International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(2) 2026 pp. 1672-1694
https://doi.org/10.70917/ijcisim-2026-4762
Article

Hybrid ECC-ASCON Security Framework-based Lightweight Encryption Model for Improving Security in WSN

Libi Kurian [1], P Sumitra [2]

[1] Department of Computer Science and Applications, Vivekanandha College of Arts and Sciences for Women, Tamil Nadu, India.
[2] Department of Computer Science, PSGR Krishnammal College for Women, Tamil Nadu, India
Corresponding Author: libi.kurian@yahoo.com

Abstract: Wireless Sensor Networks (WSNs) deployed in Internet of Things (IoT) environments require communication mechanisms that ensure robust security while operating within stringent computational, memory, and energy constraints. Conventional cryptographic techniques often impose considerable processing overhead, limiting their suitability for resource-constrained sensor nodes. This paper proposes a hybrid lightweight security framework that integrates Advanced LEACH-based clustering, Elliptic Curve Cryptography (ECC), Elliptic Curve Diffie–Hellman (ECDH) key establishment, HKDF-SHA256 key derivation, and ASCON-AEAD128 authenticated encryption to achieve secure and energy-efficient data communication in WSNs. In the proposed framework, ECDH establishes a shared secret between communicating nodes, which is transformed into a 128-bit symmetric session key using HKDF-SHA256. The derived session key is subsequently employed by ASCON-AEAD128 to provide authenticated encryption, thereby ensuring data confidentiality, integrity, and authenticity with minimal computational overhead. To further enhance network sustainability, an energy-aware dynamic key rotation mechanism is introduced that adapts key updates according to residual node energy and communication requirements, thereby maintaining key freshness while minimizing unnecessary rekeying operations. The proposed framework was implemented using Python and evaluated through NS-3 simulations with packet payloads extracted from PCAP traces to emulate realistic WSN communication scenarios. Experimental results demonstrate that the framework consistently achieves a Packet Delivery Ratio (PDR) of approximately 98%, maintains an average key expansion time of approximately 29 ms for 256-bit key generation, and limits average energy consumption to nearly 247 µJ across network sizes ranging from 10 to 100 sensor nodes. The findings demonstrate that the proposed framework effectively combines lightweight authenticated encryption, secure key management, and energy-aware communication to provide reliable, scalable, and computationally efficient security for IoT-enabled Wireless Sensor Networks.
***Keywords*:** Wireless Sensor Networks, Internet of Things, Advanced LEACH, Elliptic Curve Cryptography, Elliptic Curve Diffie–Hellman, HKDF-SHA256; ASCON-AEAD128, Lightweight Authenticated Encryption, Energy-Aware Key Management**.**

1. Introduction

A. Background and Motivation

Wireless Sensor Networks (WSNs) have emerged as a fundamental communication technology for the Internet of Things (IoT), enabling distributed sensing, continuous monitoring, and intelligent data collection across a wide range of application domains, including environmental surveillance, industrial automation, precision agriculture, healthcare monitoring, and smart city infrastructures [1]. A typical WSN consists of numerous sensor nodes equipped with sensing, processing, and wireless communication capabilities that collaboratively monitor physical or environmental parameters such as temperature, humidity, pressure, vibration, and motion. The sensed information is transmitted to cluster heads, where data aggregation and preliminary processing are performed before forwarding the information to a base station. The base station subsequently relays the collected data to cloud platforms or IoT services for storage, analytics, visualization, and decision-making, thereby enabling efficient management of large-scale distributed sensing environments [2].

The rapid growth of IoT-enabled WSN deployments has significantly increased the demand for reliable and secure wireless communication. Since sensor nodes are commonly deployed in unattended or hostile environments and communicate through open wireless channels, they are highly vulnerable to a wide range of security threats. Adversaries may exploit these vulnerabilities through eavesdropping, replay attacks, node

impersonation, sinkhole attacks, wormhole attacks, Sybil attacks, selective forwarding, and denial-of-service attacks, potentially compromising data confidentiality, communication integrity, network availability, and the overall reliability of IoT services [3]. Consequently, ensuring secure communication has become a critical requirement for maintaining the trustworthiness of WSN-based IoT applications. A secure communication framework must therefore preserve confidentiality, integrity, authenticity, availability, and data freshness while simultaneously supporting uninterrupted network operation under resource-constrained conditions [4].

Despite their broad applicability, sensor nodes operate under stringent resource limitations, including restricted computational capability, limited memory capacity, finite battery energy, and low communication bandwidth. These constraints present significant challenges when implementing conventional cryptographic algorithms that often require computationally intensive key management procedures, multiple encryption rounds, and substantial processing resources. Although classical cryptographic architectures based on Feistel networks and Substitution–Permutation Networks (SPNs) provide robust security, their computational complexity and energy requirements may adversely affect network lifetime and communication efficiency in resource-constrained WSN environments [5]. Consequently, lightweight cryptographic techniques have gained considerable attention as they are specifically designed to provide strong security guarantees while minimizing computational overhead, memory utilization, and energy consumption, making them more suitable for IoT-enabled sensor networks [6].

In addition to lightweight encryption, efficient routing and network organization play an equally important role in extending the operational lifetime of WSNs. Clustering-based communication protocols have been widely adopted to reduce redundant data transmission, improve scalability, and distribute communication loads among sensor nodes. Among these protocols, the Low-Energy Adaptive Clustering Hierarchy (LEACH) has been extensively employed because of its distributed cluster-head rotation mechanism, which effectively balances communication energy across the network. However, conventional LEACH primarily relies on probabilistic cluster-head selection and does not adequately consider multiple node characteristics, such as residual energy, communication distance, and node distribution, which may result in uneven energy consumption and reduced network lifetime [7]. Recent studies have therefore emphasized the importance of developing enhanced clustering strategies that improve energy utilization while maintaining reliable and secure communication in increasingly complex IoT environments [8].

Recent advances in lightweight cryptography have further demonstrated that secure communication in resource-constrained environments can be strengthened by integrating efficient public-key cryptography with lightweight authenticated encryption mechanisms. Elliptic Curve Diffie–Hellman (ECDH) provides an efficient approach for establishing secure shared secrets with significantly lower computational complexity than conventional public-key algorithms, making it well suited for constrained IoT devices [9]. Similarly, modern lightweight authenticated encryption algorithms provide confidentiality, integrity, and authentication within a unified cryptographic framework while reducing computational and communication overhead [10]. These developments highlight the growing need for integrated communication frameworks that jointly address secure key establishment, lightweight authenticated encryption, efficient key management, and energy-aware communication to support reliable and sustainable Wireless Sensor Networks in modern IoT applications.

B. Research Challenges

Using the revised reference numbering, the numeric citations in this paragraph should be retained as follows:

The rapid expansion of Internet of Things (IoT) applications has substantially increased the scale, complexity, and heterogeneity of Wireless Sensor Networks (WSNs), making secure and energy-efficient communication an increasingly difficult objective to achieve. Although significant advances have been made in clustering protocols, lightweight cryptography, and secure routing mechanisms, designing an integrated framework that simultaneously satisfies stringent security requirements and severe resource constraints remains a major research challenge. The limited computational capability, memory capacity, communication bandwidth, and battery resources of sensor nodes impose strict constraints on the selection of security mechanisms, requiring an appropriate balance between cryptographic strength, communication efficiency, and network lifetime [11].

One of the primary challenges in WSN security is the establishment and maintenance of secure cryptographic keys. Traditional public-key cryptographic algorithms provide robust security but generally require substantial computational resources and communication overhead, making them unsuitable for many resource-constrained sensor platforms. Although Elliptic Curve Cryptography (ECC) significantly reduces key sizes and computational complexity compared with conventional public-key algorithms, efficient session key establishment and secure key management remain challenging in dynamic WSN environments where sensor nodes frequently experience topology changes, energy depletion, and intermittent communication [20].

Furthermore, repeatedly performing key establishment operations may increase computational cost and accelerate battery depletion, particularly in large-scale sensor deployments.

Another important challenge involves preserving communication security while minimizing computational overhead. Conventional encryption techniques often employ separate mechanisms for encryption, authentication, and integrity verification, increasing both processing time and communication overhead. Recent lightweight authenticated encryption algorithms have demonstrated considerable improvements in reducing computational complexity; however, many existing implementations primarily emphasize cryptographic performance while giving limited attention to their integration with energy-aware routing and adaptive key management strategies required for practical WSN deployments [8]. Consequently, maintaining strong security without adversely affecting communication latency or network lifetime continues to represent a significant design challenge.

Efficient clustering and routing also remain critical factors influencing the overall performance of WSNs. Clustering protocols such as LEACH have been widely adopted to distribute communication loads and reduce energy consumption through periodic cluster-head rotation. Nevertheless, conventional LEACH primarily relies on probabilistic cluster-head selection and does not comprehensively consider factors such as residual node energy, communication distance, node distribution, and network conditions during cluster formation. This limitation may result in uneven energy consumption, premature cluster-head failure, reduced packet delivery performance, and shorter network lifetime, particularly in dense or dynamically changing IoT environments [15]. Therefore, improving cluster-head selection while simultaneously incorporating secure communication mechanisms remains an important research challenge.

Maintaining long-term communication security introduces an additional challenge associated with cryptographic key freshness. Static session keys increase the risk of prolonged key exposure if a node is compromised, whereas excessively frequent rekeying introduces unnecessary communication overhead and additional energy consumption. Designing adaptive key management mechanisms that preserve forward secrecy and periodically refresh cryptographic keys according to network conditions and residual node energy therefore represents an important requirement for achieving both communication security and energy efficiency in resource-constrained WSNs [14].

Finally, the growing diversity of IoT applications demands security frameworks that remain scalable as network size increases while maintaining consistent communication performance. Many existing studies evaluate secure communication using relatively small network configurations or focus primarily on cryptographic efficiency without fully considering the combined influence of clustering efficiency, secure key establishment, authenticated encryption, and adaptive key management on overall network performance. Developing an integrated communication framework capable of balancing these interdependent requirements therefore remains a fundamental challenge for modern Wireless Sensor Networks operating in resource-constrained IoT environments [16].

C. Research Gap and Novel Contributions

Recent advances in Wireless Sensor Networks (WSNs) have produced considerable progress in clustering protocols, lightweight cryptography, and secure communication mechanisms. Existing studies have proposed various approaches that independently improve cluster-head selection, lightweight encryption, key establishment, or authentication for resource-constrained IoT environments [12]. Similarly, several hybrid cryptographic frameworks have combined public-key and symmetric-key algorithms to strengthen communication security while reducing computational overhead [13]. More recently, lightweight authenticated encryption algorithms have emerged as promising solutions for securing constrained devices because they simultaneously provide confidentiality, integrity, and authentication with lower resource requirements than conventional cryptographic techniques [10].

Despite these developments, several important research limitations remain unresolved. Many clustering-based security frameworks primarily focus on improving routing efficiency without incorporating modern authenticated encryption and adaptive cryptographic key management into the communication process [7]. Conversely, numerous lightweight cryptographic solutions concentrate on reducing encryption overhead but do not explicitly consider energy-aware routing, cluster-head optimization, or the dynamic operational characteristics of WSNs [6]. Existing ECC-based communication frameworks generally provide efficient key establishment; however, they frequently employ static or fixed key management strategies that may increase the risk of long-term key exposure or introduce unnecessary communication overhead when periodic key updates are performed without considering network conditions or residual node energy [9]. Consequently, most existing approaches optimize individual components of secure communication rather than providing a unified framework

that jointly addresses clustering efficiency, lightweight authenticated encryption, secure session key establishment, adaptive key management, and energy-aware communication.

To address these limitations, this research develops an integrated lightweight security framework that combines communication efficiency and cryptographic protection within a unified architecture. The proposed framework employs an enhanced LEACH-based clustering mechanism to improve energy-aware cluster-head selection, thereby reducing communication overhead and balancing energy consumption among sensor nodes. Secure session key establishment is achieved using Elliptic Curve Diffie–Hellman (ECDH), while HKDF-SHA256 derives high-entropy symmetric session keys from the shared secret before authenticated encryption is performed using the ASCON-AEAD128 algorithm. In contrast to conventional approaches that rely on static rekeying intervals, the proposed framework incorporates an energy-aware dynamic key rotation mechanism that adapts key updates according to residual node energy and communication conditions. This strategy maintains key freshness and forward secrecy while minimizing unnecessary rekeying operations that could otherwise reduce network lifetime.

Accordingly, the principal contributions of this research are summarized as follows:

- Development of an enhanced energy-aware communication framework that integrates Advanced LEACH clustering with secure cryptographic communication to improve routing efficiency and balance energy consumption across Wireless Sensor Networks.
- Integration of an efficient hybrid key management mechanism in which Elliptic Curve Diffie–Hellman establishes a secure shared secret and HKDF-SHA256 derives a high-entropy symmetric session key suitable for lightweight authenticated encryption in resource-constrained sensor nodes.
- Deployment of ASCON-AEAD128 authenticated encryption to simultaneously provide confidentiality, integrity, and message authentication while maintaining low computational and communication overhead suitable for IoT-enabled WSN environments.
- Introduction of an adaptive energy-aware dynamic key rotation mechanism that updates cryptographic session keys according to residual node energy and communication requirements, thereby preserving key freshness and forward secrecy while reducing unnecessary rekeying overhead.
- Comprehensive implementation and performance evaluation using NS-3 and Python-based simulations with realistic packet communication scenarios to assess packet delivery performance, key expansion efficiency, and energy consumption in comparison with representative lightweight cryptographic approaches.

The proposed framework therefore contributes a practical integration of energy-aware clustering, lightweight authenticated encryption, efficient session key establishment, and adaptive key management into a unified communication architecture designed specifically for resource-constrained Wireless Sensor Networks. Rather than introducing a new cryptographic primitive, the novelty of this work lies in the coordinated integration and optimization of these complementary components to achieve secure, energy-efficient, and scalable communication for modern IoT applications.

D. Organization of the Paper

The remainder of this paper is organized as follows. Section 2 presents a comprehensive review of the existing literature on Wireless Sensor Network security, lightweight cryptographic techniques, clustering mechanisms, and secure communication frameworks, followed by the identification of the research gap addressed in this study. Section 3 describes the proposed hybrid lightweight security framework, including the Advanced LEACH-based clustering mechanism, the ECC-ECDH key establishment process, the HKDF-SHA256 session key derivation procedure, the ASCON-AEAD128 authenticated encryption mechanism, and the energy-aware dynamic key rotation strategy. Section 4 presents the experimental setup, implementation details, performance evaluation metrics, and comparative analysis, together with a detailed discussion of the obtained results. Finally, Section 5 summarizes the major findings of the study, highlights the contributions and limitations of the proposed framework, and outlines potential directions for future research.

2. Literature Review

A. Lightweight Cryptographic Frameworks for Wireless Sensor Networks

The growing adoption of Wireless Sensor Networks (WSNs) within Internet of Things (IoT) applications has intensified the need for cryptographic mechanisms that can provide strong communication security while operating within stringent resource constraints. Unlike conventional computing systems, sensor nodes possess limited processing capability, memory, communication bandwidth, and battery capacity, making the deployment

of computationally intensive cryptographic algorithms impractical for long-term operation. Consequently, lightweight cryptography has emerged as an effective approach for securing WSN communications by reducing computational complexity, memory requirements, and energy consumption without compromising essential security properties such as confidentiality, integrity, and authentication [6].

Recent studies have demonstrated that lightweight cryptographic techniques provide an effective balance between security and resource efficiency for constrained IoT devices. Kaur *et al.* [6] emphasized that modern lightweight cryptographic algorithms are specifically designed to address the limitations of conventional encryption techniques by reducing processing overhead while maintaining an acceptable level of cryptographic strength. Their study highlighted the increasing importance of lightweight security mechanisms for resource-constrained environments such as WSNs, IoT devices, and cyber-physical systems. However, the review primarily focused on algorithmic performance and provided limited discussion regarding the integration of lightweight encryption with adaptive communication protocols and energy-aware network management.

Hybrid cryptographic approaches have also been investigated to enhance communication security by combining the advantages of multiple encryption paradigms. Tripathy *et al.* [13] introduced a Hybrid Encryption Technique (HET) that integrates Elliptic Curve Cryptography (ECC) with Lempel–Ziv–Welch (LZW) compression to improve data confidentiality while reducing ciphertext size. The proposed framework demonstrated improved authentication and secure data transmission with relatively low computational complexity. Nevertheless, the study did not evaluate the energy consumption associated with repeated cryptographic operations, leaving uncertainties regarding its suitability for long-term deployment in battery-powered Wireless Sensor Networks.

To enhance secure data sharing in distributed IoT environments, Karunkuzhali *et al.* [16] proposed a lightweight attribute-based encryption framework capable of supporting expressive access control, dynamic policy updates, and white-box traceability. Although the proposed framework improved flexible access management, its computational complexity increases with frequent attribute updates and key exchanges, potentially introducing additional communication latency in large-scale sensor deployments. Furthermore, the study did not investigate adaptive energy management strategies that are essential for extending network lifetime in resource-constrained WSN environments.

Systematic investigations into lightweight cryptographic techniques have further confirmed their significance for modern IoT security. Ansari and Ali [10] reviewed a wide range of lightweight cryptographic schemes and concluded that lightweight authenticated encryption has become increasingly important for protecting constrained devices against evolving cyber threats while minimizing computational overhead. Despite the considerable progress achieved by existing lightweight algorithms, the review identified efficient key management, adaptive security mechanisms, and practical deployment in heterogeneous IoT environments as continuing research challenges.

Similarly, Saha [4] presented a lightweight authentication protocol designed to provide secure mutual authentication with reduced computational requirements for Wireless Sensor Networks. While the protocol demonstrated lower processing overhead, its reliance on relatively static key management mechanisms may increase vulnerability to long-term key compromise if cryptographic keys are not refreshed according to changing network conditions. This observation highlights the importance of integrating lightweight encryption with adaptive session key management to maintain communication security throughout the operational lifetime of resource-constrained sensor networks.

Overall, the existing literature demonstrates that lightweight cryptographic techniques substantially improve the feasibility of secure communication in Wireless Sensor Networks. Nevertheless, most current approaches emphasize either cryptographic efficiency or authentication performance independently, while comparatively limited attention has been given to the coordinated integration of lightweight authenticated encryption, efficient key establishment, adaptive key management, and energy-aware communication within a unified security framework. Addressing these interconnected requirements remains essential for supporting secure and sustainable IoT-enabled WSN deployments.

B. ECC-Based Secure Communication Mechanisms

Secure key establishments remain one of the most critical requirements for protecting data transmission in Wireless Sensor Networks (WSNs). Although symmetric encryption algorithms offer high computational efficiency, their effectiveness largely depends on the secure generation, distribution, and management of cryptographic keys. Traditional public-key cryptographic algorithms, such as RSA, generally require large key sizes and extensive computational resources, making them unsuitable for resource-constrained sensor nodes. Consequently, Elliptic Curve Cryptography (ECC) has become one of the most widely adopted public-key

cryptographic techniques for WSNs because it provides equivalent security with substantially smaller key sizes, lower computational complexity, and reduced communication overhead [9].

Hybrid cryptographic frameworks have increasingly adopted ECC to establish secure session keys before applying lightweight symmetric encryption for data protection. Tripathy *et al.* [13] proposed a Hybrid Encryption Technique (HET) that combines Elliptic Curve Cryptography with Lempel–Ziv–Welch (LZW) compression to enhance secure communication while reducing ciphertext size. The proposed framework demonstrated improvements in confidentiality, authentication, and communication efficiency. However, its evaluation primarily focused on encryption performance and compression efficiency, without investigating the energy implications of repeated cryptographic operations or the scalability of secure key establishment in large-scale WSN deployments.

To strengthen secure communication in wireless sensor environments, Shang *et al.* [11] introduced an ECC-based anonymous authentication protocol that integrates elliptic curve key exchange with lightweight authentication mechanisms. Their protocol demonstrated improved resistance against common communication attacks while reducing computational overhead compared with conventional authentication approaches. Nevertheless, the proposed framework relied on relatively static session key management, limiting its ability to maintain forward secrecy through continuous key updates during prolonged network operation. This limitation may increase security risks in scenarios where communication sessions remain active for extended periods or sensor nodes are exposed to physical compromise.

Recent studies have further demonstrated that Elliptic Curve Diffie–Hellman (ECDH) provides an efficient mechanism for establishing shared secret keys in resource-constrained IoT environments. By enabling communicating nodes to derive identical session keys without directly transmitting confidential information over the wireless channel, ECDH significantly reduces the risk of key interception while maintaining lower computational complexity than conventional public-key key exchange algorithms [9]. Despite these advantages, secure session key establishment alone does not guarantee long-term communication security. Additional mechanisms for secure key derivation, periodic key renewal, and authenticated encryption remain necessary to protect against key compromise, replay attacks, and evolving communication threats.

Existing ECC-based communication frameworks primarily emphasize authentication accuracy or key establishment efficiency as independent objectives. Comparatively limited attention has been devoted to integrating efficient key establishment with adaptive key management, lightweight authenticated encryption, and energy-aware communication strategies within a unified security architecture. Furthermore, many existing studies evaluate cryptographic performance independently of network-level characteristics such as routing efficiency, communication overhead, and residual node energy, making it difficult to assess their practical suitability for long-term Wireless Sensor Network deployments.

Overall, the literature confirms that ECC and ECDH provide a robust foundation for secure key establishment in resource-constrained WSNs because of their favorable balance between security strength and computational efficiency. However, achieving reliable long-term communication security requires complementary mechanisms that efficiently derive session keys, preserve key freshness, support authenticated encryption, and operate in harmony with energy-aware communication protocols. These unresolved challenges continue to motivate the development of integrated lightweight security frameworks for modern IoT-enabled Wireless Sensor Networks.

C. Energy-Efficient Clustering and Routing Strategies

Energy efficiency is one of the primary design considerations in Wireless Sensor Networks (WSNs) because sensor nodes operate with limited battery resources that are often difficult or impossible to replenish after deployment. Inefficient communication and unbalanced energy consumption can significantly reduce network lifetime, increase packet loss, and degrade the overall reliability of data transmission. Consequently, clustering-based routing has become one of the most widely adopted strategies for improving communication efficiency by organizing sensor nodes into clusters, where designated cluster heads aggregate and forward data to the base station, thereby reducing redundant transmissions and communication overhead [15].

Recent studies have demonstrated that effective cluster-head selection plays a decisive role in achieving balanced energy consumption across the network. Gheisari *et al.* [14] proposed an energy-efficient cluster-head selection mechanism for smart agriculture applications that considered residual node energy and communication distance to improve routing performance. Their results indicated improvements in network lifetime and energy utilization; however, the security mechanisms were limited and did not incorporate lightweight cryptographic protection during inter-cluster and cluster-to-base station communication.

Similarly, Roberts and Ramasamy [15] developed an improved clustering-based routing protocol that enhanced packet forwarding efficiency through optimized cluster formation and routing decisions. Although the proposed protocol reduced communication delay and improved network throughput, it primarily focused on routing optimization without integrating secure key management or authenticated encryption into the communication framework. As a result, the protocol remained susceptible to security threats commonly encountered in open wireless communication environments.

Comprehensive reviews of clustering techniques have further emphasized that energy-aware cluster-head selection is essential for extending the operational lifetime of Wireless Sensor Networks. Nedham and Qurabat [7] analyzed a wide range of clustering approaches and concluded that residual energy, communication distance, and balanced cluster formation are among the most influential factors affecting routing efficiency. Nevertheless, many existing clustering protocols prioritize communication performance while treating security as a separate design component, resulting in architectures that may achieve energy efficiency but remain vulnerable to eavesdropping, replay attacks, and unauthorized data modification.

Likewise, Alomari *et al.* [8] systematically evaluated dynamic clustering techniques for heterogeneous Wireless Sensor Networks and highlighted the advantages of adaptive cluster-head selection based on residual energy and network conditions. Their review demonstrated that dynamic clustering can effectively distribute communication load among sensor nodes and improve network stability. However, the study also indicated that existing clustering protocols rarely coordinate routing decisions with adaptive cryptographic mechanisms, leaving opportunities to further improve both communication security and energy efficiency through integrated framework design.

Collectively, the existing literature confirms that clustering-based routing significantly improves communication efficiency, network scalability, and energy utilization in Wireless Sensor Networks. However, most current approaches concentrate on optimizing routing performance independently of secure communication mechanisms. The limited integration of adaptive cluster-head selection with lightweight key management, authenticated encryption, and energy-aware security policies restricts the ability of existing solutions to simultaneously achieve strong security, balanced energy consumption, and long-term network sustainability. These limitations underscore the need for an integrated communication framework in which energy-efficient clustering and lightweight cryptographic protection operate cooperatively to enhance the overall performance of resource-constrained WSNs.

D. Classical Lightweight Cryptographic Architectures

Classical cryptographic architecture has served as the foundation for the development of modern symmetric encryption algorithms used in secure communication systems. Among the most widely adopted structures are the Feistel Network and the Substitution–Permutation Network (SPN), both of which achieve data confidentiality through repeated substitution, permutation, and key mixing operations. These architectures have been extensively employed in conventional permutation-based authenticated encryptions because of their proven security properties and resistance to various cryptanalytic attacks [17].

The Feistel architecture divides plaintext into two equal halves and performs multiple rounds of iterative transformations, where one half is modified using a round function while the other half remains unchanged before the two halves are exchanged. This structure enables the same computational framework to be employed for both encryption and decryption, making Feistel-based algorithms attractive for a wide range of cryptographic applications. However, achieving strong security typically requires numerous encryption rounds, increasing computational complexity, processing latency, and energy consumption when implemented on resource-constrained Wireless Sensor Network nodes [18].

Similarly, Substitution–Permutation Network (SPN) architectures employ successive substitution layers and permutation operations to provide confusion and diffusion throughout the encryption process. Numerous conventional permutation-based authenticated encryptions have been developed using the SPN design because of its strong cryptographic characteristics and high resistance to statistical attacks [17]. Nevertheless, SPN-based algorithms generally require repeated nonlinear transformations and multiple processing stages, resulting in increased computational overhead, memory utilization, and execution time. These characteristics limit their suitability for low-power IoT devices that operate under stringent energy and processing constraints [18].

Recent advances in lightweight cryptography have shifted research attention from traditional cryptographic architectures toward authenticated encryption schemes that simultaneously provide confidentiality, integrity, and message authentication with significantly lower computational overhead [6]. Modern lightweight algorithms are specifically designed to minimize processing complexity while maintaining strong security guarantees for constrained computing environments. Among these, ASCON has gained considerable recognition following its standardization as the National Institute of Standards and Technology (NIST) lightweight

cryptography standard, owing to its efficient authenticated encryption mechanism, compact implementation, and suitability for resource-limited embedded systems [11].

Although classical Feistel and SPN architecture continue to provide valuable cryptographic foundations, their relatively higher computational requirements make them less appropriate for energy-constrained Wireless Sensor Networks when compared with modern lightweight authenticated encryption algorithms. Furthermore, many existing frameworks employing these traditional architectures primarily focus on encryption functionality without integrating efficient key establishment, adaptive session key management, and energy-aware communication strategies. Consequently, recent research has increasingly emphasized lightweight authenticated encryption frameworks that combine secure key management with efficient communication protocols to achieve improved security and resource utilization in IoT-enabled Wireless Sensor Networks.

Overall, the existing literature demonstrates that while classical cryptographic architectures remain fundamental to secure communication, the evolving requirements of modern Wireless Sensor Networks necessitate lightweight authenticated encryption mechanisms capable of providing comprehensive security with lower computational and energy overhead. This evolution provides the motivation for integrating efficient key establishment, adaptive key management, and ASCON-based authenticated encryption within the proposed lightweight security framework.

E. Critical Analysis and Research Gap

The reviewed literature demonstrates substantial progress in improving the security and energy efficiency of Wireless Sensor Networks through lightweight cryptography, elliptic curve cryptography, authentication protocols, and clustering-based routing mechanisms. Existing studies have successfully reduced computational complexity, improved secure key establishment, and enhanced communication efficiency for resource-constrained IoT devices [6], [10]. Similarly, clustering strategies have contributed to extending network lifetime by balancing communication loads and reducing redundant transmissions through energy-aware routing mechanisms [7], [8].

Despite these advancements, the current body of research reveals several important limitations. First, many lightweight cryptographic frameworks primarily focus on encryption efficiency while giving limited attention to secure and adaptive session key management. Although ECC-based key exchange provides an efficient mechanism for establishing shared secrets, several existing approaches rely on static or infrequently updated session keys, which may reduce forward secrecy and increase the risk of long-term key exposure during prolonged network operation [11], [9]. Likewise, authentication-oriented protocols generally emphasize secure user or node verification but often overlook the coordination between authentication, key derivation, and authenticated encryption within a unified communication framework.

Second, existing clustering protocols mainly optimize routing performance, cluster-head selection, and energy utilization but frequently treat communication security as an independent process rather than an integral component of routing decisions [14], [15], [7]. As a result, improvements in network lifetime are not always accompanied by corresponding enhancements in secure communication. The absence of close coordination between energy-aware routing and cryptographic key management may introduce additional communication overhead and reduce the overall efficiency of resource-constrained Wireless Sensor Networks.

Furthermore, most reported hybrid cryptographic frameworks combine asymmetric and symmetric encryption techniques to strengthen data confidentiality and authentication [13], [16]. However, comparatively fewer studies integrate efficient key establishment, secure key derivation, lightweight authenticated encryption, and adaptive key rotation within a single architecture designed specifically for energy-constrained WSN environments. This fragmented approach limits the ability of existing solutions to simultaneously achieve strong security, communication efficiency, and long-term network sustainability.

Based on the above observations, the principal research gap identified in this study is the lack of an integrated lightweight security framework that jointly combines energy-aware clustering, efficient elliptic curve-based session key establishment, secure key derivation, lightweight authenticated encryption, and adaptive key management for Wireless Sensor Networks. Existing studies generally optimize these components individually, whereas practical IoT deployments require them to operate in a coordinated manner to achieve reliable, scalable, and energy-efficient secure communication.

To address this research gap, the present work develops a unified lightweight security framework that integrates an Advanced LEACH-based clustering mechanism with Elliptic Curve Diffie–Hellman (ECDH) key establishment, HKDF-SHA256 session key derivation, ASCON-AEAD128 authenticated encryption, and an energy-aware dynamic key rotation strategy. By coordinating these complementary components within a single communication architecture, the proposed framework aims to improve secure data transmission, maintain key

freshness and forward secrecy, reduce computational and communication overhead, and enhance the operational lifetime of resource-constrained Wireless Sensor Networks. The implementation and performance evaluation presented in the subsequent sections demonstrate the effectiveness of this integrated design under realistic network conditions.

3. Proposed Methodology

The proposed framework employs a Hybrid ECC-ASCON lightweight security model that will improve the security of communication in a WSN and IoT. The data that is transmitted over WSNs must be safeguarded from attacks, threats, and misuse [19]. The hybrid cryptographic scheme covers the combination of the advanced LEACH clustering to build an energy-efficient network structure with Elliptic Curve Cryptography (ECC)-based ECDH key exchange to build a secure session key setup over open channels. ASCON-AEAD128 is used to perform lightweight authenticated encryption, which has built-in confidentiality, integrity, and authentication with low computation requirements. The asymmetric operations are restricted to initialize and rekeying phases, thereby significantly reducing energy overhead while ensuring confidentiality, integrity and forward secrecy in clustered WSNs. The permutation-based authenticated encryption design is utilized for the facilitation of authenticated encryption with associated data (AEAD) in communication protocol. Because of the dual protection of (ECC)-based ECDH key exchange and ASCON-AEAD128 lightweight authenticated encryption, the data in transit is safe. Figure 1 depict the system architecture of the proposed Hybrid ECC-ASCON security model. The architecture is designed to reduce computational overhead and save energy, essential when devices are limited by resources.

A. Advanced LEACH clustering protocol

Wireless Sensor Networks (WSNs) operate under stringent resource constraints, where sensor nodes possess limited battery capacity, computational capability, memory, and communication bandwidth. Since wireless communication is the primary source of energy consumption, efficient cluster formation and cluster-head (CH) selection play a critical role in extending network lifetime while maintaining reliable data transmission. Conventional Low-Energy Adaptive Clustering Hierarchy (LEACH) elects cluster heads using a probabilistic rotation mechanism, which distributes energy consumption among nodes. However, because the selection process is largely random, nodes with low residual energy or poor communication characteristics may still become cluster heads, leading to premature energy depletion, unbalanced load distribution, and increased packet loss. These limitations become more significant in secure WSN applications where cluster heads also participate in cryptographic key management and secure data forwarding.

To overcome these limitations, the proposed framework employs an Advanced LEACH clustering protocol that replaces the conventional random cluster-head election with a weighted multi-parameter decision model. Rather than relying solely on probability, the proposed approach evaluates each sensor node using four complementary criteria: residual energy, node trust, distance to the base station, and local node density. Integrating these parameters enables the protocol to simultaneously improve routing efficiency, reduce communication overhead, and provide a more reliable foundation for secure key establishment and encrypted data transmission.

The cluster-head selection probability for node *i* is calculated as

$$P_i = \alpha \left(\frac{E_{res,i}}{E_{max}}\right) + \beta T_i + \gamma \left(\frac{1}{D_i}\right) + \delta W_i \qquad (1)$$

where:

- E_i represents the current residual energy of node *i*.
- $E_{\max}$ denotes the initial maximum battery energy.
- T_i is the trust value assigned to node *i*.
- D_i is the Euclidean distance between node *i* and the base station.
- N_i represents the normalized neighbourhood density.
- $\alpha, \beta, \gamma, \delta$ are weighing coefficients satisfying to ensure balanced contribution from all decision parameters.

$$\alpha + \beta + \gamma + \delta = 1$$

The normalized residual energy term favours nodes with higher remaining battery capacity, thereby preventing premature failure of energy-constrained nodes and improving overall network lifetime. The trust value assigned to each node is incorporated into the cluster-head selection process to avoid selecting unreliable nodes for secure communication. Nodes with higher trust values are given greater priority during cluster-head election, thereby improving routing reliability and supporting secure key establishment.

The inverse-distance component prioritizes nodes located closer to the base station, thereby reducing transmission distance, lowering communication energy consumption, and improving packet delivery reliability. The neighbourhood density parameter prevents the formation of isolated or heavily overloaded clusters by preferring nodes with balanced local connectivity, resulting in improved load distribution across the network.

Unlike conventional LEACH, which considers only probabilistic rotation, the proposed Advanced LEACH protocol jointly optimizes energy availability, communication reliability, network topology, and load balancing before cluster-head election. This produces more stable clusters that require fewer re-clustering operations and reduce unnecessary communication overhead. Since secure key establishment and encrypted packet forwarding are performed through the elected cluster heads, selecting stable and energy-efficient cluster heads directly improves the reliability of the subsequent ECC-based key exchange and ASCON authenticated encryption stages.

The weighting coefficients provide balanced contributions from the normalized decision parameters during cluster-head selection. The normalized weighted formulation prevents any single parameter from dominating the election process while supporting stable cluster formation, energy-efficient routing, and reliable communication for secure data transmission.

Figure 1 illustrates the overall architecture of the proposed framework. After the Advanced LEACH protocol establishes energy-efficient clusters and elects reliable cluster heads, sensed data are forwarded to the security layer, where ECC-based key establishment, HKDF session-key derivation, ASCON authenticated encryption, secure packet transmission, packet verification, authenticated decryption, and adaptive session-key rekeying are performed before delivering authenticated sensor data to the application layer.

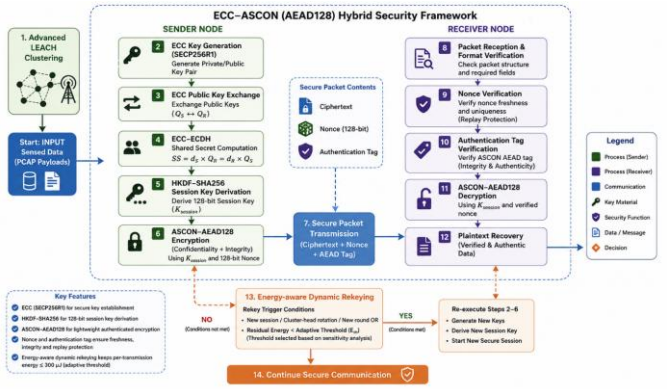

Figure 1. Overall Architecture of the Proposed Advanced LEACH–ECC–HKDF–ASCON Security Framework for Secure and Energy-Efficient WSN Communication

B. Hybrid ECC–ASCON Security Framework

The proposed framework integrates Elliptic Curve Cryptography (ECC) with the lightweight authenticated encryption algorithm ASCON-128 to establish a secure and energy-efficient communication mechanism for Wireless Sensor Networks (WSNs) deployed in Internet of Things (IoT) environments. The framework combines Advanced LEACH clustering, ECC-based key agreement, Elliptic Curve Diffie–Hellman (ECDH) shared secret generation, Hash-based Key Derivation Function (HKDF-SHA256), and ASCON-128 Authenticated Encryption with Associated Data (AEAD) to provide confidentiality, integrity, authentication, forward secrecy, and replay protection while maintaining low computational and communication overhead.

Initially, the Advanced LEACH protocol organizes sensor nodes into energy-aware clusters by selecting trustworthy cluster heads based on residual energy, trust value, communication distance, and local node density. Once cluster formation is completed, communicating nodes independently generate ECC key pairs using the SECP256R1 elliptic curve and securely establish a shared secret through the ECDH key agreement protocol. The shared secret is subsequently processed using HKDF-SHA256 to derive a unique 128-bit session key, which is employed by the ASCON-128 encryption algorithm for secure packet transmission. A unique nonce is generated for every transmitted packet to ensure message freshness and prevent replay attacks.

At the receiver side, the same session key is independently reconstructed through the ECDH-HKDF procedure. The received nonce and authentication tag are verified before decryption is performed. Packets failing either nonce validation or authentication tag verification are immediately discarded, thereby preventing unauthorized access and malicious packet injections. During communication security and reduce cryptographic risks during prolonged network operation, the proposed framework incorporates an energy-aware dynamic

rekeying mechanism that periodically regenerates session keys according to network events and node energy conditions. The complete architecture of the proposed secure communication framework is illustrated in Figure 1.

C. Key Management

The key is the most crucial part of encoding or decoding. An adversary discovering this key Efficient and secure key management is fundamental to protecting data transmitted in Wireless Sensor Networks (WSNs) and IoT environments. The proposed framework employs Elliptic Curve Cryptography (ECC) for public-key generation, Elliptic Curve Diffie–Hellman (ECDH) for secure shared secret establishment, and the Hash-based Key Derivation Function (HKDF-SHA256) for generating a secure symmetric session key used by ASCON-AEAD128 encryption.

ECC Key Generation (SECP256R1 Curve)

Each communicating node (sender and receiver) independently generates an ECC key pair consisting of a private key and a corresponding public key.

Private key generation

$$d \in [1, n-1] \qquad (2)$$

Public key computation

$$Q = d \cdot G \qquad (3)$$

where G denotes the base point of the SECP256R1 elliptic curve, n represents the order of the curve, d is the randomly selected private key, and Q is the corresponding public key. The public key is obtained through elliptic curve scalar multiplication. The security of ECC relies on the computational hardness of the Elliptic Curve Discrete Logarithm Problem (ECDLP), making recovery of the private key from the public key computationally infeasible.

After key generation, the communicating nodes exchange their public keys (SPub and RPub) over the communication channel, while the private keys remain confidential and are never transmitted. Compared with RSA, ECC provides an equivalent level of security using significantly smaller key sizes (256-bit ECC provides security comparable to 3072-bit RSA), thereby reducing computational complexity, memory usage, and energy consumption. These characteristics make ECC well suited for resource-constrained WSN and IoT devices.

ECDH Shared Secret Computation

Following public key exchange, the proposed framework employs Elliptic Curve Diffie–Hellman (ECDH) to establish a secure shared secret between the communicating nodes. ECDH enables both nodes to independently compute an identical shared secret without transmitting confidential key material over the communication channel [20].

The sender computes the shared secret as

$$SS = d_S \cdot Q_R \qquad (4)$$

while the receiver computes

$$SS = d_R \cdot Q_S \qquad (5)$$

where $d_S$and $d_R$denote the private keys of the sender and receiver, respectively, and $Q_S$and $Q_R$represent their corresponding public keys. Owing to the properties of elliptic curve scalar multiplication, both communicating nodes independently derive the same shared secret. Since the private keys are never exchanged, an attacker cannot compute the shared secret through passive eavesdropping, thereby supporting secure key establishment and forward secrecy.

HKDF Key Derivation (Extract and Expand)

The shared secret generated through ECDH may not possess sufficient randomness for direct use as a symmetric encryption key. Therefore, the proposed framework applies the Hash-based Key Derivation Function (HKDF-SHA256) to derive a secure and independent 128-bit session key for ASCON-AEAD128 encryption.

Extract Phase

$$PRK = HMAC(salt, SS) \qquad (6)$$

Expand Phase

$$OKM = HMAC\text{-}SHA256(PRK, info, length) \qquad (7)$$

During the Extract phase, HKDF generates a pseudorandom key (PRK) from the ECDH shared secret using an optional non-secret salt, thereby improving entropy distribution. In the Expand phase, the pseudorandom key is processed to generate the required output key material (OKM) of the desired length.

The derived OKM serves as the 128-bit master session key for ASCON-AEAD128 encryption. HKDF provides strong entropy extraction, maintains key separation between communication sessions, and prevents direct reuse of the ECDH shared secret. Consequently, the derived session key enhances the overall security and robustness of the proposed communication framework while remaining computationally efficient for resource-constrained WSN and IoT devices.

D. ASCON-AEAD128 Encryption and Decryption

ASCON-AEAD128 is employed to provide authenticated encryption for secure communication in the proposed ECC–ASCON framework. It simultaneously ensures confidentiality, integrity, and authenticity of sensor data while maintaining low computational and memory overhead, making it suitable for resource-constrained WSN and IoT devices. The symmetric session key used by ASCON is derived through the ECC–ECDH–HKDF key establishment process described in this section.

ASCON-128 Encryption

Step 1: Derive a master ASCON

$$K\_ASCON=HKDF\ (d_S \cdot Q_R) \tag{8}$$

The ECDH shared secret (SS) is computed at the sender using its private key $(d_S)$and the receiver's public key (Q_R), as defined in Equation (4). The shared secret is then processed through the HKDF-SHA256 extract and expand phases described in Equations (6) and (7) to derive a secure 128-bit ASCON session key. The receiver's public key is obtained during the initial key exchange or cluster formation process, while its authenticity is ensured through the trust-based clustering and session validation mechanisms implemented in the proposed framework. The derived ASCON session key is stored temporarily in volatile memory for the duration of the communication session and is securely erased upon session completion. This approach minimizes the risk of key exposure while supporting forward secrecy and secure session-based communication.

Step 2: Nonce Generation: A nonce (N) is generated per session

A unique nonce is generated for every communication session as

$$N=Counter||Timestamp \tag{9}$$

where the packet counter is incremented sequentially for every transmitted packet, while the timestamp guarantees uniqueness across communication sessions. This design prevents nonce reuse, protects against replay attacks, and preserves the semantic security of the authenticated encryption process.

Step 3: ASCON-128 Encryption is as follows:

Authenticated encryption is performed as

$$Ciphertext, Tag = ASCON\_Encrypt\ (K, N, AD, Plaintext) \tag{10}$$

Where,

- **K** represents the derived ASCON session key.
- **N** represents the generated nonce.
- **AD** denotes the associated data.
- **Plaintext** represents the sensed sensor data.

The ASCON-AEAD128 encryption procedure consists of the following stages:

1. Initialize the ASCON state using the derived session key and nonce.
2. Absorb the associated data (AD).

3. Perform the ASCON permutation operations.
4. Encrypt the plaintext sensor data.
5. Generate the authentication tag and produce the encrypted packet consisting of the ciphertext and authentication tag.

ASCON integrates encryption and authentication within a single lightweight authenticated encryption operation, eliminating the need for separate encryption and message authentication mechanisms. Consequently, the proposed framework achieves secure data transmission with reduced computational complexity, communication overhead, and energy consumption.

ASCON-128 Decryption

Step 1: Derive the same master ASCON Key.

$$K_{ASCON}=HKDF\ (d_R \cdot Q_S) \qquad (11)$$

The ECDH shared secret (SS) is computed at the receiver using its private key $(d_R)$and the sender's public key (Q_S), as defined in Equation (5). The shared secret is processed through the HKDF-SHA256 extract and expand phases to derive the identical 128-bit ASCON session key used during encryption. Since the session key is independently generated at both communicating nodes, no secret key is transmitted over the communication channel, thereby reducing the risk of interception while maintaining forward secrecy.

Step 2: Nonce validation: The received packet data is made up of two major parts Nonce (N) and Ciphertext (consisting of an authentication tag)

Before decryption, the received nonce is validated to verify packet freshness and detect replay attacks. The receiver checks that the received packet counter is greater than the previously accepted counter value. Packets containing duplicate or invalid nonces are immediately discarded to prevent replay attacks and unauthorized packet retransmission. ASCON-128 Decryption process

ASCON-128 Decryption Process

Authenticated decryption is performed as

$$Plaintext = ASCON_{Decrypt}(K, N, AD, Ciphertext) \qquad (12)$$

The ASCON-AEAD128 decryption procedure consists of the following stages:

1. Reconstruct the ASCON state using the derived session key and validated nonce.
2. Process the associated data (AD).
3. Perform the ASCON permutation operations.
4. Decrypt the received ciphertext.
5. Generate the authentication tag and compare it with the received authentication tag.
6. If the authentication tags match, the original plaintext is recovered successfully; otherwise, the received packet is discarded.

The authenticated decryption process verifies both data integrity and authenticity before recovering the original sensor data. By integrating ECC-based key establishment with ASCON-AEAD128 authenticated encryption, the proposed framework provides secure end-to-end communication while maintaining low computational complexity and energy consumption, making it suitable for resource-constrained Wireless Sensor Networks and IoT environments.

E. Energy-Aware Dynamic Key Management

Long-term deployment of Wireless Sensor Networks (WSNs) requires periodic renewal of cryptographic keys to prevent key exposure while minimizing additional energy consumption. To achieve this objective, the proposed ECC–ASCON framework incorporates an energy-aware dynamic rekeying mechanism that updates the session key only when predefined network events occur. Unlike conventional periodic rekeying schemes that introduce unnecessary computational overhead, the proposed approach performs adaptive rekeying according to the operational state of the network, thereby achieving an effective balance between security and energy efficiency.

The rekeying process is triggered under one or more of the following conditions:

- A new communication session is established.
- A new LEACH clustering round begins.
- Cluster-head rotation occurs.
- The residual energy of a communicating node falls below the predefined energy threshold.

When a rekeying event is triggered, the communicating node generates a new ECC key pair using the SECP256R1 curve and exchanges the updated public key with its communication peer. A new ECDH shared secret is subsequently established, and HKDF-SHA256 derives a fresh 128-bit ASCON session key. The previous session key is securely replaced, and the nonce counter is reset before encrypted communication resumes. If none of the rekeying conditions are satisfied, the existing session key is retained, thereby avoiding unnecessary cryptographic computations and reducing overall energy consumption.

This adaptive key management strategy provides continuous key freshness, limits the impact of long-term key exposure, enhances forward secrecy, and minimizes computational overhead. Consequently, the proposed framework maintains secure communication while extending network lifetime in resource-constrained WSN and IoT environments. The complete rekeying procedure is presented in Algorithm 1.

Algorithm 1: Energy-Aware Dynamic Rekeying

Input:
E_current = Current residual energy of node
E_threshold = Minimum energy threshold for secure operation
Begin
Monitor node residual energy E_current
if E_current < E_threshold then
    /* Trigger secure rekeying procedure */
    Generate new ECC key pair (d_new , Q_new)
    Exchange public keys with communication peer
    Compute new shared secret:
        SS_new = d_new × Q_peer
    Derive fresh session key using HKDF:
        K_session_new = HKDF(SS_new)
    Replace old session key with K_session_new
    Reset nonce counter
else
    Continue secure communication using existing session key
end if
End
Output:Updated session key K_session_new (if rekey triggered)

Algorithm 1 summarizes the adaptive rekeying procedure implemented in the proposed framework. The algorithm continuously monitors the residual energy of sensor nodes and initiates secure rekeying only when the predefined energy threshold is reached. During rekeying, a new ECC key pair is generated, a fresh ECDH shared secret is established, and HKDF-SHA256 derives a new ASCON session key. Otherwise, the existing session key is retained, thereby minimizing computational overhead while maintaining secure communication.

a. Secure Communication Workflow

The proposed secure communication workflow integrates Advanced LEACH clustering, ECC-based key agreement, HKDF session key derivation, ASCON-128 authenticated encryption, and energy-aware dynamic rekeying to provide secure and energy-efficient data transmission in Wireless Sensor Networks (WSNs). The complete communication process between the sender and receiver is illustrated in Fig. 2.

Initially, sensor nodes are organized into clusters using the Advanced LEACH clustering protocol. After cluster formation, the communicating sender and receiver independently generate ECC key pairs based on the SECP256R1 elliptic curve and exchange only their public keys through the wireless communication channel. Using the exchanged public keys, both nodes execute the Elliptic Curve Diffie–Hellman (ECDH) protocol to establish an identical shared secret without transmitting any secret information across the network.

The generated shared secret is subsequently processed using HKDF-SHA256 to derive a unique 128-bit ASCON session key. This session key is maintained locally at both communicating nodes and is used exclusively

for the current communication session. Since the session key is independently derived rather than transmitted, the proposed framework minimizes the possibility of key interception while supporting secure session establishment.

Before transmitting sensor data, the sender generates a unique nonce by combining a packet counter with the current timestamp. The sensed data are then encrypted using the ASCON-128 AEAD algorithm, which simultaneously produces ciphertext and an authentication tag. The transmitted packet therefore consists of the ciphertext, nonce, and authentication tag, enabling both confidentiality and integrity protection without requiring additional authentication mechanisms.

Upon receiving the encrypted packet, the receiver independently derives the identical ASCON session key using the ECDH-HKDF procedure. The received nonce is first validated to ensure message freshness and detect replay attacks. If nonce verification is successful, authenticated decryption is performed using ASCON-128. During the decryption process, the authentication tag is automatically verified to confirm that the received packet has not been modified during transmission. Packets that fail either non-ce verification or authentication tag validation are immediately discarded, whereas successfully authenticated packets are decrypted and delivered to the application layer.

To maintain long-term communication security, the proposed framework continuously monitors network events and node energy status. Whenever a new communication session is established, a cluster head rotation occurs, a new clustering round begins, or the residual energy falls below the predefined threshold, the Energy-Aware Dynamic Rekeying mechanism is activated. A fresh ECC key pair is generated, a new ECDH shared secret is established, and HKDF derives a new ASCON session key before secure communication resumes. This adaptive process maintains key freshness while minimizing unnecessary cryptographic computations.

By integrating Advanced LEACH clustering with ECC-based key establishment, HKDF session key derivation, ASCON-128 authenticated encryption, nonce-based replay protection, authentication tag verification, and adaptive dynamic rekeying, the proposed framework simultaneously achieves confidentiality, integrity, authentication, forward secrecy, replay protection, and energy-efficient secure communication for resource-constrained IoT-enabled Wireless Sensor Networks. The complete sender–receiver communication process is illustrated in Figure 2, while the achieved security features are summarized in Table 1.

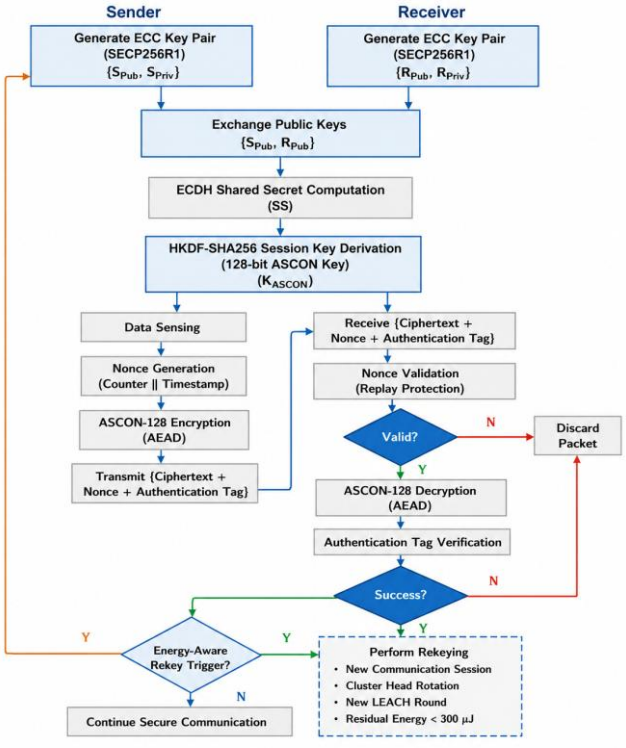

Fig. 2 Data Flow Diagram of the Proposed ECC–ASCON Secure Communication Workflow

Figure 2. Data Flow Diagram of the Proposed ECC–ASCON Secure Communication Workflow

4. Experimental results and discussions

A. Implementation Environment

The proposed Hybrid ECC–ASCON security framework was implemented and evaluated in a simulation-based Internet of Things–Wireless Sensor Network (IoT-WSN) environment using the NS-3 network simulator integrated with Python-based cryptographic modules. The simulation environment was designed to emulate secure communication among resource-constrained sensor nodes operating under realistic network conditions. To improve communication efficiency and reduce transmission overhead, the wireless sensor network was organized using Advanced LEACH-inspired clustering together with K-Means clustering, where Cluster Heads (CHs) aggregate data from member nodes and forward the collected information to the base station. This clustering strategy enables balanced communication while supporting energy-efficient network operation.

During network initialization, each sensor node generates an Elliptic Curve Cryptography (ECC) public-private key pair using the SECP256R1 elliptic curve. Before data transmission, communicating nodes perform an Elliptic Curve Diffie–Hellman (ECDH) key exchange to establish a shared secret without transmitting the secret key over the communication channel. The generated shared secret is subsequently processed through the HMAC-based Key Derivation Function (HKDF) with SHA-256 to derive a secure 128-bit symmetric master key. This master key is employed by the ASCON-128 Authenticated Encryption with Associated Data (AEAD) algorithm to provide confidential and authenticated packet transmission. To maintain secure communication throughout the session, the framework further incorporates an energy-aware dynamic key rotation mechanism together with version-based key management, allowing secure session-key updates while minimizing computational and energy overhead in resource-constrained IoT devices.

Network traffic generated during the NS-3 simulation was exported as Packet Capture (PCAP) files, which preserve the actual packets exchanged during the simulated communication process. The generated PCAP files were analyzed using the Wireshark network protocol analyzer to examine packet-level communication characteristics before cryptographic processing. The extracted packet payloads serve as the input to the proposed Hybrid ECC–ASCON framework, where secure key establishment, authenticated encryption, packet transmission, authentication verification, and decryption are executed according to the implemented communication workflow. This implementation approach enables the proposed framework to be evaluated using realistic simulated network traffic while preserving the complete communication sequence from packet generation to secure packet delivery.

Figure 3 presents the packet statistics obtained from the PCAP file generated during the NS-3 simulation and analysed using the Wireshark protocol analyser.

Table 1. Security Features of the Proposed Hybrid ECC–ASCON Framework

Security Property	**Implemented Mechanism**	**Purpose**
Confidentiality	ASCON-128 AEAD	Protects transmitted data against unauthorized disclosure through lightweight authenticated encryption.
Integrity	ASCON Authentication Tag Verification	Detects unauthorized modification of transmitted packets and ensures data integrity during communication.
Authentication	ECC-ECDH with ASCON-128 AEAD	Authenticates communicating nodes and verifies the legitimacy of transmitted packets.
Forward Secrecy	ECDH Shared Secret Establishment	Establishes secure session keys without transmitting secret keys over the communication channel.
Replay Protection	Nonce and Packet Counter Validation	Prevents replay attacks by ensuring that previously transmitted packets cannot be reused.
Key Freshness	HKDF-Derived Session Keys with Energy-Aware Dynamic Key	Periodically refreshes session keys to minimize key exposure and strengthen long-term

	Rotation	communication security.
Energy Efficiency	Advanced LEACH Clustering with Energy-Aware Rekeying	Reduces communication overhead and energy consumption while maintaining secure network operation.

The captured network traffic contains the packets exchanged among the simulated sensor nodes during secure communication and provides statistical information such as packet count, average packet length, minimum and maximum packet lengths, transmission rate, and burst characteristics. These captured packet payloads are subsequently extracted and processed by the proposed Hybrid ECC–ASCON framework, where ECC-based key establishment, HKDF-based session key derivation, ASCON-128 authenticated encryption, and secure packet verification are performed according to the implemented communication workflow. The PCAP-based analysis confirms that the proposed framework is evaluated using realistic simulated network traffic rather than synthetically generated plaintext data, thereby providing a practical basis for assessing secure communication in IoT-WSN environments.

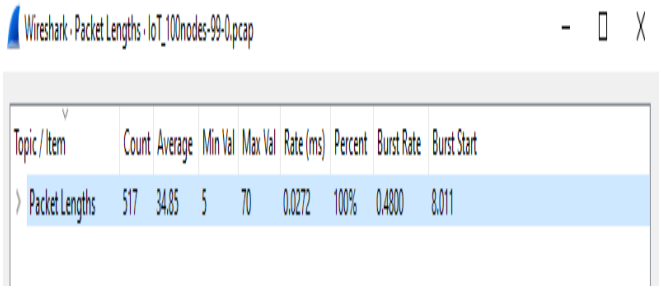

Figure 3. Packet statistics extracted from the NS-3 generated PCAP file and analysed using the Wireshark protocol analyser prior to cryptographic processing.

B. Evaluation Parameters

The performance of the proposed Hybrid ECC–ASCON framework was evaluated using three performance metrics that collectively assess the reliability of secure communication, the computational overhead of cryptographic processing, and the energy efficiency of the IoT-based wireless sensor network. These evaluation parameters were selected because they directly reflect the impact of the proposed framework on network performance while considering the resource constraints of wireless sensor nodes. The selected metrics include Packet Delivery Ratio (PDR), Key Expansion Time, and Energy Consumption, which together provide a comprehensive assessment of the proposed secure communication framework.

C. Packet Delivery Ratio (PDR)

Packet Delivery Ratio (PDR) is used to evaluate the reliability of data transmission in the proposed IoT-WSN communication framework. It represents the percentage of data packets successfully received at the destination with respect to the total number of packets transmitted by the source node. A higher PDR indicates reliable communication with minimal packet loss and efficient packet delivery across the wireless sensor network.

$$PDR = (\text{Number of packets received} / \text{Number of packets sent}) * 100 \quad (13)$$

To emulate realistic wireless communication conditions, packet loss is modelled using a probabilistic drop model that considers the effects of background channel conditions, packet payload size, and network density.

$$drop\_prob = base + payload\_factor + node\_factor \quad (14)$$

where base represents the background network noise, payload_factor denotes the influence of packet size on transmission reliability, and node_factor represents network congestion caused by increasing node density. During simulation, a probabilistic decision determines whether an individual packet is successfully delivered or dropped, thereby approximating practical wireless channel behaviour. Consequently, a higher Packet Delivery Ratio indicates improved communication reliability, reduced packet collisions, and enhanced network performance within the proposed secure communication framework.

D. Key Expansion Time

Key Expansion Time represents the computational time required to generate the cryptographic keys before secure communication is established. In the proposed Hybrid ECC–ASCON framework, this process includes the generation of the ECC public–private key pair, computation of the ECDH shared secret, derivation of

the 128-bit symmetric session key using HKDF with SHA-256, and initialization of the ASCON-128 authenticated encryption process. These operations are performed only during session establishment or subsequent dynamic rekeying events before secure packet transmission begins.

Since computationally intensive ECC operations are executed only during key establishment rather than for every transmitted packet, the cryptographic overhead introduced during normal communication remains low. Once the session key has been established, the lightweight ASCON-128 authenticated encryption algorithm is used for secure packet transmission, thereby reducing computational complexity while maintaining confidentiality, integrity, and authentication throughout the communication session.

E. Energy Consumption

Energy Consumption is a critical performance metric for wireless sensor networks because sensor nodes operate with limited battery resources. The proposed framework evaluates the total energy required for secure communication by considering both the computational energy associated with cryptographic operations and the communication energy consumed during wireless packet transmission. The total energy consumption is measured in microjoules (μJ).

The total energy consumption is calculated as

$$E = P_{cpu} (t_{enc} + t_{dec} + t_{key}) + P_{tx} . t_{tx} + P_{rx} . t_{rx} \quad (15)$$

where P_{cpu} represents the processor power consumed during cryptographic operations, t_{enc} and t_{dec} denote the encryption and decryption times, respectively, t_{key} represents the time required for key generation and key expansion, P_{tx} and P_{rx} represent the transmission and reception power of the wireless transceiver, while t_{tx} and t_{rx} denote the packet transmission and reception durations, respectively. This metric quantifies the overall energy overhead introduced by the proposed Hybrid ECC–ASCON framework while accounting for both cryptographic processing and wireless communication activities.

F. Simulation Results and Analysis

This section presents the simulation results obtained to evaluate the performance of the proposed Hybrid ECC–ASCON framework under different wireless sensor network configurations. The performance is assessed using Packet Delivery Ratio (PDR), Key Expansion Time, and Energy Consumption, which collectively evaluate communication reliability, cryptographic processing overhead, and energy efficiency. The proposed framework is compared with the Lightweight Security Algorithm (LSA), Substitution–Permutation Network (SPN), and Feistel-based cryptographic models, as these approaches represent commonly adopted cryptographic architectures for wireless sensor network security. While SPN and Feistel-based models primarily provide symmetric encryption, they do not inherently support authenticated encryption, dynamic session key establishment, or forward secrecy. Similarly, LSA improves the efficiency of conventional symmetric encryption through lightweight processing but relies on static symmetric key management and separate authentication mechanisms. In contrast, the proposed Hybrid ECC–ASCON framework integrates Advanced LEACH-based clustering, ECC–ECDH key establishment, HKDF-based session key derivation, ASCON-128 authenticated encryption, and energy-aware dynamic key management within a unified communication framework. This integrated design improves communication reliability while maintaining low computational and energy overhead, making it suitable for resource-constrained IoT-enabled wireless sensor network environments.

G. Packet Delivery Ratio (PDR)

Figure 3 presents the Packet Delivery Ratio (PDR) of the proposed Hybrid ECC–ASCON framework in comparison with LSA, SPN, and Feistel-based cryptographic models for network sizes ranging from 20 to 100 sensor nodes. Packet Delivery Ratio represents the percentage of data packets successfully received at the destination relative to the total number of packets transmitted by the source node and serves as an important indicator of communication reliability in wireless sensor networks.

The proposed Hybrid ECC–ASCON framework consistently achieved the highest packet delivery performance, maintaining a PDR between 97% and 100% across all evaluated network sizes. In comparison, the PDR of LSA gradually decreased from 98% to 90% as the number of sensor nodes increased, whereas SPN and Feistel-based cryptographic models exhibited a more significant reduction in packet delivery performance under higher network loads [7]. These results demonstrate that the proposed framework maintains stable communication reliability even under increasing network density.

The improved packet delivery performance is attributed to the integration of Advanced LEACH-based clustering, which efficiently distributes communication traffic among cluster heads and reduces network congestion during packet forwarding. Furthermore, secure session establishment through ECC–ECDH key

exchange, followed by HKDF-based session key derivation, enables secure communication without repeatedly performing computationally intensive key establishment operations during packet transmission. The implementation of ASCON-128 authenticated encryption, together with nonce-based authentication and packet counters, provides secure packet transmission while preventing replay attacks with minimal communication overhead. Consequently, the proposed framework maintains reliable packet delivery under increasing communication loads, demonstrating its suitability for scalable IoT-enabled wireless sensor network deployments.

H. Key Expansion Time

Figure 4 compares the key expansion time of the proposed Hybrid ECC–ASCON framework with LSA, SPN, and Feistel-based cryptographic models for key lengths ranging from 8 bits to 256 bits. Key Expansion Time represents the computational time required to establish the cryptographic keys before secure communication begins.

The proposed Hybrid ECC–ASCON framework required 2.26 ms for an 8-bit key length and 29.58 ms for a 256-bit key length, demonstrating consistently lower key expansion time than the comparison methods. In contrast, the key expansion time of LSA, SPN, and Feistel-based cryptographic models increased more rapidly with increasing key length, while SPN required approximately 140 ms for the largest evaluated key size [7]. These results indicate that the proposed framework introduces lower computational overhead during secure session establishment.

The lower key expansion time is achieved because ECC operations are executed only during initial session establishment and subsequent rekeying events, while HKDF efficiently derives the symmetric session key from the generated ECDH shared secret. Once the session key has been established, ASCON-128 performs lightweight authenticated encryption without repeated asymmetric cryptographic computations during packet transmission. Compared with SPN and Feistel architecture, which require more computationally intensive round-based encryption and key scheduling operations, the proposed framework reduces cryptographic processing overhead while maintaining secure communication.

I. Energy Consumption

Figure 5 presents the energy consumption of the proposed Hybrid ECC–ASCON framework in comparison with LSA, SPN, and Feistel-based cryptographic models for network sizes ranging from 20 to 100 sensor nodes. Energy consumption represents the total energy required for cryptographic computation and wireless communication and is a critical performance metric for battery-powered wireless sensor networks.

The proposed Hybrid ECC–ASCON framework achieved the lowest energy consumption among all evaluated approaches, consuming 244.41 μJ for a network consisting of 20 sensor nodes and 256.25 μJ for the largest evaluated network. The average energy consumption of the proposed framework was 247.6 μJ, whereas LSA exhibited an average energy consumption of 411.2 μJ [7]. In comparison, SPN and Feistel-based cryptographic models recorded significantly higher average energy consumptions of 781.6 μJ and 795.3 μJ, respectively [7]. These results demonstrate that the proposed framework provides superior energy efficiency while maintaining secure communication.

The improved energy efficiency is achieved through the combined implementation of Advanced LEACH-based clustering, ECC–ECDH session establishment, HKDF-based session key derivation, ASCON-128 authenticated encryption, and energy-aware dynamic key management. Advanced LEACH reduces communication overhead by balancing traffic among cluster heads, while ASCON-128 minimizes computational energy during encryption and decryption. Since ECC-based operations are limited to session establishment and rekeying events, repeated asymmetric cryptographic computations during packet transmission are avoided, thereby reducing both computational and communication energy consumption. Consequently, the proposed framework is well suited for long-term deployment in resource-constrained IoT-enabled wireless sensor network environments.

Overall, the simulation results demonstrate that the proposed Hybrid ECC–ASCON framework provides higher packet delivery reliability, lower key expansion time, and reduced energy consumption than LSA, SPN, and Feistel-based cryptographic models. These improvements are achieved through the implemented integration of Advanced LEACH-based clustering, ECC–ECDH key establishment, HKDF-based session key derivation, ASCON-128 authenticated encryption, and energy-aware dynamic key management, thereby enabling secure, lightweight, and energy-efficient communication for resource-constrained IoT-based wireless sensor networks.

J. Security Analysis

The proposed Hybrid ECC–ASCON framework provides a lightweight and secure communication mechanism for IoT-enabled Wireless Sensor Networks (WSNs) by integrating Advanced LEACH clustering, ECC–ECDH key establishment, HKDF-based session key derivation, ASCON-128 authenticated encryption, nonce-based packet encryption, packet counters, and energy-aware dynamic key management. The integration of these mechanisms enhances communication security while maintaining low computational overhead and energy consumption suitable for resource-constrained sensor nodes.

K. Eavesdropping Protection

The proposed framework protects communication against passive eavesdropping through the implementation of Elliptic Curve Diffie–Hellman (ECDH) key exchange. During session establishment, communicating nodes independently generate a shared secret using their private key and the corresponding peer's public key without transmitting the secret key through the communication channel. The generated shared secret is subsequently processed using HKDF-SHA256 to derive the 128-bit symmetric master key used by ASCON-128 AEAD for packet encryption. Since the cryptographic key is never exchanged directly over the network, intercepted communication packets cannot reveal the encryption key, thereby preserving the confidentiality of transmitted data.

L. Replay Attack Prevention

Replay attacks are mitigated through the combined implementation of unique nonces and packet counters. A new random nonce is generated for every transmitted packet, while the packet counter maintains the transmission sequence during the communication session. Upon packet reception, the receiver verifies the packet counter before decryption. Packets containing duplicate or invalid sequence information are discarded, thereby preventing attackers from successfully retransmitting previously captured packets.

M. Data Integrity and Authentication

The proposed framework employs ASCON-128 Authenticated Encryption with Associated Data (AEAD) to provide confidentiality, integrity, and authentication simultaneously. Each encrypted packet contains an authentication tag generated during encryption. Before decrypting the received packet, the receiver verifies the authentication tag using the locally derived session key. If packet contents are modified during transmission or the authentication tag is invalid, the packet is rejected immediately. This mechanism ensures that only authentic and unmodified packets generated by legitimate communicating nodes are accepted for further processing.

N. Resistance to Man-in-the-Middle Attacks

The framework strengthens resistance against man-in-the-middle attacks through ECC-based ECDH secure key establishment. Since the shared session key is independently computed by the communicating nodes using their respective ECC key pairs, the session key is never transmitted across the communication channel. Without access to the corresponding private keys, an attacker cannot derive the shared secret or generate the valid session key required for authenticated communication. Consequently, unauthorized interception and modification of communication sessions become significantly more difficult.

O. Key Freshness and Node Compromise Mitigation

The proposed framework incorporates energy-aware dynamic key management together with periodic session-key rotation to improve long-term communication security. The session key is periodically updated according to communication requirements and predefined energy constraints using the implemented key rotation mechanism. Each key update increases the key version maintained by the communicating nodes, ensuring that newly established session keys replace previous keys during secure communication. Consequently, prolonged reuse of the same cryptographic key is avoided, reducing the potential impact of key exposure while maintaining secure communication with minimal additional computational overhead.

Overall, the proposed Hybrid ECC–ASCON framework demonstrates an effective balance between communication security, computational efficiency, and energy consumption. The integration of Advanced LEACH-based communication, ECC–ECDH secure key establishment, HKDF-based session key derivation, ASCON-128 authenticated encryption, nonce-based replay protection, and energy-aware dynamic key management enables secure, lightweight, and reliable communication for resource-constrained IoT-enabled Wireless Sensor Networks. The experimental results presented in Figures 4–6 further demonstrate that the proposed framework maintains high packet delivery reliability while reducing key expansion time and energy consumption compared with the selected baseline methods, indicating its suitability for practical WSN and IoT deployments.

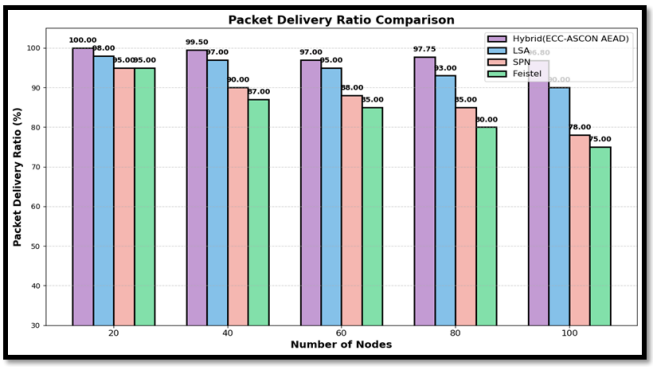

Figure 4. Packet Delivery Ratio comparison of the proposed Hybrid ECC–ASCON framework with LSA, SPN, and Feistel-based cryptographic models.

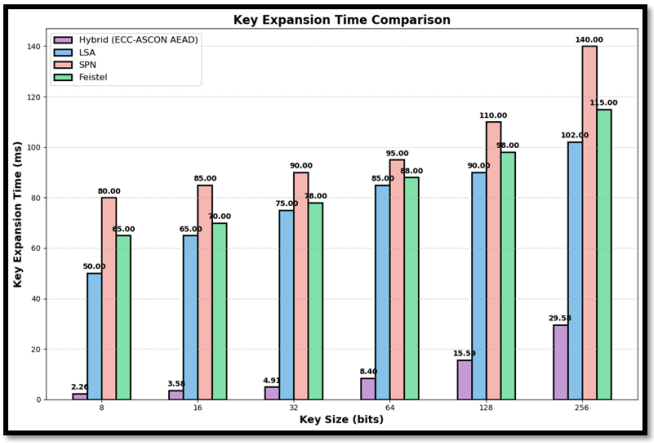

Figure 5. Key Expansion Time comparison of the proposed Hybrid ECC–ASCON framework with LSA, SPN, and Feistel-based cryptographic models.

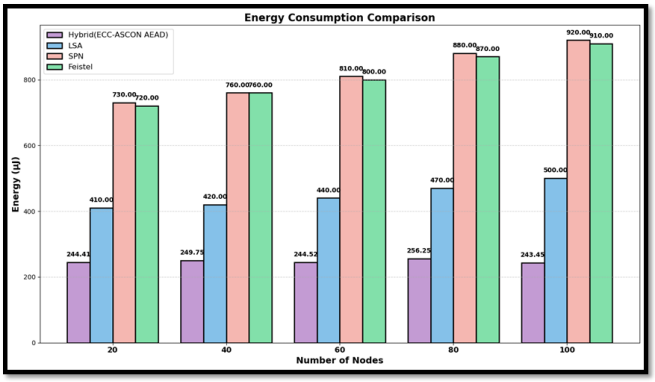

Figure 6. Energy Consumption comparison of the proposed Hybrid ECC–ASCON framework with LSA, SPN, and Feistel-based cryptographic models.

5. Conclusion

This study presented a Hybrid ECC–ASCON security framework for secure and energy-efficient communication in IoT-enabled Wireless Sensor Networks (WSNs). The proposed framework integrates Advanced LEACH-based clustering, ECC-based Elliptic Curve Diffie–Hellman (ECDH) key establishment, HKDF-SHA256 session key derivation, ASCON-128 authenticated encryption, nonce-based packet protection, packet counters, and energy-aware dynamic key management to provide lightweight and reliable secure communication for resource-constrained sensor nodes.

The simulation results demonstrate that the proposed framework achieves improved communication reliability while maintaining low computational and energy overhead. Compared with the selected baseline approaches, namely LSA, SPN, and Feistel-based cryptographic models, the proposed framework consistently achieved a higher Packet Delivery Ratio (97–100%), lower Key Expansion Time (2.26–29.58 ms), and lower

Energy Consumption (244.41–256.25 μJ) across the evaluated network configurations. These results indicate that the integration of lightweight authenticated encryption with secure session key establishment provides an effective balance between communication security and network performance.

From a security perspective, the proposed framework strengthens communication confidentiality, integrity, authentication, replay protection, resistance to man-in-the-middle attacks, and key freshness through the combined implementation of ECC–ECDH, HKDF-SHA256, ASCON-128 AEAD, unique nonces, packet counters, and periodic session-key updates. In addition, Advanced LEACH-based clustering efficiently distributes communication traffic among cluster heads, contributing to reduced communication overhead and improved energy utilization.

Overall, the proposed Hybrid ECC–ASCON framework demonstrates its suitability for secure communication in resource-constrained IoT-enabled WSN environments by combining lightweight cryptographic processing with energy-efficient communication management. The proposed architecture provides a practical foundation for secure wireless sensing applications where communication reliability, low computational overhead, and energy efficiency are critical requirements.

The present study is limited to simulation-based evaluation using the implemented network configuration and the selected performance metrics. Future work may extend the proposed framework through implementation in real-world IoT deployments, evaluation under larger and more heterogeneous network environments, comparison with additional lightweight cryptographic schemes, and formal security verification to further validate the robustness of the proposed communication framework.

Acknowledgment

The authors would like to express their sincere gratitude to their institution, colleagues, and all those who provided support and encouragement throughout this research. The authors also acknowledge the valuable contributions of all individuals who assisted directly or indirectly in the completion of this work.

References

1. D. Giji Kiruba and J. Benita. “A Survey of Secured Cluster Head: SCH Based Routing Scheme for IOT Based Mobile Wireless Sensor Network,” *ECS Transactions*, vol. 107, no. 1, pp. 16725–16745, 2022. doi: 10.1149/10701.16725ecst.
2. S. Singh, D. Garg, M. Manju, and A. Malik. “A Novel Cluster Head Selection Algorithm Based IoT Enabled Heterogeneous WSNs Distributed Architecture for Smart City,” *Microprocessors and Microsystems*, vol. 101, p. 104892, 2023. doi: 10.1016/j.micpro.2023.104892.
3. M. A. Burhanuddin, A. A. Mohammed, R. Ismail, M. Hameed, A. N. Kareem, and H. Basiron. “A Review on Security Challenges and Features in Wireless Sensor Networks: IoT Perspective,” *Journal of Telecommunication, Electronic, and Computer Engineering*, vol. 10, pp. 17–21, 2018.
4. D. Saha. “Improving IoT Security in Wireless Sensor Networks,” *Smart Internet of Things*, vol. 1, no. 4, pp. 289–297, 2024. doi: 10.22105/siot.v1i4.138.
5. S. Dhall and K. Yadav. “Cryptanalysis of Substitution-Permutation Network Based Image Encryption Schemes: A Systematic Review,” *Nonlinear Dynamics*, vol. 112, no. 17, pp. 14719–14744, 2024. doi: 10.1007/s11071-024-09816-0.
6. B. Kaur, M. Rakhra, D. Singh, A. Singh, and S. Shruti. “Advancements in Lightweight Cryptography: Secure Solutions for Resource-Constrained Environments in IoT, WSNs, and CPS,” pp. 1–7, 2024. doi: 10.1109/ICRITO61523.2024.10522297.
7. W. B. Nedham and A. K. M. A. Qurabat. “A Comprehensive Review of Clustering Approaches for Energy Efficiency in Wireless Sensor Networks,” *International Journal of Computer Applications in Technology*, vol. 72, no. 2, pp. 139–160, 2023. doi: 10.1504/IJCAT.2023.133035.
8. M. F. Alomari, M. A. Mahmoud, and R. Ramli. “A Systematic Review on the Energy Efficiency of Dynamic Clustering in a Heterogeneous Environment of Wireless Sensor Networks (WSNs),” *Electronics*, vol. 11, no. 18, p. 2837, 2022. doi: 10.3390/electronics11182837.
9. V. Tanksale. “Efficient Elliptic Curve Diffie–Hellman Key Exchange for Resource-Constrained IoT Devices,” *Electronics*, vol. 13, no. 18, p. 3631, 2024. doi: 10.3390/electronics13183631.
10. S. A. Ansari and S. Ali. “A Systematic Review of Lightweight Cryptographic Schemes for Security and Privacy in IoT,” *Discover Computing*, vol. 28, no. 1, 2025. doi: 10.1007/s10791-025-09755-3.
11. Y. Shang, J. Chen, S. Wang, Y. Zhang, and K. Ma. “A Secure and Lightweight ECC-Based Authentication Protocol for Wireless Medical Sensors Networks,” *Sensors*, vol. 25, no. 21, p. 6567, 2025. doi: 10.3390/s25216567.
12. A. Srivastava and P. K. Mishra. “Load-Balanced Cluster Head Selection Enhancing Network Lifetime in WSN Using Hybrid Approach for IoT Applications,” *Journal of Sensors*, vol. 2023, no. 1, 2023. doi: 10.1155/2023/4343404.
13. Tripathy, S. K. Pradhan, A. K. Nayak, and A. R. Tripathy. “Hybrid Cryptography for Data Security in Wireless Sensor Network,” in *Data Engineering and Intelligent Computing: Proceedings of ICICC 2020*, pp. 597–606, Singapore: Springer Singapore, 2021. doi: 10.1007/978-981-16-0171-2_57.

14. M. Gheisari *et al.* “An Efficient Cluster Head Selection for Wireless Sensor Network-Based Smart Agriculture Systems,” *Computers and Electronics in Agriculture*, vol. 198, p. 107105, 2022. doi: 10.1016/j.compag.2022.107105.
15. M. K. Roberts and P. Ramasamy. “An Improved High Performance Clustering Based Routing Protocol for Wireless Sensor Networks in IoT,” *Telecommunication Systems*, vol. 82, no. 1, pp. 45–59, 2023. doi: 10.1007/s11235-022-00968-1.
16. D. Karunkuzhali, A. A. Shaikh, R. Suguna, and M. Venkatesan. “Hybrid Lightweight Cryptography with Attribute-Based Encryption for Secure Health Monitoring in IoT-Wireless Body Area Sensor Network,” *Biomedical Materials & Devices*, 2025. doi: 10.1007/s44174-025-00402-5.
17. N. Mahlake, T. E. Mathonsi, D. Du Plessis, and T. Muchenje. “A Lightweight Encryption Algorithm to Enhance Wireless Sensor Network Security on the Internet of Things,” *Journal of Communications*, vol. 18, no. 1, pp. 47–57, 2023. doi: 10.12720/jcm.18.1.47-57.
18. W. El-Shafai, A. K. Mesrega, A. Ahmed, N. A. Elbahnasawy, and F. Fathi. “Hybrid Lightweight Encryption for IoT: Integrating Chaotic Key Generators with Feistel and Substitution-Permutation Networks for Secure 3DV Transmission,” *Multimedia Tools and Applications*, 2025. doi: 10.1007/s11042-024-19203-x.

.