies like SMORP did not provide support to security, which they were very effective in maximizing energy consumption. Notably, the new research carried out in [17-19], is a significant step forward regarding the trust-based routing, optimization-based clustering, and reliability-based communication. Nonetheless, all these works do not offer primitives of lightweight cryptography or authenticated aggregation of data, which are crucial in providing a reliable operation in adversarial HWSN setting. The continued divide highlights the necessity of having an integrated energy-security routing architecture, which inspired the proposed framework of integrated SMORP-IECC-ELGDS, reported in this paper.

2.2. LIGHTWEIGHT CRYPTOGRAPHIC AND SECURE AGGREGATION TECHNIQUES IN HWSNS

Heterogeneous wireless sensor networks (HWSNs) are constantly faced with the issue of security because the sensor nodes pose harsh requirements on the system since they have a minimal calculation ability, limited memory storage and lack of a power source that can be recharged. Although widely known to provide high levels of security with the use of less key, elliptic curve cryptography (ECC) based on public-key encryption is relatively costly in terms of its computational attributes, thus rendering its conventional implementations costly in energy-limited systems. In turn, there is a significant amount of literature devoted to the creation of lightweight cryptography, the optimization of ECC implementation, hybrid encryption schemes, authenticated communication schemes specific to WSNs. However, these methods have significant weaknesses that do not allow them to fit in clustering-based routing schemes or privacy ductile data aggregation chains in HWSNs. Among the first models, which have incorporated the use of ECC in terms of secure data forwarding, there is the ECC-Homomorphic Encryption (ECC-HE) model by Elhoseny *et al*. [13]. They can be cryptically aggregated to perform elliptic curve encryption and additive homomorphic operations, and their design supports it. Even though the approach can guarantee high confidentiality and allow the aggregation of results at intermediate nodes, without decryption, the homomorphic component greatly expands the size of ciphertext and the computational burden. Homomorphic addition and multiplicative operations are expensive which results in high processing latency, increases energy consumption, and reduces bandwidth. These inefficiencies make ECC-HE inappropriate in units whose battery is of low power like L-nodes in heterogeneous environments and its implementation is not practical in a network that needs long lifetime stability. Simultaneously, a number of works have tried to trim down the cryptographic weight load by suggesting lightweight or better ECC versions. Ramadevi *et al*. [14] brought the improvements aimed at major management efficiency and arithmetic reduction on a modular basis. Likewise, Hammi *et al*. in [23] and Mahlak *et al*. in [24] suggested the lightweight ECC techniques in which the complexity of scalar multiplication-the most prevalent cost in ECC operations-is minimized. Although these enhancements provide significant improvements in terms of encryption time and energy expenditure, they pay more attention to key exchange or node authentication. Notably, these works consider no authenticated secure aggregation, and they have no provision of checking integrity of aggregated data in the CHs. As a result, such plans do not fit well into hierarchical routing schemes whereby multi-level aggregation and authentication must be performed simultaneously. The literature has also covered hybrid cryptographic architectures. In particular, one should reference the ECDH-RSA model proposed by Abood *et al*. [15], that is, the diffusion of hardware via the Elliptic-Curve Diffie-Hellman of a secure key exchange strategy with the encryption of the payload using RSA. Despite the enhanced confidentiality and immunity to key compromise in hybrid designs, the RSA element

creates excessive modular exponentiation a highly power-intensive function in asymmetric cryptology. That is why ECDH-RSA cannot be used with HWSNs where the CHs have to work with data aggregation of multiple nodes subject to strict energy constraints. Moreover, such hybrid models do not have a lightweight signature mechanism, and therefore, they will not be able to authenticate aggregated data or provide multi-hop integrity. Other methods have sought to increase sensor network authentication. The commonly used digital signature schema has been suggested by Bashirpour *et al*. (2018) in [25], which provided a better authentication scheme on broadcasting using ECC-based signatures. Although the scheme provides good integrity and avoids the broadcast of unauthorised messages, the repetition of generation of signatures as well as their validation has heavy computational requirements. More important, this scheme is not applicable to the clustered routing architectures as well as to secure in-network aggregation. Consequently, the model does not match the operational specifications of heterogeneous and cluster-based WSNs even though it has a robust cryptographic basis. In this literature, some recurrent gaps can be seen to exist with regard to Major Shortcomings in Existing Security Models.

1. **High computational overhead**: Homomorphic ECC and RSA-based hybrids require excessive time and energy for cryptographic operations.
2. **Lack of integrated authentication and aggregation**: Most techniques address either confidentiality or authentication, but not both in one unified architecture.
3. **Incompatibility with clustered HWSNs**: Existing schemes are not designed for hierarchical routing structures where CHs perform multi-level aggregation.
4. **Absence of lightweight digital signatures**: ECC-based signatures remain costly and impractical for repeated verification at CH and BS levels.
5. **No optimization for heterogeneity**: Most models treat nodes as homogeneous, ignoring the energy imbalance inherent in HWSNs.
6. **Scalability concerns**: homomorphic systems do not scale efficiently in dense deployments.

Table 2 provides a comparative analysis of major lightweight cryptographic and secure aggregation schemes relevant to heterogeneous WSNs.

Novelty and Distinct Contribution

The novelty of the proposed SMORP–IECC–ELGDS framework lies in combining optimized energy-efficient routing with lightweight cryptographic protection in a single integrated architecture tailored for heterogeneous WSNs. In contrast to the previous SMORP-based works which solely optimize energy, the suggested design also presents the concept of security-conscious routing, where the selection of the CH factors in the residual energy and cryptography preparedness. The second contribution is the use of a lightweight IECC ciphertext-aggregation procedure to enable CHs without the need to decrypt encrypted input and ciphertext in a two-way communication to multi-hop aggregate ciphertext ECC-HE has been found to be computationally expensive, and plaintext exposure during multi-hop address this issue. In addition, the suggested ELGDS signature mechanism allows aggregation of authenticated results at relatively reduced cost compared to ECC-based signatures like those suggested by Bashirpour *et al*. [25], that is inappropriate in a clustered context as it involves repeated verification at high cost. Combined with the foregoing, these contributions can present the first framework where SMORP energy balancing and lightweight security are mutually influencing alongside one another therefore generating quantifiable advancements in lifetime, secure aggregation cost, and reliability of delivery.

2.3. INTEGRATED ENERGY–SECURITY FRAMEWORKS IN WSNS

Although both energy efficient routing and light-weight cryptographical schemes have been made with huge progress, not much literature has aimed at combining the two dimensions into a single architecture of heterogeneous wireless sensor networks (HWSNs). The current hybrid designs typically seek to integrate the secure communications models with routing protocols, but they are limited in scope, scalability, or application to clustered, multi-hop aggregation spaces. In [26], implemented one of the initial lightweight secure routing protocols in the IoT-oriented WSNs, a protocol combining the crypto-operations with multi-hop routing to reduce the black-hole and sinkhole attacks. The model supports only route's reliability though it fails to support hierarchical clustering or secure in-network aggregation, so it can only be applicable to HWSNs. Equally, [27] introduced an authenticated routing scheme that uses hashing primitives, which are used to maintain the integrity of the message and validation of the route. Although the model has a very high safeguard against packet tampering, repeated hashing and verification bring non-negligible overhead on the CHs and absent confidentiality-preserving aggregation, which makes the scheme inapplicable to hierarchies that are energy-sensitive. Liu [28] tried to make integration more security-conscious by integrating elliptic curve cryptography into a reliable routing protocol, to enhance link-level privacy and authentication. Although this design uses ECC to decrease key size and computational cost, it does not support ciphertext aggregation or lightweight digital signatures, two requirements in supporting multi-hop secure data fusion. As a result, even with security provided by ECC, the absence of the aggregation-aware optimization limits the framework to be used effectively within the densely populated or heterogeneous deployment. The overall result of these hybrid solutions shows increased popularity of using a combination of security and routing but they are not capable of providing a tightly integrated solution that may deliver encrypted aggregation, multi-level authentication, and optimization of energy consumption at the same time. No of the analyzed literature have a combined design of routing choices, cryptographic force, and signature examination in a heterogeneous cluster-based design. This deficiency highlights the necessity of a common architecture like the suggested SMORP-IECC-ELGDS concept-in which energy efficient routing and low weight security work together towards attainment of the rare needs of safe and scalable HWSNs. The table 1 recapsulates the main related works that are discussed in Section 2.1 and 2.2. Energy-efficient routing strategies are represented by rows 1-5, lightweight security and cryptographic mechanisms findings are summarized by rows 6-10, and the suggested SMORP-IECC-ELGDS model is mentioned in row 11.

Table 1. Unified Comparison of Energy-Efficient Routing and Lightweight Security Mechanism

Method	Technique Category	Key Idea	Strength	Limitation	Relevance to Proposed Work
TEARP (Muneeswari *et al*., 2023) [17]	Energy-efficient routing	Trust and energy-aware CH selection	Improves reliability and stability	High overhead in dense networks	Baseline for energy improvements
Taylor-GSA (Balan *et al*., 2023) [18]	Optimization-based routing	Taylor-based GSA for multihop load balancing	Good scalability	Parameter sensitivity	Energy comparison baseline
Direction-aware V2V (Vanitha & Prakash, 2024) [19]	Mobility-aware routing	Directional multicast routing	Robust to topology changes	Not suitable for static HWSNs	Shows limits of mobility-based models
SMORP (Jabbar & Alshawi, 2021) [16]	Metaheuristic clustering	Spider Monkey Optimization for CH rotation	Strong energy balancing	No security integration	Energy base protocol for integration
Reddy *et al*. (IGWO-CH, 2023) [20]	Metaheuristic-based clustering	Applies an improved Grey Wolf Optimization for energy-aware cluster-head selection	Improves energy balance and network lifetime	Does not consider security or secure data aggregation	Serves as an energy-efficient clustering reference motivating secure optimized routing
ECC Digital Signature (Bashirpour *et al*., 2018) [25]	Security authentication	ECC-based broadcast authentication	Strong integrity	High signature overhead	Security baseline for comparison
ECC-HE (Elhoseny *et al*., 2016) [13]	Homomorphic encryption	Encrypted aggregation using ECC-HE	Confidentiality + aggregation	Large ciphertext and high cost	Aggregation security comparison
Ramadevi *et al* ., 2023 IKEC [14]	ECC key exchange, Lightweight cryptography	Improved ECC key management and Reduced-complexity crypto for WSN	Lightweight key handling for Low computational cost	No aggregation support for Limited authentication features	Cryptographic complement baseline by Supports lightweight design rationale
ECDH–RSA (Abood *et al*., 2022) [15]	Hybrid cryptography	ECDH + RSA for secure transmission	Strong confidentiality	RSA overhead heavy for CHs	Motivation for lightweight hybrid
Proposed SMORP–IECC–ELGDS	Integrated routing + security	Energy-aware routing + hybrid ECC security	Unified secure aggregation + efficiency	—	Main contribution

3. PROPOSED METHODOLOGY

The research design adopted in this study is structured around an integrated workflow that links routing optimization with secure data aggregation. The routing layer is first responsible for cluster formation and multi-hop data forwarding, while the security layer operates concurrently to protect the transmitted data without interfering with routing decisions. This design ensures that energy efficiency and data security are addressed within a single operational process rather than as separate or sequential stages.

3.1. INTEGRATED ENERGY-EFFICIENT ROUTING AND SECURE DATA AGGREGATION METHODOLOGY

This part provides a holistic approach that combines an optimization-based clustering and routing framework with a lightweight cryptography framework in order to provide secure and energy-efficient data aggregation in heterogeneous wireless sensor networks (HWSNs). The new framework will utilize the (SMORP) to build dynamic cluster topology and balanced multi-hop routing paths, and a new hybrid security model, which consists of (IECC) and a hybrid security model (ELGDS) will be used to provide end-to-end confidentiality, integrity, and authentication. The proposed model integrates cluster formation, route stabilization, ciphertext aggregation and signature verification in a single operational pipeline, in contrast with traditional methods where routing and security processes have been engineered like applications without connection to each other. We have summarized the interactions between these components and the sequential execution of them conceptually in Fig. 1 and elaborated on each in the following section. Fig. 1 illustrates the interaction between SMORP clustering, optimized routing, IECC encryption, ciphertext aggregation, and ELGDS authentication within the integrated framework.

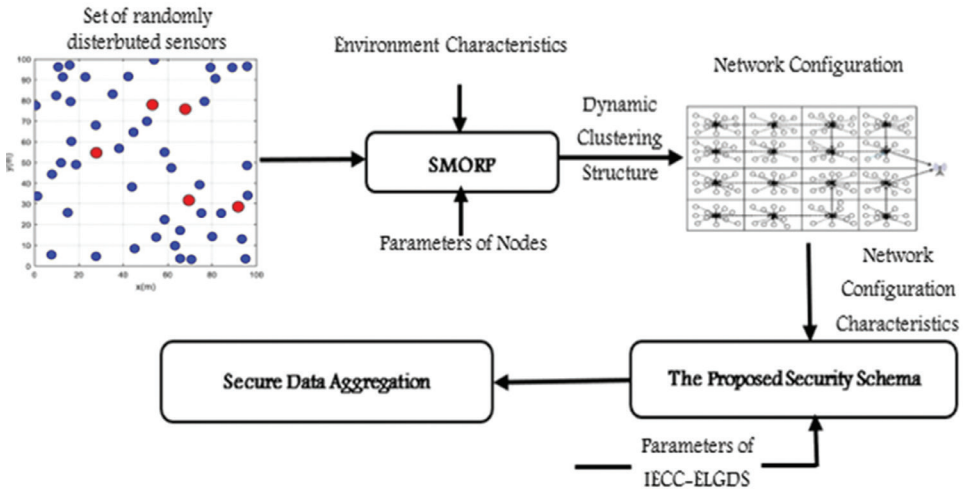

Fig. 1. Proposed Secure Data Aggregation Workflow Schema

3.2. SMORP-BASED CLUSTERING AND ROUTING PROTOCOL

The core procedure that is utilized in the development of the energy-balanced clusters and calculating the optimal multi-hop paths through the heterogeneous wireless sensor network is the Spider Monkey Optimization Routing Protocol (SMORP). The protocol is inspired by these social behaviors of spider monkeys, namely the fission-fusion foraging, subgroup form and rotation of leaders, are the elements that help maximize the energy efficiency. Under the proposed framework, SMORP has the responsibility of CH selection, election of a leader, formation of subgroups and refurbishment of routes as the residual energy goes down, and/or intra/inter-cluster distance. SMORP works in a series of iterative phases which entail network start, Local Leader Phase (LLP), Global Leader Phase (GLP), Local Leader Updating, Global Leader Updating and termination. All the stages help in the selection of balance CHs and construction of strong routing paths towards the sink.

3.2.1. Network Initialization and Node Evaluation

In the starting stage, the positional coordinates, residual energy and neighbor-list information of each sensor node are broadcast to give the initial network state involved in SMORP activities. It is on the basis of this information that candidate forwarding nodes are obtained and their suitability evaluated to proceed with being part of the routing structure. Evaluation is then done spatially to calculate the closeness of each node to the sink, as a node that is closer to sink usually takes lesser cost of transmission. Given the coordinates (x_s, y_s) of the sink and (x_l, y_l) of the candidate node l, the Euclidean distance is computed as:

$$\boldsymbol{d(l)} = \sqrt{(\boldsymbol{x_s} - \boldsymbol{x_l})^2 + (\boldsymbol{y_s} - \boldsymbol{y_l})^2} \quad (1)$$

This distance measure along with the nodes residual energy along with intra/inter cluster distance forms directly part of the calculate of the fitness value which rules routing potential of every node. The fitness function has the definition of:

$$\boldsymbol{fitness}\ (\boldsymbol{l}) = \boldsymbol{\alpha} \times \boldsymbol{RE(l)} + (\boldsymbol{\beta} \times \frac{\mathbf{1}}{\boldsymbol{D_1}} + \boldsymbol{\gamma} \times \frac{\mathbf{1}}{\boldsymbol{D_2}}) \quad (2)$$

- $RE(l)$ is the residual energy of node l.
- $D_1$is the distance between an L-sensor node and its associated CH.
- D_2 is the distance between the CH and the sink,
- (α, β, γ) are weighting coefficients regulating the impact of each parameter.

The fittest nodes are said to be the most suitable in terms of serving as nodes of CHs or forwarding nodes. This evaluation step gives SMORP an energy aware, spatially efficient, analysis of the network structure that can be utilized in effective decision-making during later local and global decision-making steps in choosing local and global leaders and routing states.

3.2.2. Fitness Evaluation and Forwarding Candidate Assessment

SMORP routing is based on a systematic analysis of forwarding candidate evaluation criteria depending on the availability of energy, spatial proximity, and cluster-specific metrics. Once initialized each node keeps current data on its remaining energy, its distance to the CH to which it belongs, and the distance between the CH and the sink. The metrics allow the protocol to build a spatially efficient and an energy-balanced forwarding infrastructure. At every expansion phase, candidate nodes are analyzed in order to be considered suitable to add to the routing path. A Euclidean distance d (l) of a candidate node l and sink calculated above in Eq. (1) is one of the basic spatial descriptors. The fitness in Eq. 2 is a combination of this distance and the nodes energy and distances associated with clusters produced and a total routing utility score. After the computing of the values of fitness of all the nearby candidates, the Global Leader Spider Monkey (GLSM) will examine them during which the forwarder with the most promise is identified. The forwarding possibility of a candidate node l_i is determined as

$$P(l_i) = \frac{fitness(l_i)}{\sum_{j=1}^{N} fitness(l_j)} \quad (3)$$

Where:

- $P(l_i)$ is the forwarding probability of node l_i.
- $fitness(l_i)$ is the fitness value of node l_i.

- N is the number of neighboring nodes considered in the expansion stage.

The candidate nodes that are found in the same iteration are successors to the expanded node and custodians of it by way of pack-pointers. This design allows SMORP to build a hierarchical expansion tree effectively searching the possibilities of routing. The growth will be repeated until the sink is reached and all data sensed will be sent via the optimal path. These forwarding measures are the basis of the process of leader coordination where multi-level leaders optimize the routing search and direct the expansion in the direction of the sink. The sequential interactions between the Local Leaders (LLs), their subgroup members (LLSMs) and the Global Leader (GLSM) are expounded in the subsequent section.

3.2.3. Leader Hierarchy and Sub-Group Formation in SMORP

SMORP arranges sensor nodes in a hierarchical leader-member framework which creates the opportunity to explore forwarding paths in a coordinated manner and equally balanced energy use. This is built by repeated estimation of the fitness of nodes when by the nodes with high fitness level become leaders of their local neighborhoods. Every neighborhood of nodes comprises a Local Leader Sub-Group (LLSG). In every LLSG, the node that has the largest fitness score is made the Local Leader (LL), and the rest of the nodes the Local Leader Sub-Group Members (LLSMs). The LL is able to examine several forwarding opportunities in its immediate environment. This design can guarantee that routing choices is not constrained on a particular node and is robust to local failures or fast failure of energy sources. At an international level, the node with the highest global fitness in the network is made the GLSM. The GLSM manages the further upper hierarchical advancement of the routing search and directs the choice of the most promising next level of expansion towards the sink. This strictly hierarchical team structure, where LLSGs develop into LLs and then into LLSMs overseen by the GLSM, lets SMORP build up a multi-level strategy of exploration. The LLSM oversees global refinement, the LLs control interaction between subgroups, and LLSMs are involved in the assessment of candidate successors. This multi-level coordination is the structural basis to the determination of the most suitable forwarding path. The complete operation of this mechanism is summarized in Algorithm 1 below.

Algorithm 1. SMORP-Based Packet Forwarding Procedures in HWSNs

Input:

- Set of sensor nodes N with positions and residual energy $RE(l)$
- Distances D_1 (L-sensor → CH) and D_2 (CH → $Sink$)
- Fitness parameters α, β, γ
- Sink node S

Output:

- Optimal forwarding path from source node to sink

1. Initialize network state and compute distances $d(l)$ to the sink for all nodes using Eq. (1).
2. Compute $fitness(l)$ for each node using Eq. (2).
3. Form Local Leader Sub-Groups (LLSGs) based on neighbourhood proximity.
4. For each LLSG do
5. Identify Local Leader (LL) as the node with maximum fitness.
6. Assign remaining nodes in the sub-group as LLSMs.
7. End for
8. Determine the Global Leader Spider Monkey (GLSM) as the node with highest global fitness.
9. Set current node ← source node.
10. Initialize Forwarding Path.
11. While current node ≠ Sink do
12. Extract neighbour set L of current node.
13. For each node $l_i \in L$ do
14. Compute forwarding probability $P(l_i)$ using Eq. (3).
15. End for
16. Select next node ← argmax $P(l_i)$, $l_i \in L$.
17. Set pack-pointer (next node) ← current node.
18. Append next node to Forwarding Path.
19. Update current node ← next node.
20. End while
21. Return Forwarding Path.

The steps outlined in Algorithm 1 describe how routing decisions are progressively refined based on node fitness and forwarding probability. By prioritizing nodes with higher residual energy and favorable spatial positions, the routing process avoids overloading specific nodes and maintains balanced energy consumption across the network. This procedural design supports stable multi-hop communication while preserving the energy efficiency required for long-term HWSN operation. In the enhanced formulation of SMORP adopted in this work, several structural and operational refinements are incorporated to overcome the limitations of the classical SMORP routing mechanism and to better accommodate the requirements of heterogeneous wireless sensor networks. Among the significant enhancements, it is possible to list the following:

- **Multi-Metric Fitness Evaluation**: The distance-centric SMORP model is expanded by including a composite fitness functional which takes into account jointly the residual energy and the L-sensor-to-CH distance as well as the CH-to-Sink distance. This multi-parameter assessment makes the forwarding decisions more balanced and avoids the early exhaustion of the critical nodes.
- **Probability-Driven Forwarder Selection**: To better improve on heuristic exploration, instead of using a simple heuristic exploration, candidate forwarding nodes are being selected based on a normalized probability that is based on the fitness values of the candidate forwarding node. This deterministic choice allows contributing to the ability of routing stability and the reduction of the risk of repetitive selection of the same nodes in the subsequent round.
- **Refined Multi-Level Leadership Hierarchy**: It is an extension of organizational hierarchy explicitly expanding it to encompass (LLSMs), (LLs), (LLSGs) and (GLSM). Such high-level refinement enhances coordination and decentralized decision-making in heterogeneous nodes in subgroups.
- **Heterogeneity-Aware Role Assignment**: The improved SMORP is able to incorporate the distinct roles

of L-sensor nodes and CHs as part of the optimization cycle. This is to make sure that nodes that have less energy or ones with lesser communication ability are not overwhelmed, which means that routing performance of HWSNs can be made more sustainable.

Security-Compatible Routing Design: The routing paths resulting under the enhanced SMORP are built in a way to allow ciphertext forwarding and authenticated aggregation, which make them easy to integrate with the IECC-ELGDS security architecture presented in the following section. The traditional SMORP formulation lacks such a compatibility. All of these improvements make SMORP an energy-conscious, heterogeneity-aware, and security-enabled routing mechanism than the conventional SMORP model that was applied in previous works. As an explanation to an outline of the hierarchical coordination process applied in the enhanced SMORP formulation, Fig. 2 represents the multi-level leadership structure that is adopted in subgroup construction and route construction.

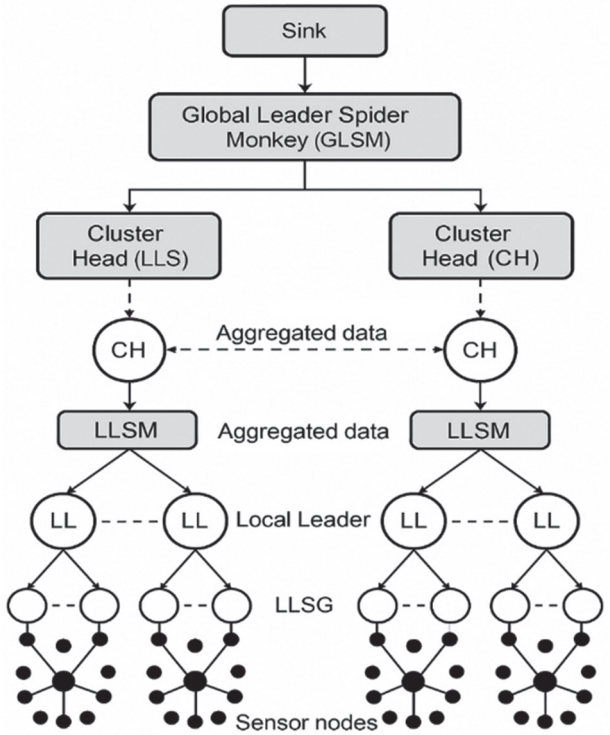

Fig. 2. Multi-Level SMORP Hierarchy

In this architecture the sensor nodes will first be clustered into (LLSGs), which are controlled by (LL) that would facilitate localized decision making. Higher on, several LLs will be assigned to (LLSM), whereby the consolidation of reports on subgroups is made, and the routing activities are coherent among distributed routing activities. The topmost position of decision-making is controlled by (GLSM), and it is the one that coordinates inter-cluster communication, and guides the construction of the ultimate multi-hop routing path to the sink. This hierarchy allows forwarding candidate evaluation in distributed fashion that is scalable, routing overhead reduction and also improves stability of constructed paths. Also, the illustration points out the smoothness of the interaction between these layers of leadership and the underlying cluster-based architecture of the heterogeneous network and which basis the structural foundation of the optimized routing process illustrated in the previous subsections.

3.1. INTEGRATED SECURITY ARCHITECTURE USING IECC AND ELGDS

To ensure confidentiality, integrity and authenticity at proposed routing framework, the proposed work uses dual layer light weight security architecture through (IECC) scheme of data encryption and (ELGDS) scheme of authentication. These two should be used in conjunction to make the routing energy efficient as provided by SMORP and computationally manageable when facing a mixed population of the wireless sensor nodes with limited processing and energy capabilities.

The routing mechanism will operate in parallel to the security architecture where L-sensor nodes will encrypt the sensed data with IECC and the CHs will have access to the encrypted data but not to the decrypted one. Such a design makes the intermediary nodes unable to access plaintext values, and decreases eavesdropping or tampering. Besides, a digital signature is generated to every encrypted packet by ELGDS to ensure that the sink can perform end-to-end authentication of the data authenticity and prevent any form of data manipulation in the event that the packet is forwarded through a multihop. This is ensured by the combination of IECC and ELGDS to ensure that safe data aggregation is carried out effectively and efficiently without imposing excessive computing load on low-power nodes. The elements of the proposed security architecture are discussed in the subsections below starting with description of encrypted communications to be used in the system i.e. the IECC encryption model, and then the description of the ELGDS signature mechanism and finally the inbuilt workflow of secure aggregation.

3.3.1. IECC-Based Lightweight Encryption Model

The Improved Elliptic Curve Cryptography (IECC) model suggested to be used as the first element of the proposed security architecture is used to deliver lightweight and energy-efficient data confidentiality to heterogeneous wireless sensor networks. IECC has been chosen because it can provide high cryptography security certain key sizes, which are small enough to be applicable to sensor nodes with small computational capacity and restricted battery power. Under the proposed framework, an elliptic-curve public-private key pair is produced by every L-sensor node and the sinks public key is used to encrypt transmission sensory data by the sending node before transmission. This guarantees that the original plaintext can only be garnered by the sink which holds the corresponding private key. The encryption process of the IECC is as follows: the sensed data of the sensor nodes is first mapped to a point in the elliptic curve and a scalar multiplication with the sinks public key is performed to obtain a pair of ciphertext elements. Such ciphertext values are then sent across the intermediate nodes and CHs without being decrypted and therefore they cannot be accessed by unauthorized users in the multi-hop routing. The energy overhead of encryption is further diminished because the head of the cluster can provide aggregation of ciphertext directly; this means that the energy cost of encryption is only realized once at the sensing node thereby minimizing the total level of computational overhead experienced by secure data aggregation. The IECC model can provide confidentiality with the, in comparison, very small key sizes of elliptic-curve operations, which does not compromise the long-term viability of the heterogeneous sensor nodes.

This lightweight encryption mechanism forms the foundation for the authenticated secure aggregation workflow described in the subsequent subsections. "The operational steps of the IECC key generation and encryption process at each L-sensor node are summarized in Algorithm 2.

Algorithm 2. IECC Key Generation and Encryption at L-Sensor Node

Input:

- Elliptic curve parameters (p, a, b), base point G of order n,
- sink public key Q_{sink}, plaintext message M.

Output:

- Ciphertext pair (C_1, C_2).

% Offline key generation phase (performed once per L-sensor node)

1. Select an elliptic curve E over a finite field F_p defined by
- $E: y^2 = x^3 + ax + b \pmod p$, where a and b are integers such that E is non-singular.
2. Choose a base point $G \in E(F_p)$ with large prime order n.
3. Select a private key d_{node} randomly such that $1 \le d_{node} \le n - 1$.
4. Compute the corresponding public key of the node as $Q_{node} = d_{node} \cdot G$.

% Online encryption phase at the L-sensor node

5. Represent the sensed data as a point M on the elliptic curve E.
6. Select a fresh random integer k such that $1 \le k \le n - 1$.
7. Compute the first ciphertext component as $C_1 = k \cdot G$.
8. Compute the second ciphertext component as $C_2 = M + k \cdot Q_{sink}$.
9. Form the IECC ciphertext as the pair $C = (C_1, C_2)$.
10. Transmit the ciphertext C to the cluster head or next-hop node.
11. Return (C_1, C_2).

3.3.2. ELGDS Digital Signature and Authentication

The second component of the proposed security architecture is (ELGDS) scheme, which is employed to ensure end-to-end data authenticity and integrity throughout the multi-hop transmission process. CO The flow of control in ELGDS is similar to that of IECC in that the sink can confirm that every received ciphertext was produced by a trustful source and no alterations were made to the message when it was forwarded. Such a two-layer design will keep the enemies off-balance-sheet as they cannot send spoofed packets, modify encrypted values, or repeat already transmitted messages in the network. Since the digital signature is generated with the help of the private signing key of each L-sensor node in the suggested framework, each node uses its own key to create a signature to every packet encrypted with the help of IECC. The signature is calculated against a hashed version of the ciphertext so that subtle changes in a cipher-text payload will spoil the signature. The signature pair that is obtained is added to the ciphertext prior to sending, allowing the intermediate nodes to transmit the information without doing any authentication. The computational load of signature generation is therefore restricted to the source L-sensor nodes since CHs are only used as a point to aggregate, and are never involved in the authentication. When the sink receives a ciphertext packet made up of aggregates, it decrypts the packet with the public verification keys supplied to the sink to confirm the ciphertext signatures attached to the packet. Effective verification guarantees that the ciphertext elements were created by honest nodes and in addition to that, they were not distorted during the routing. This end-to-end authentication mechanism eliminates impersonation, tampering and replay attack, thereby strengthening the security guarantees of the proposed secure data aggregation model without imposing excessive computational overhead on intermediate nodes.

Algorithm 3. ELGDS Key Generation and Signature Generation at L-Sensor Node

Input:

- Large prime modulus p, generator g of Zp^*,
- private signing key x ($1 < x < p - 1$),
- hash function $H(\cdot)$, message m.

Output:

- Public verification key y, digital signature (r, s) for m.

% Offline key generation phase (executed once per L-sensor node)

1. Select a large prime number p and a generator g of the multiplicative group Zp^*.
2. Choose a private signing key x such that $1 < x < p - 1$.
3. Compute the corresponding public verification key as $y = g^x \bmod p$.

% Online signature generation phase (executed whenever a message m is sent)

4. Compute the message hash $h = H(m)$, where h is mapped into $Zp-1$.
5. Repeat
6. Select a random ephemeral key k such that $1 < k < p - 1$.
7. Until $gcd(k, p - 1) = 1$.
8. Compute $r = g^k \bmod p$.
9. Compute the modular inverse k^{-1} of k *modul o* $(p - 1)$.
10. Compute the second signature component as $s = k^{-1} \times (h - x \cdot r) \bmod (p - 1)$.
11. Output the public verification key y and the digital signature pair (r, s).

It is worth noting that the key generation phase in Algorithm 3 is executed infrequently and can be performed offline, ensuring that only lightweight signing operations are carried out during regular sensing rounds.

3.3.3. Integration of IECC and ELGDS for Secure Data Aggregation

The concluding phase of the presented security architecture offers the assurance of confidentiality (IECC) with the assistance of the authentication and integrity services given by the (ELGDS) scheme to create a single effective wise data aggregation pipeline. Each L- sensor node in this model optimizes the sinks IECC public key with its encrypted data and

then entities a digital signature over the encrypted data. This joint encryption-signing process also provides confidentiality, authenticity and integrity of data are applied before a packet is sent by the sending node. In the routing step, packet ciphertexts and their signatures are sent out by intermediate nodes such as CHs and are not decrypted or validated. This design inhibits plaintext exposure and does not distribute computationally expensive cryptographic operations across resource restricted forwarding nodes. CHs perform ciphertext-preserving aggregation, which is a process that allows data forwarding over multi-hops and keeps the encrypted version of the information all the way across the routing path. Since aggregation is performed directly on ciphertext, no intermediate node would have access to the underlying sensing data, which practically performs leakage elimination even in case compromised forwarding nodes. When the aggregated ciphertext and the corresponding set of signatures are received the sink starts to run a two-stage recovery process. To ascertain an authenticity and integrity of every encrypted contribution, first, ELGDS public verification keys are applied. Block ciphertexts that do a pass are only stored to undergo further processing after signature check passes. Second, timely verification is performed, and secondary to it is IECC decryption, as a result of which the sink constructs the organized plaintext.

A verification-first architecture ensures that manipulated or replayed ciphertext is completely dropped before decryption and thus prevents impersonation attacks, tampering and fake-contributions to the network. The integrated IECC-ELGDS model achieves a strong end-to-end end-authentication and confidentiality with the use of the L-sensor nodes and the sink alone and conserves the energy resources of the intermediate nodes. Algorithms 4, essentially express the whole workflow of the new scheme, including generation of ciphertext, building signature, middle-level forwarding, signature verification and recovery of plaintext.

Algorithm 4. Integrated IECC–ELGDS Secure Aggregation

Input:

- For each L-sensor node i: plain text message Mi, IECC parameters (p, a, b, G, n),
- sink public key Q_{sink}, ELGDS parameters (p, g, x_i, y_i), hash function $H(\cdot)$.

Output:

- At the sink: verified aggregated plaintext M_{agg}.

% Phase 1: IECC encryption and ELGDS signing at each L-sensor node

1. For each L-sensor node i do
2. Map the sensed data to a point M_{ion} the elliptic curve E over F_p.
3. Select a random k_i such that $1 \le k_i \le n - 1$.
4. Compute $(C_1)_i = k_i \times G$.
5. Compute $(C_2)_i = M_i + k_i \times Q_{sink}$.
6. Form the IECC ciphertext $C_i = ((C_1)_i, (C_2)_i)$.
7. Compute the message hash $h_i = H((C_1)_i, (C_2)_i)$.
8. Select a random ephemeral key k_s such that $1 < k_s < p - 1$ and $gcd(k_s, p - 1) = 1$.
9. Compute $r_i = g^{(ks)} \bmod p$.
10. Compute $k_{s(-1)}$ as the modular inverse of k_s modulo $(p - 1)$.
11. Compute $s_i = k_{s(-1)} \times (h_i - x_i \times r_i) \bmod (p-1)$.
12. Attach the signature $\sigma_i = (r_i, s_i)$ to the ciphertext Ci.
13. Transmit the packet $P_i = ((C_1)_i, (C_2)_i, r_i, s_i)$ to the corresponding cluster head.
14. End for

% Phase 2: *Ciphertext* forwarding and aggregation at intermediate nodes / *CHs*

15. For each cluster head CH do
16. Collect incoming packets P_i from associated L-sensor nodes.
17. Perform ciphertext aggregation:
    $(C_1)_{agg} = f_1\{(C_1)_i\}$, $(C_2)_{agg} = f_2\{(C_2)_i\}$,
    where f_1 and f_2 preserve *ciphertext* structure.
18. Forward aggregated *ciphertext* $C_{agg} = ((C_1)_{agg}, (C_2)_{agg})$
    Along with signatures(σ_i) toward the sink.
19. End for

% Phase 3: Signature verification and IECC decryption at the sink

20. Upon receiving C_{agg} and the set (σ_i), the sink performs:
21. For each node i do
22. Recompute $h_i = H((C_1)_i \,||\, ((C_2)_i)$.
23. Compute $(v_1)_i = (yi^{(ri)} \times r_i^{(si)}) mod\ p$.
24. Compute $(v_2)_i = g^{(hi)} \bmod p$.
25. If $(v_1)_i \neq (v_2)_i$ then
26. Discard the corresponding ciphertext contribution.
27. End if
28. End for
29. Apply IECC decryption to recover aggregated plaintext (M_{agg})
    $M_{agg} = (C_2)_{agg} - d_{sink} \times (C_1)_{agg}$.
30. Output the verified aggregated plaintext M_{agg}.

3.4. NOVELTY AND DISTINCT DESIGN CONTRIBUTIONS

The suggested framework presents a collection of unique design provisions that will separate it with the current routing and security plans in heterogeneous wireless sensor networks (HWSNs). In contrast to the original SMORP formulation in Jabbar and Alshawi (2021) [16], where the protocol is concerned only with the formation of clusters through energy-efficient routing and multi-hop routing, but no cybersecurity integrity version is introduced-the methodology established in this paper inserts a full cryptographic pipeline directly into the SMORP framework of operation. The improved model adds confidentiality-saving IECC encryption to SMORP, end-to-end signature enforcement by ELGDS, ciphertext-presaving CH aggregation and secure signatures propagated on-top of the hierarchical LLSM-GLSM routing process. This forms a hybrid between SMORP as a simple optimization-driven routing protocol, and as a resilient, secure-by-design communication architecture, which can support resilient multi-hop data forwarding in adversarial environments. Compared to the single ELGDS digital signature protocol modeled by Bashirpour *et al*. in [25], where user authentication is enabled by the protocol, but routing is not, multi-hop data aggregation, and the ability to adapt to the resource constraints inherent to HWSNs, the proposed framework integrates lightweight encryption and authentication into an energy-aware communication substrate. IECC-ELGDS hybrid mechanism is specially designed to be implemented in heterogeneous environment of sensors so that all the cryptographic actions are performed at L- sensor

nodes and at the sink. This design reduces the calculational burden of computing nodes and allows relaying encrypted and signed packets without the decryption or verification steps in the middle of the path. The innovative character of the offered approach is thus in three aspects:

- Co-design in routing-security networks, SMORPs leader-based optimization structure has been generalized to support ciphertext routing, signature propagation, and secure aggregation with no modification of protocols energy-efficiency goals.
- Multi-hop aggregation uses ciphers, such that the CHs are allowed to receive the aggregation of encrypted numbers and ensure the utmost confidentiality of sensor data.
- A verification-first decryption model, whereby the sink validates all received ciphertext elements with ELGDS prior to the IECC decryption, which gives a high level of resistance to tampering, replay and impersonation.

These collectively enhanced advances make the proposed system have a single secure routing and aggregation pipeline that has never existed in any other SMORP-based research, or ECC-based authentication system. This combined design is the basic contribution of the work and it is used in the development of the better performance and security properties in the further parts.

3.5. INTEGRATION OF SMORP WITH THE IECC–ELGDS SECURITY MECHANISM

The presented framework ensures the integration of SMORPs optimization-based routing framework and lightweight IECC-ELGDS security framework to offer an integrated and thorough approach to data aggregation of heterogeneous wireless sensor networks both in energy efficiency and full security. In contrast to a more traditional design where routing and security are separate, integration here means the implementation of confidentiality, authentication and ciphertext aggregation directly into the SMORPs multi-level Leadership and forwarding work. This allows the routing operation to be energy sensitive and at the same time minimize delays on how data is sent without the wrongdoer violating the data integrity against eavesdropping, manipulation, and impersonation. Each L-sensor at the sensing layer ciphers its result with the sinks IECC public key and creates an ELGDS signature over the resultant ciphertext before participating in the SMORP routing workflow. This will make sure that the packets played in the forwarding procedure are already encrypted. Just like in the original SMORP, the encrypted packets and the respective SMORP signature are propagated in the same route as the optimization-built routes in the hierarchy of (LLs), (LLSM), and (GLSM). Importantly, cutting points such as head of a cluster only do forwarding actions without decryption or validation of signature. This architecture avoids exposing plaintext at energy-constrained nodes, as well as maintains the lightness of the routing substrate. The forwarding mechanism of every SMORP level is unchanged in that the suitability of forwarding candidates is still using the formulation of energy-aware fitness presented earlier in the form of Eq. (2), except that the fitness of forwarding is now determined using residual energy and cluster-specific distance measures(D_1, D_2). By keeping the original routing utility measure introduced in Section 3.2.1, the integration will preserve the efficiency of SMORPs without compromising the efficiency of the security layer in any way. In multi-hop propagation, elements of the ciphertext, namely (C_1, C_2) in the structure of ciphertext in Section 3.3.1, are propagated, and CHs do ciphertext-preserving aggregation using the homomorphic addition property of the IECC construction. This enables a direct aggregation of encrypted values to be done without any loss of its complete confidentiality.

The sink starts a two-step recovery process after aggregated ciphertext contributions have been received. Signatures authentication is initially carried out with the ELGDS verification condition in algorithm 4 of Section 3.3.3. Only ciphertext blocks whose signatures satisfy the relation (v_1, v_2)are accepted for further processing. Second, the validated ciphertext is decrypted using the IECC private key to reconstruct the aggregated plaintext. This verification-first model prevents forged or manipulated ciphertext from entering the decryption pipeline and enhances the system's resilience against replay, impersonation, and tampering attacks. By integrating the routing utility of Eq. (2), the IECC ciphertext formulation of Section 3.3.1., and the ELGDS signature verification rule in Algoritm 4, the proposed system produces a cohesive secure-SMORP framework capable of delivering energy-efficient, confidential, and authenticated multi-hop communication. The complete operational flowchart of this integrated model is illustrated in Fig. 3, which summarizes the interaction between SMORP routing stages and the IECC–ELGDS cryptographic operations.

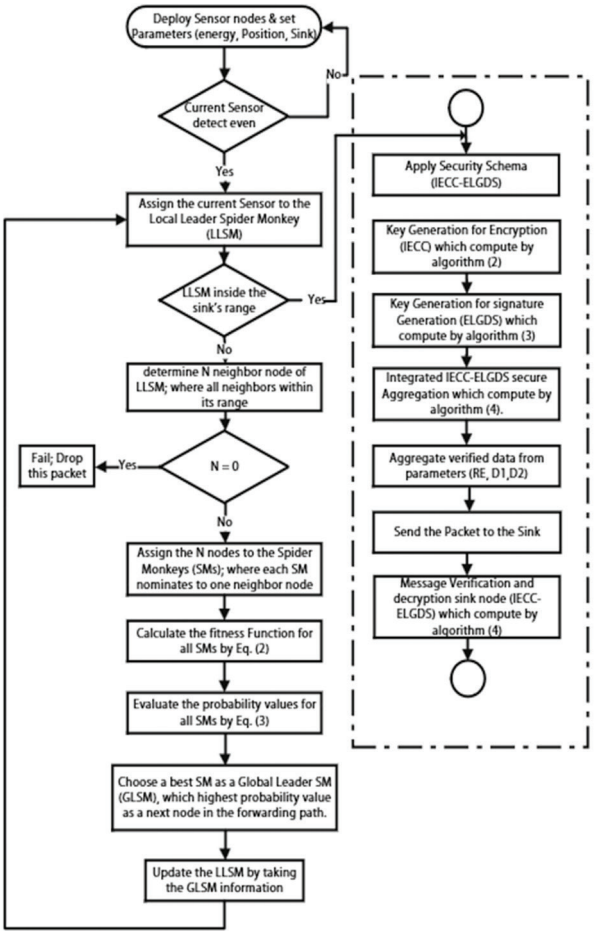

Fig. 3. Flowchart of Proposed method (Security schema IECC-ELGDS) in SMORP for HWSNs

4. SIMULATION ENVIRONMENT AND PERFORMANCE EVALUATION

A structured simulation environment was established to rigorously examine the performance of the proposed SMORP routing and IECC–ELGDS security mechanisms. This section outlines the evaluation framework, including deployment assumptions, communication model, parameter settings, and metrics employed to assess efficiency and robustness. The simulation assumes static sensor nodes and ideal channel conditions; therefore, the obtained results reflect performance under controlled network scenarios.

4.1. NETWORK DEPLOYMENT

The deployment of heterogeneous wireless sensor network is under a square sensing area of (100 m by 100 m). One hundred L-sensor nodes and five CHs are randomly distributed throughout the field to have a realistic and non-uniform spatial distributions. Fig. 4 gives a structure, in a schematic way, of the heterogeneous network layout that represents the spatial distribution of L- sensor nodes, hierarchical arrangement of CHs, and the location of sink such that it gives a vivid visualization of the deployment structure assumed in the work.

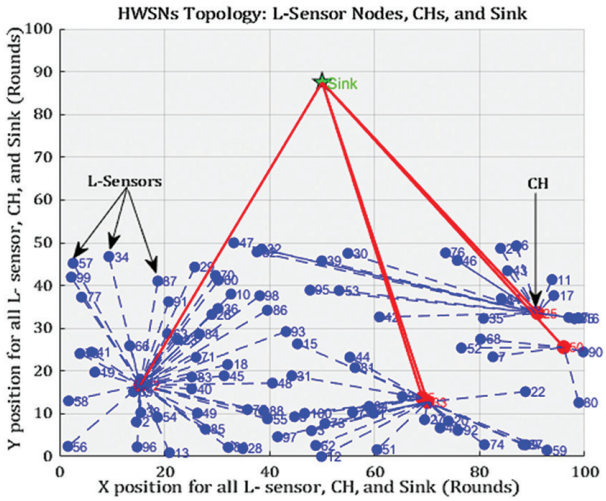

Fig. 4. HWSN topology showing L-sensor nodes, cluster heads (CHs), and sink placement

The nodes are stationary during the simulation and the geography is assumed to be known. One sink node is deployed at (50 m, 85 m), which is at the boundary that is close to the upper limit of the field to create routing asymmetry and resembles real-life multi-hop communication pattern. The L-sensors carry sensed information into their corresponding CH, where ciphertext aggregation is carried out into the sink. The transmission distances of L-sensors and CHs are set to 20 m and 80 m respectively, and this allows the creation of a three-level routing topology, which is based on the dispersity of the energies of nodes. Energy levels will be configured initially to 0.5 J/L-sensors and 2.5 J/CHs, which are consistent with the standard specifications of the heterogeneous WSN hardware platforms. The game continues up to 2000 rounds, with each round consisting of one full sensing-aggregation-transmission cycle on the network. This implementation scheme aligns with real-world use of HWSN deployments in environmental surveillance, and smart-city systems, where nodes will be heteronymously deployed, and will not be moved once in place. With such a set-up, realistic energy-depleting behavior, variability of routes, and the joint effect of SMORP routing and IECCELGDS secure data aggregation on that of the entire network is measured.

4.2. RADIO ENERGY MODEL

The energy consumption of wireless communication in the heterogeneous sensor network is modeled using the first-order radio model, which is widely employed in WSN performance evaluation and remains consistent with foundational studies such as LEACH [10]. This model provides an analytically tractable and experimentally validated representation of radio dissipation, making it suitable for both short-range L-sensor transmissions and *long-range CH*-to-sink links within heterogeneous architectures. In this model, the energy required to transmit a k-bit packet over a distance d depends on whether the communication operates in the free-space regime or the multipath-fading regime.

$$E_n T(k) = \begin{cases} k \times \left(E_{ele} + E_{fs} \times d^2\right) & if\ d < d_0 \\ k \times \left(E_{ele} + E_{fs} \times d^4\right) & if\ d \geq d_0 \end{cases} \quad (4)$$

Where:

- E_{elec} is the per-bit electronic circuitry cost.
- E_{fs} and E_{mp} represent the free-space and multipath amplifier coefficients, respectively.

The threshold distance that separates the free-space and the multi-path fading channel models is:

$$d_0 = \sqrt{\frac{E_{fs}}{E_{mp}}} \quad (5)$$

The energy consumed to receive a k-bit packet is defined by:

$$E_n R(k) = k \times E_{elec} \quad (6)$$

This model follows the formulation introduced by Heinzelman *et al.* [10], and it provides a widely accepted abstraction for radio communication energy in wireless sensor networks. Its linear-plus-distance-dependent structure accurately reflects the physical behavior of low-power transceivers and ensures fair comparison with prior routing- and clustering-based WSN protocols. In heterogeneous sensing environments, L-sensor nodes perform primarily short-range transmissions to their nearest CHs, while CHs conduct longer-range forwarding toward the sink. This asymmetry is best represented by the adopted dual-regime model in which short range transmissions would be within the free-space region whereas CH-to-sink links would often induce the multipath model because of larger transmission distances. This difference can accurately estimate node level energy consumption, visible energy dynamics and network lifetime characteristics using SMORP routing with the built in IECC-ELGDS secure aggregation. Fig 5. and Table 1 summarizes the radio-model parameters used in the simulations, including (E_{elec}, E_{fs}, E_{mp}) and E_{DA}. These parameters are identical for both L-sensor nodes and CHs, since they represent hardware-level characteristics of the transceiver module used across all nodes. The sole differences between L-sensors and CHs are their initial energy capabilities and range of transmission which are indicated separately in Table 2.

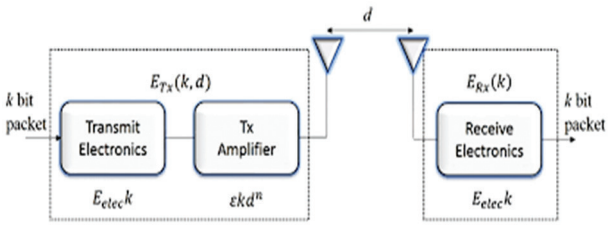

Fig. 5. first-order radio model

Table 2. Specifications of the Initial Radio Model for Both L-Sensors and CH

Parameter	Description	Value
E_{elec}	Energy for T_x/R_x electronics	50 nJ/bit
E_{fs}	Free-space amplifier coefficient	10 $pJ/bit/m^2$
E_{mp}	Multipath amplifier coefficient	0.0013 $pJ/bit/m^4$

4.3. SIMULATION PARAMETERS

Every simulation test was performed in the MATLAB R2023a under the singular assessment atmosphere so that each and every scheme was evaluated equitably and reproducibly. The complete operational cycle; the sensing stage, the aggregating stage, the process of secure processing, the routing stage, the radio-energy updating stage occur in each simulation round, and the overall assessment is 2000 rounds. Every routing and security protocol functions within the same communication constraints of the first-order radio energy model of Section 4.2. All protocols use a fixed value of 2 kB packet-size to ensure uniformity when being evaluated in terms of transmission-cost. All the comparative benchmark protocols were implemented with identical node deployment, sink position, radio parameters and initial energy settings. The most widely used baseline routing algorithms are LEACH [10], SEP [11], and FSEP [12], whereas the security-oriented schemes are ECC-HE [13], IEKC [14], and ECDH-RSA [15]. These protocols are also popular reference models in the optimization of WSNs and secure data aggregation, and their presence in the evaluation guarantees that the success of the suggested SMORP routing and IECC-ELGDS security framework are performance contributions of the evaluation. Cluster heads use a fixed cost of data-aggregation (E_{DA})and L-sensor nodes send un aggregated values to the corresponding CHs before they are processed securely. In order to reduce bias in statistics due to randomly selected nodes or the sequence of events, every experiment was repeated a couple of times and the mean of the outcomes was published. The same three-tier hierarchy of communication L-sensors, CHs and sink was determined in all simulations, and the ranges of L-sensors and CHs transmission were 20 m and 80 m, respectively, to indicate the heterogeneous network energy capacity. Table 3 gives a full overview of all the parameters of the simulation considered in the evaluation.

Table 3. Parameters of the simulation

	Parameters	Value
	Topographical area (meters)	(100 m×100 m)
	Sink location (meters)	(50 m×85 m)
	Control packet length	2 k
L-Sensors	No. of transmission packets (rounds)	2×10^3
	No. of SMORP , FSEP, and LEACH	100
	Distance limit for transmission	20 m
	Initial energy	0.5 J
CH	No. of SMORP and SEP	5
	Distance limit for transmission	80 m
	Initial energy	2.5 J
	Energy data aggregate	5 nJ/bit

4.4. PERFORMANCE METRICS

In order to provide a rigorous and reproducible analysis of the suggested SMORP-IECC-ELGDS framework, the following subsection offers the performance metrics applied in the course of the simulation study. Both metrics will be given a definition, a mathematical formula, and a clear explanation of all the variables. All of these measures evaluate the efficiency of routing, energy sensitivity, latency response, network lifetime, and computational cost associated with the built-in security solutions.

4.4.1. Network Lifetime

Network lifetime is a measure reflecting the efficiency of the routing structure concerning the consumption of energy and the balancing of consumption amongst heterogeneous nodes. Two indicators are adopted, which are:

- **First Node Dead (FND)**: the round at which the first sensor exhausts its energy, reflecting the stability period of the network. The earliest time at which any L-sensor exhausts its energy as shown in Eq. (7)

$$FND = r\{\min|E_i(r) = 0, i = 1, \ldots, N\}\cdot(7) \quad (7)$$

Where $E_i(r)$ denotes the residual energy of node i at round r, and N is the total number of deployed sensors. FND is especially important in HWSNs where the loss of even a single L-sensor creates a sensing void.

- **Last Node Dead (LND):** Denotes the round index at which the final remaining node exhausts its residual energy. With the help of this metric, the maximum sustainable lifetime of the network can be measured and how well the energy consumption is distributed between L-sensors and CHs. A larger LND means better load balancing and greater duration of full-network operation as includes in the Eq. 8.

$$LND = r\{\max|E_i(r) = 0\} \quad (8)$$

4.4.2. Average Residual Energy (ARE)

In the same way that equation (9) is used to compute the arithmetic mean of the remaining energy of all the nodes in each round, we get a worldwide view of what network sustainability is doing. Higher ARE values indicate that the proposed routing and secure-aggregation processes avoid concentrating energy consumption on specific nodes, especially CHs or high-traffic forwarders, which is critical for prolonging system lifetime in heterogeneous WSN environments.

$$ARE(r) = \frac{1}{N}\sum_{i=1}^{N} E_i(r) \quad (9)$$

4.4.3. Packet Delivery Ratio (PDR)

Packet Delivery Ratio quantifies reliability by measuring the ratio between the number of received packets and the number of packets generated by sensing nodes. It is defined as:

$$PDR = \frac{P_{recv}}{P_{sent}} \quad (10)$$

Where: P_{recv} is number of packets correctly received at the sink, and P_{sent} is total packets transmitted by L-sensors. A higher PDR reflects robustness against packet loss, interference, and route instability, as shown in Eq. (10).

4.4.4. End-to-End Delay (E2E)

End-to-End Delay measures the total time required for a data packet to travel from an L-sensor node to the sink through multi-hop aggregation. Let $t_{recv}(p)$ be the packet reception time at the sink and $t_{send}(p)$ be the packet transmission time at the source. E2E is defined as Eq. (11):

$$E2E = t_{recv}(p) - t_{send}(p) \tag{11}$$

Where: $t_{send}(p)$ is a time of the packet is generated, and $t_{recv}(p)$ is a time of the sink receives the packet. Lower delay indicates better routing efficiency and reduced congestion.

4.4.5. Data Aggregation Security Overhead

This measure represents the incremental cost of the security layer of the IECC-ELGDS compared to the base communication and calculation cost of the operation done by the scorecard through the aggregation and routing of this service. The overhead encompasses the power consumption of elliptic-curve-based encryption, generation of digital signature, verification of digital signatures, and aggregation of ciphertext undertaken during the routing path. The overall security overhead per message E_s in the form of equations is expressed as E_q (12):

$$E_{sec} = E_{enc} + E_{sig} + E_{ver} + E_{agg} \tag{12}$$

Where:

- E_{enc}: energy consumed by IECC encryption.
- E_{sig}: energy required for ELGDS signature generation.
- E_{ver}: verification cost at the sink.
- E_{agg}: cost of ciphertext aggregation at CHs.

A reduced security overhead gives a more efficient cryptography structure of heterogeneous WSNs. Comparative costs of the proposed IECC-ELGDS scheme and competent techniques (ECC-HE, IEKC, ECDH-RSA) are shown in Fig. 6.

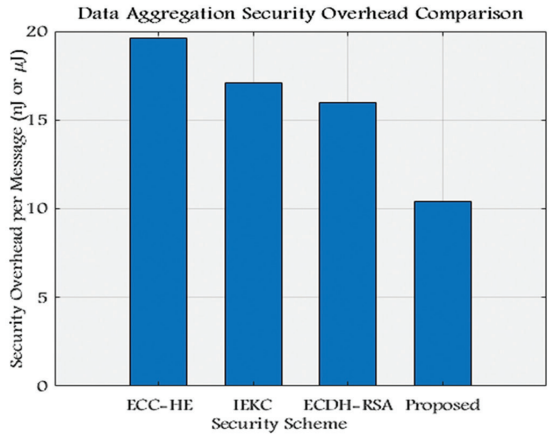

Fig. 6. Data Aggregation Security Overhead Components

The Fig. 6, integrates the security-processing terms and highlights their combined contribution to the overall secure-aggregation overhead, offering a concise visual summary of the protocol's security-related energy footprint.

4.5. COMPARATIVE EVALUATION FRAMEWORK

A single evaluation framework is used to conduct all routing and security schemes evaluated in this study to have a scientifically rigorous and unbiased comparison. The analysis represents the dualistic nature of the proposed solution-energy-efficient routing with the help of SMORP and secure data aggregation with the help of the IECC-ELGDS mechanism-and makes sure that the two are considered under the same identical and reproducible conditions. In the case of routing layer, SMORP has been compared to three of the well-known clustering based protocols: LEACH [10], SEP [11] and FSEP [12]. These baselines are heterogeneous-WSN fundamental routing methods, and employ similar radio-energy assumptions. The routing protocols are all carried out in the same deployment setting, initial energy distribution, transmission radii, and first-order radio parameters as in Sections 4.1 to 4.3. This ensures that performance difference is only due to behavior in an algorithm and not due to environmental variation. In case of the security layer, the IECC-ELGDS framework will be assessed on three exemplary examples of the cryptographic schemes that use the elliptic-curve: ECC-HE [13], IEKC [14] and ECDH-RSA [15]. These techniques are commonly used in the lightweight secure aggregation step and hence form the right baselines. Each security scheme uses the same message size, computation assumptions and traffic loads, which makes one directly compare the cost of encryption, signature-generation overhead, verification effort, and a general impact on network lifetime. Comparative analysis will be based on the standardized performance measures reported in section 4.4. such as network lifetime, residual-energy distribution, packet-delivery behavior, end-to-end delay and total security-processing overhead. The evaluation framework offers a clear and reproducible framework on isolating the actual performance contribution of the both SMORP routing and the IECC-ELGDS secure aggregation because all the simulated methods were fully parametrically consistent. Simulation environment, radio-energy model, parameter institution and evaluation metrics collectively provide a single and methodologically equal platform of assessment. Every routing and security plan has been implemented under exactly the same conditions in order to post fairness, transparency and reproducibility. Having this background, the following section forms the results of detailed performance and analysis of results and comparison of the performance between the proposed SMORP routing strategy and the IECC-ELGDS secure aggregation mechanism.

5. RESULT AND PERFORMANCE ANALYSIS

In this section, the performance outcomes of the recommended integrated framework are presented in the single simulation scenario that is described by Section 4. Each and every routing scheme and security scheme were tested under the same deployment conditions and radio-energy parameters in order to compare the schemes fairly. The evaluation is based on routing efficiency, energy behavior, delay behavior, packet-delivery reliability, and secure aggregation impact, which allow giving a clear understanding of the gains made by using SMORP routing along with the IECC-ELGDS security mechanism.

5.1. SMORP ROUTING PERFORMANCE

The proposed SMORP-based forwarding architecture is evaluated in terms of the routing throughput with three established clustering protocols: LEACH [10], FSEP [12], and SEP [11]. Each of the approaches has been implemented using the same simulation conditions and radio-energy parameters in order to make sure that the difference in the performance is due to the routing logic and not related to the environment itself. The assessment concerns three main metrics of routing effectiveness, namely network lifetime, residual-energy behavior and end-to-end delay.

5.1.1. Network Lifetime

Figs. 7 and 8 show the number of active L-sensor nodes and CHs over successive transmission rounds. SMORP demonstrates a substantially longer operational duration compared to LEACH, SEP, and FSEP.

Table 4. Number of rounds with the first dead node based on the four approaches

Approaches	LEACH	FSEP	SEP	SMORP
First dead L-sensor lifetime (Rounds)	176	293	—	975
First dead CHs Lifetime (Rounds)	—	—	377	1046

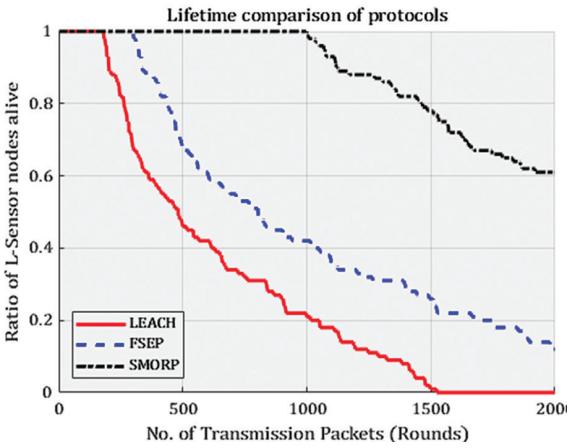

Fig. 7. Ratio of L-sensors still alive on different approaches (LEACH, FSEP, and proposed)

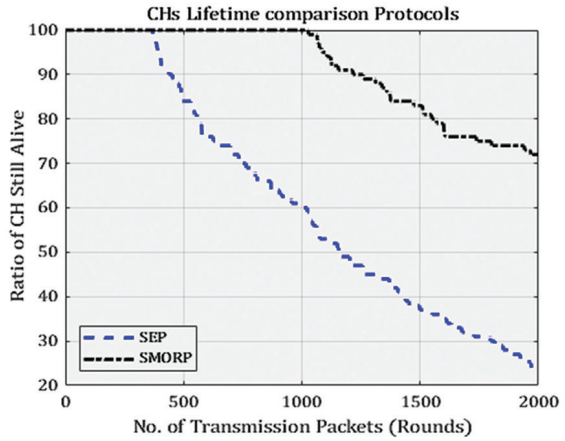

Fig. 8. Ratio of CHs still alive on different approaches (SEP, and proposed)

For L-sensors, the first node dies after 975 rounds, representing an improvement of approximately (+35% and +47%) over the approaches (FSEP and LEACH) respectively. For CHs, SMORP prolongs the first-dead-node lifetime by nearly 34% relative to SEP. These numerical results are summarized in Table 4 that obviously demonstrates that the proposed SMORP protocol provides the longest first-dead lifetime of all the considered strategies which proves its better capability to postpone the early failures of nodes and provide stable sensing coverage. These improvements directly align with the analytical formulations presented in Section 4. In particular, the prolonged survival time of SMORP nodes is explained by the radio-energy dissipation model (Eqs. (4)–(6)), where transmission cost grows quadratically with distance. Because SMORP continuously selects forwarding nodes with favorable spatial positions and sufficient residual energy according to the fitness and probability functions defined in Eqs. (1)–(3) the protocol naturally avoids high-cost transmissions and balances energy depletion across the network. This analytical grounding clarifies why SMORP maintains a larger population of active nodes across all rounds and achieves significantly longer network lifetime than LEACH, SEP, and FSEP.

Fig. 7 illustrates the ratio of active L-sensor nodes over the simulation rounds for the evaluated routing schemes. It can be observed that the proposed SMORP-based approach maintains a higher number of alive L-sensors compared to LEACH and FSEP throughout the network operation. This behavior indicates a more balanced energy consumption pattern, where forwarding and clustering decisions avoid overburdening individual nodes, thereby delaying early node failures and extending the stability period of the network.

5.1.2. Residual Energy Behavior

Figs. 9 and 10 illustrate the remaining energy ratio for L-sensors and CHs under the evaluated protocols. SMORP consistently maintains a higher residual-energy profile throughout the simulation.

This is attributed to:

- multi-hop forwarding guided by fitness-based decisions.
- adaptive subgroup organization.
- balanced load distribution between L-sensors and CHs.

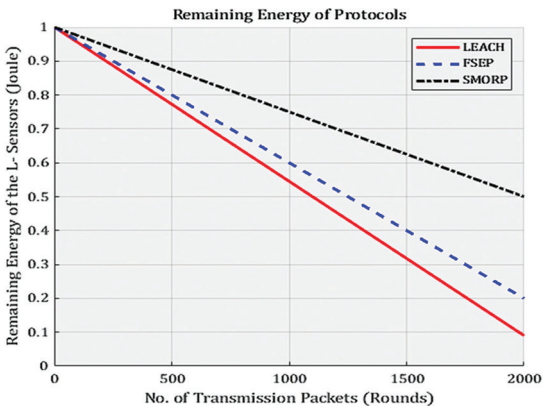

Fig. 9. Ratio remaining energy of L-sensors on different approaches (LEACH, FSEP, and proposed)

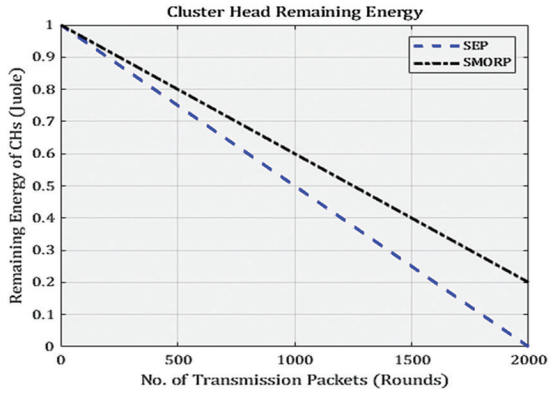

Fig. 10. Ratio remaining energy of H-sensors on the approaches (SEP, and proposed)

The results verify that SMORP achieves a more uniform energy-depletion pattern, preventing premature exhaustion of heavily loaded nodes and ensuring stable cluster performance.

Fig. 9 presents the remaining energy ratio of L-sensor nodes under different routing approaches. The proposed SMORP-based routing maintains a higher residual energy level throughout the simulation compared to LEACH and FSEP. This trend indicates that energy consumption is more evenly distributed among L-sensors, reducing excessive energy drain on individual nodes and supporting prolonged network operation.

5.1.3. End-to-End Delay and Transmission Efficiency

Figs. 11 and 12 demonstrate that SMORP significantly reduces simulation time and end-to-end delay compared to the baseline protocols.

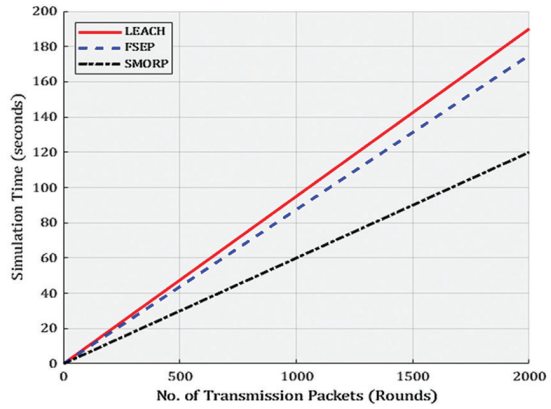

Fig. 11. Data transmission delay (simulation time for all packets) on different approaches (LEACH, FSEP, and proposed)

Packets experience fewer retransmissions and shorter forwarding paths due to:

- optimal next-hop selection via fitness evaluation.
- avoidance of overloaded or low-energy nodes.
- hierarchical pack-pointer–based path construction.

Lower delay directly translates to reduce per-packet energy expenditure, reinforcing the protocol's overall efficiency.

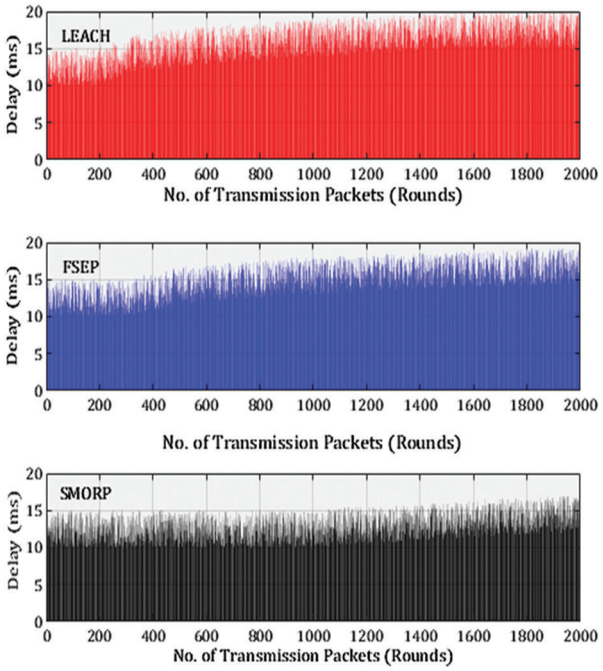

Fig. 12. Number of hops (end to end delay) on different approaches (LEACH, FSEP, and proposed)

5.1.4. Cluster Stability

Fig. 13 shows that SMORP preserves a near-optimal number of CHs over time, unlike LEACH and FSEP, which exhibit unstable CH formation patterns. Stable CH counts result in:

- predictable cluster structures.
- efficient aggregation.
- reduced control-message overhead.

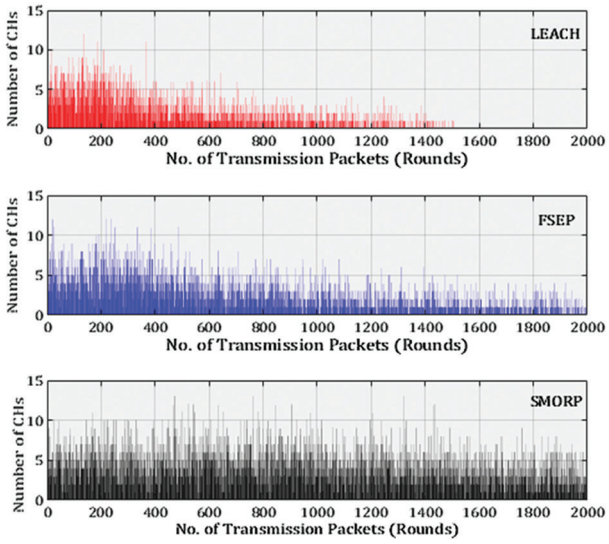

Fig. 13. Number of CHs on different approaches (LEACH, FSEP, and proposed)

5.1.5. Packet Delivery Dynamics

Figs. 14 and 15 indicate that SMORP achieves higher packet-delivery rates to both CHs and the sink. This reflects effective routing-path stability and reduced node failures, enabling reliable data flow across the network.

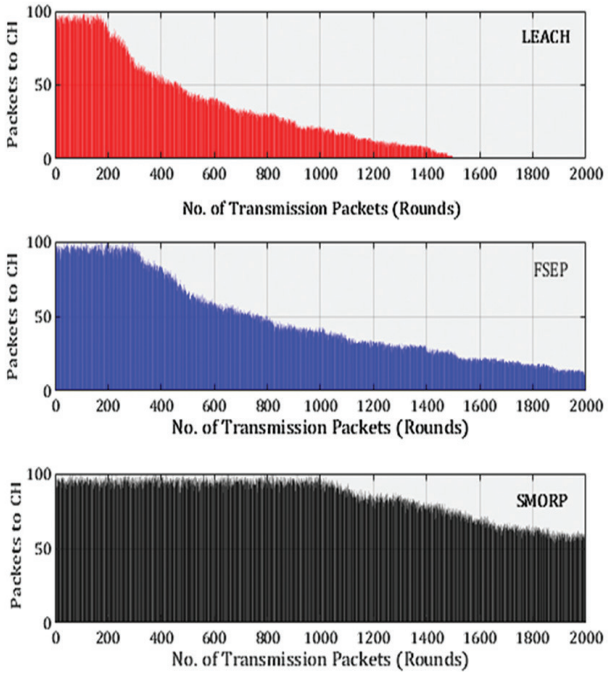

Fig. 14. Number of packets transmitted to CHs on different approaches (LEACH, FSEP, and proposed)

The collective results confirm that SMORP outperforms LEACH, SEP, and FSEP across all major routing-performance metrics. Its hierarchical leader-coordination, fitness-based next-hop evaluation, and balanced energy exploitation significantly enhance network lifetime, stability, and data-delivery reliability.

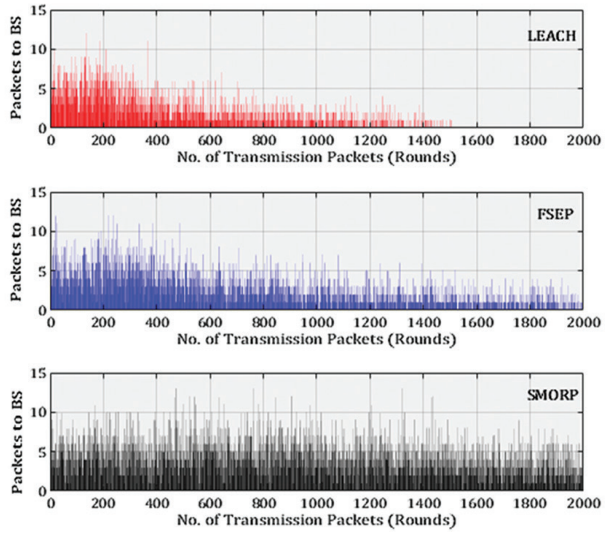

Fig. 15. Number of packets transmitted to BS on different approaches (LEACH, FSEP, and proposed)

5.2. IECC–ELGDS SECURITY PERFORMANCE

The effectiveness of the proposed IECC–ELGDS security mechanism is evaluated by comparing it with three well-known elliptic-curve-based security schemes: ECC-HE[13], IEKC [14], and ECDH-RSA [15]. All approaches were executed under identical simulation conditions, traffic load, aggregation structure, and cryptographic assumptions to ensure that performance differences arise solely from each method's security-processing efficiency. The evaluation focuses on four primary indicators: secure network lifetime, residual energy sustainability, encryption/decryption computational cost, and packet-delivery behavior under secure transmission.

5.2.1. Secure Network Lifetime

Fig. 16 shows the number of active sensor nodes under each security scheme. The proposed IECC–ELGDS mechanism maintains a significantly larger population of active nodes across all simulation rounds. The lifetime of the first-dead-node of the proposed method is 1223 rounds; this improvement is about (+44%), (+39%), and (+28%) over ECC-HE, IEKC, and ECDH-RSA. This finding, summarized in Table 5, affirms that both the lightweight Ness of the scalar- multiplication of the IECC and the lower computational intensity of ELGDS reduce security overheads and prevent node death alike.

Table 5. Number of rounds with the first dead node based on the four approaches

Approaches	ECC-HE	IEKC	ECDH-RSA	Proposed
First dead Lifetime (rounds)	342	451	659	1223

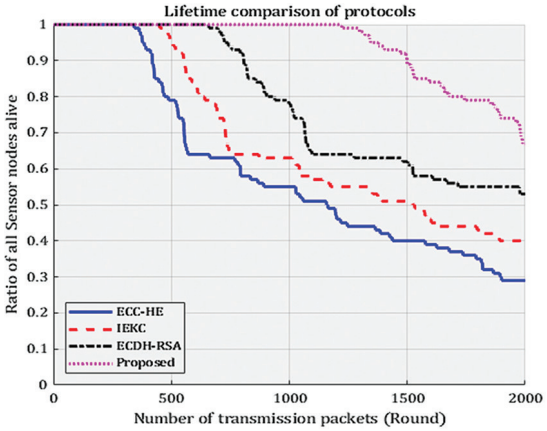

Fig. 16. Ratio of all sensor nodes still alive on different approaches (ECC-HE, IEKC, ECDH-RSA, and proposed)

5.2.2. Residual Energy Behavior Under Secure Processing

The residual energy trajectory, presented in Fig. 17, demonstrates that IECC–ELGDS preserves energy more effectively than the benchmark schemes.

ECC-HE and ECDH-RSA incur substantially higher cryptographic costs due to their use of homomorphic.

Fig. 16 shows the proportion of sensor nodes remaining alive under different security mechanisms. The proposed IECC–ELGDS scheme sustains a larger number of active nodes over the simulation rounds compared to ECC-HE, IEKC, and ECDH-RSA. This outcome reflects the reduced computational and energy overhead of the proposed security design, which limits premature energy depletion caused by cryptographic operations. Conversely, the optimized elliptic-curve

operations in IECC, combined with the single-round signature generation of ELGDS, reduce the per-packet cryptographic burden. This efficient processing yields a smoother energy-decline pattern and delays the onset of critical-energy states across sensor nodes.

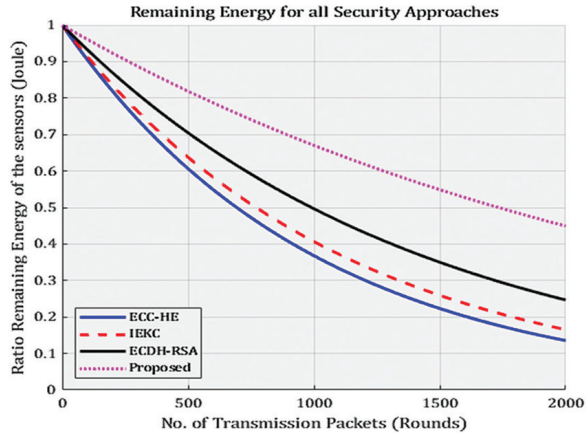

Fig. 17. Ratio remaining energy of all sensor nodes on different approaches (ECC-HE, IEKC, ECDH-RSA, and proposed)

5.2.3. Encryption/Decryption Cost Analysis

Fig. 18 compares the computational cost associated with ciphertext generation and recovery. The proposed IECC–ELGDS method consistently achieves the smallest processing cost for all evaluated data sizes. The improved ECC scalar multiplication in IECC and the two-step linear-modular computation of ELGDS require fewer arithmetic operations per message than the multi-layer encrypt–aggregate–decrypt structure used in ECC-HE and the RSA-based verification in ECDH-RSA. This lightweight operation significantly lowers both encryption and decryption delays, enabling faster secure forwarding and reduced energy expenditure.

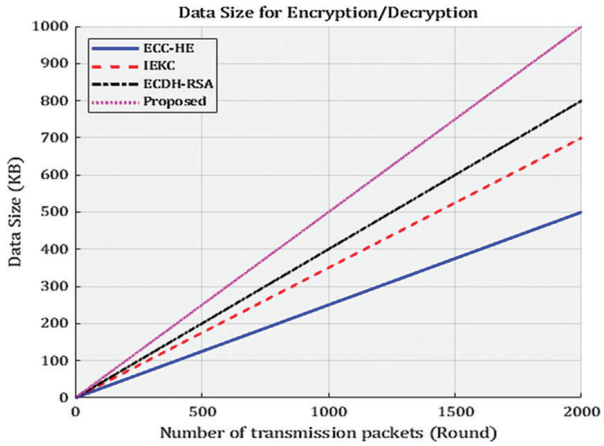

Fig. 18. Data Size for Encryption / Decryption on different approaches (ECC-HE, IEKC, ECDH-RSA, and proposed)

Fig. 18 compares the encryption and decryption cost of different security schemes. The proposed IECC–ELGDS approach exhibits lower computational overhead than ECC-HE and ECDH-RSA due to lightweight elliptic-curve operations and reduced cryptographic processing.

5.2.4. Secure Packet-Delivery Characteristics

Fig. 19 presents the secure packet-delivery time for all approaches. The IECC–ELGDS mechanism demonstrates the shortest end-to-end secure transmission delay, attributable to two primary factors:

1. Intermediate nodes forward ciphertext without decryption, eliminating the overhead associated with hop-by-hop key operations.
2. Signature verification is restricted to the sink, reducing per-hop processing costs and mitigating congestion on forwarding nodes.

Consequently, the suggested approach will have a better delivery ratio even under conditions of multipath forwarding. The level of packet-delivery is always higher as it is impossible to conduct opportunistic manipulation: ciphertext aggregation into CH prevents the exposure of plaintexts, whereas ELGDS authentication precludes replay, impersonation, and other forgery. Across all performance indicators—energy sustainability, secure lifetime, processing cost, and secure delivery behavior—the **IECC–ELGDS** framework consistently outperforms existing ECC-based security schemes. These results validate that the combined lightweight elliptic-curve encryption and efficient digital-signature generation deliver strong confidentiality and authentication guarantees while preserving network longevity in heterogeneous WSN environments.

5.3. COMPARATIVE DISCUSSION

Section 5.1 results, together with those in 5.2, reveal that the suggested system is able to simultaneously enhance the routing efficiency and secure data aggregation two notions that are usually at odds in resource-limited wireless sensor networks.

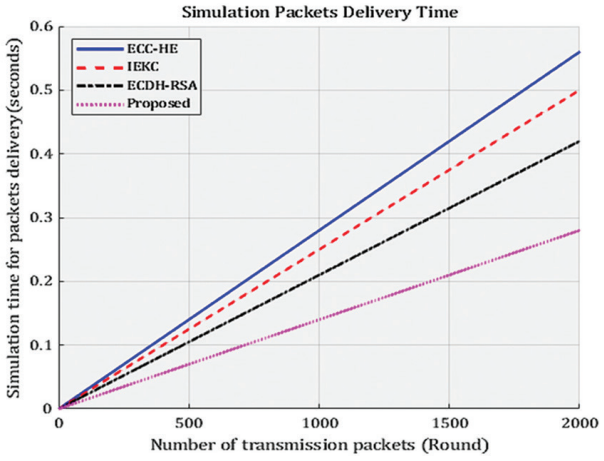

Fig. 19. Simulation Packets Delivery Time on different approaches (ECC-HE, IEKC, ECDH-RSA, and proposed)

Compared with the previous strategy of using idle routes to balance the end-to-end delay, SMORP-based routing strategy offers a longer lifetime of operation as indicated by the long first-dead-node intervals and clearer residual-energy curves in Figs. 7-14. At the same time, the IECC-ELGDS security layer can provide a high grade of confidentiality, as well as authentication assurances without impacting the energy-awareness of the underlying routing structure, which is

superior to ECC-HE, IEKC, and ECDH-RSA in all the security-related metrics than in Figs. 16-19. Of critical observation is the fact that the implementation of SMORP and IECC-ELGDS does not present a harmful trade-off between the performance and security- a problem that is common in the context of WSNs. Rather, the energy and computational cost of the secure protocols is significantly lowered by the lightweight elliptic-curve encryption and single round ElGamal signature generation. This compression makes SMORP retain its routing performance even as they operate in the secure mode, and the network can deliver a high ratio of packets and less latency than traditional schemes. Moreover, the suggested system makes sure that the aggregation of ciphertext at CHs is non-decrypted so that no data loss at intermediary nodes can be realized, not to create bottlenecks in cryptography. This design means that the multi-hop forwarding paths can have low levels of congestion, which combined with the delay performance shown in Fig. 12 and Fig. 19 increase concurrently. The overall gains, backed with the performances in Tables 3 and 4, prove the fact that the suggested integration is no longer than the sum of two mechanisms but an integrated structure in which routing intelligence and lightweight security improve one another. In general, the comparative results demonstrate that the presented framework of the SMORP-IECC-ELGDS approach provides a balanced and scalable solution that could be used to maintain the secure and energy-efficient functioning throughout the period of network existence. This twin improvement denotes the appropriateness of this proposed model to the scenario of heterogeneous sensing surroundings that are high reliability and high security warranties.

5.4. OVERALL INTERPRETATION

The combined experimental results which are obtained indicate that a balanced improvement in both energy conservation as well as safe data aggregation-two goals which generally clash in heterogeneous WSNs is realized when SMORP routing is integrated with the IECC-ELGDS security framework. SMORP tremendously enhances stabilization of routing, balances energy loss and prolongs the life of both L-sensor nodes and CHs and the IECC-ELGDS mechanism presents high level of confidentiality and authentication with low level of computer calculations. The joint effect of the optimization-based routing behavior and the lightweight elliptic-curve cryptography is in facilitating security in communication without negatively impacting network responsiveness or delay. The profile of the overall performance shows that despite the severe energy and security conditions, the proposed architecture is stable and proves its applicability to the long-term sensing applications in the heterogeneous environment with resource restrictions.

6. CONCLUSION

The obtained simulation results confirm that the proposed SMORP–IECC–ELGDS framework improves network lifetime, energy distribution, and security efficiency when compared with existing routing and cryptographic schemes. This paper presented a combined architecture that takes the SMORP complimentary routing protocol founded on optimization and the IECC-ELGDS delicate security tool to handle the two fold difficulty in terms of energy conservation as well as safe mantle of data accumulation within a heterogeneous wireless sensor network. The proposed architecture can improve the stability of clustering, load balancing through forwarding, and end-to-end confidentiality and authentication without causing too much load on the resource-limited nodes. The experimental findings illustrate a evident improvement in performance: SMORP allows increasing the first-dead-node lifetime of L-sensors and CHs by up to 47 and 34 percent respectively in comparison to LEACH, FSEP, and SEP, whereas the scheme of IECC-ELGDS can enhance the length of the safe network by a factor of 28-44 percent relative to ECC-HE, IEKC, and ECDH-RSA. Such enhancements verify the supportability of the integration of optimization-based routing and lightweight elliptic-curve security. In spite of the fact that the estimation is based on the simulation analysis and presupposes that the nodes remain still with an idealized behavior of the channels, the real-hardware validation, the adversarial attack models, and the scenarios of dynamic networks are to be included in the range of the future work to assess scalability and resilience further. Future work may consider extending the proposed framework to dynamic network scenarios, incorporating mobile sinks, and evaluating performance under realistic channel and attack models.

7. REFERENCES

[1] L.-L. Hung, F.-Y. Leu, K.-L. Tsai, C.-Y. Ko, "Energy-efficient cooperative routing scheme for heterogeneous wireless sensor networks", IEEE Access, Vol. 8, 2020, pp. 56321-56332.

[2] H. Qabouche, A. Sahel, A. Badri, "Hybrid energy efficient static routing protocol for homogeneous and heterogeneous large scale WSN", Wireless Networks, Vol. 27, No. 1, 2021, pp. 575-587.

[3] S. K. Chaurasiya, S. Mondal, A. Biswas, A. Nayyar, M. A. Shah, R. Banerjee, "An energy-efficient hybrid clustering technique (EEHCT) for IoT-based multilevel heterogeneous wireless sensor networks", IEEE Access, Vol. 11, 2023, pp. 25941-25958.

[4] U. Chatterjee, S. Ray, M. K. Khan, M. Dasgupta, C.-M. Chen, "An ECC-based lightweight remote user authentication and key management scheme for IoT communication in context of fog computing", Computing, Vol. 104, No. 6, 2022, pp. 1359-1395.

[5] S. X. Pushpa, S. K. S. Raja, "Enhanced ECC based authentication protocol in wireless sensor network with DoS mitigation", Cybernetics and Systems, Vol. 53, No. 8, 2022, pp. 734-755.

[6] S. Hu, L. Liu, L. Fang, F. Zhou, R. Ye, "A novel energy-efficient and privacy-preserving data aggregation for WSNs", IEEE Access, Vol. 8, 2019, pp. 802-813.

[7] M. A. Khan, M. T. Quasim, N. S. Alghamdi, M. Y. Khan, "A secure framework for authentication and encryption using improved ECC for IoT-based medical sensor data", IEEE Access, Vol. 8, 2020, pp. 52018-52027.

[8] H. Y. Adarbah, M. F. Moghadam, R. L. R. Maata, A. Mohajerzadeh, A. H. Al-Badi, "Security challenges of selective forwarding attack and design a secure ECDH-based authentication protocol to improve RPL security", IEEE Access, Vol. 11, 2022, pp. 11268-11280.

[9] X. Yang *et al*. "Blockchain-based secure and lightweight authentication for Internet of Things", IEEE Internet of Things Journal, Vol. 9, No. 5, 2021, pp. 3321-3332.

[10] W. B. Heinzelman, A. P. Chandrakasan, H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks", IEEE Transactions on Wireless Communications, Vol. 1, No. 4, 2002, pp. 660-670.

[11] G. Smaragdakis, I. Matta, A. Bestavros, "SEP: A stable election protocol for clustered heterogeneous wireless sensor networks", Boston University, Computer Science Department, Boston, MA, USA, 2004.

[12] A. Ali *et al*. "Enhanced fuzzy logic zone stable election protocol for cluster head election (E-FLZSEPFCH) and multipath routing in wireless sensor networks", Ain Shams Engineering Journal, Vol. 15, No. 2, 2024, p. 102356.

[13] M. Elhoseny, H. Elminir, A. Riad, X. Yuan, "A secure data routing schema for WSN using elliptic curve cryptography and homomorphic encryption", Journal of King Saud University-Computer and Information Sciences, Vol. 28, No. 3, 2016, pp. 262-275.

[14] P. Ramadevi, S. Ayyasamy, Y. Suryaprakash, C. Anilkumar, S. Vijayakumar, R. Sudha, "Security for wireless sensor networks using cryptography", Measurement: Sensors, Vol. 29, 2023, p. 100874.

[15] B. Abood, A. N. Faisal, Q. A. Hamed, "Data transmitted encryption for clustering protocol in heterogeneous wireless sensor networks", Indonesian Journal of Electrical Engineering and Computer Science, Vol. 25, No. 1, 2022, pp. 347-357.

[16] A. H. Jabbar, I. S. Alshawi, "Spider monkey optimization routing protocol for wireless sensor networks", International Journal of Electrical & Computer Engineering, Vol. 11, No. 3, 2021, pp. 2432-2442.

[17] G. Muneeswari, A. Ahilan, R. Rajeshwari, K. Kannan, C. J. C. Singh, "Trust and energy-aware routing protocol for wireless sensor networks based on secure routing", International Journal of Electrical and Computer Engineering Systems, Vol. 14, No. 9, 2023, pp. 1015-1022.

[18] S. Balan, D. Champla, M. Pushpavalli, A. Ahilan, "Energy Efficient Multi-hop routing scheme using Taylor based Gravitational Search Algorithm in Wireless Sensor Networks", International Journal of Electrical and Computer Engineering Systems, Vol. 14, No. 3, 2023, pp. 333-343.

[19] V. Lekshmi, "Increasing efficiency and reliability in multicast routing based V2V communication for direction-aware cooperative collision avoidance", International Journal of Electrical and Computer Engineering Systems, Vol. 15, No. 2, 2024, pp. 145-153.

[20] M. Rami Reddy, M. Ravi Chandra, P. Venkatramana, R. Dilli, "Energy-efficient cluster head selection in wireless sensor networks using an improved grey wolf optimization algorithm", Computers, Vol. 12, No. 2, 2023, p. 35.

[21] F. Jibreel, E. Tuyishimire, M. I. Daabo, "An enhanced heterogeneous gateway-based energy-aware multi-hop routing protocol for wireless sensor networks", Information, Vol. 13, No. 4, 2022, p. 166.

[22] S. Tabatabaei, "Provide energy-aware routing protocol in wireless sensor networks using bacterial foraging optimization algorithm and mobile sink", Plos one, Vol. 17, No. 3, 2022, p. e0265113.

[23] B. Hammi, A. Fayad, R. Khatoun, S. Zeadally, Y. Begriche, "A lightweight ECC-based authentication scheme for Internet of Things (IoT)", IEEE Systems Journal, Vol. 14, No. 3, 2020, pp. 3440-3450.

[24] N. Mahlake, T. E. Mathonsi, D. Du Plessis, T. Muchenje, "A Lightweight Encryption Algorithm to Enhance Wireless Sensor Network Security on the Internet of Things", Journal of Communications, Vol. 18, No. 1, 2023, pp. 47-57.

[25] H. Bashirpour, S. Bashirpour, S. Shamshirband, A. T. Chronopoulos, "An improved digital signature protocol to multi-user broadcast authentication based on elliptic curve cryptography in wireless sensor networks (WSNS)", Mathematical and Computational Applications, Vol. 23, No. 2, 2018, p. 17.

[26] B. R. Rao, B. Sujatha, "A hybrid elliptic curve cryptography (HECC) technique for fast encryption of data for public cloud security", Measurement: Sensors, Vol. 29, 2023, p. 100870.

[27] I. Ahmad *et al*. "Adaptive and Priority-Based Data Aggregation and Scheduling Model for Wireless Sensor Network", Knowledge-Based Systems, Vol. 303, 2024, p. 112393.

[28] X. Liu, J. Yu, K. Yu, G. Wang, X. Feng, "Trust secure data aggregation in WSN-based IIoT with single mobile sink", Ad Hoc Networks, Vol. 136, 2022, p. 102956.