IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 6 January 2024, accepted 23 January 2024, date of publication 31 January 2024, date of current version 16 February 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3360488

RESEARCH ARTICLE

Innovative Energy-Efficient Proxy Re-Encryption for Secure Data Exchange in Wireless Sensor Networks

OSAMA A. KHASHAN[1], NOUR M. KHAFAJAH[2], WALEED ALOMOUSH[3], AND MOHAMMAD ALSHINWAN[4]

[1]Research and Innovation Centers, Rabdan Academy, Abu Dhabi, United Arab Emirates
[2]MEU Research Unit, Middle East University, Amman 11831, Jordan
[3]School of Information Technology, Skyline University College, Sharjah, United Arab Emirates
[4]Faculty of Information Technology, Applied Science Private University, Amman 11931, Jordan

Corresponding author: Osama A. Khashan (okhashan@ra.ac.ae)

ABSTRACT In the realm of wireless sensor networks (WSNs), preserving data integrity, privacy, and security against cyberthreats is paramount. Proxy re-encryption (PRE) plays a pivotal role in ensuring secure intra-network communication. However, existing PRE solutions encounter persistent challenges, including processing delays due to the transfer of substantial data to the proxy for re-encryption and the computational intensity of asymmetric cryptography. This study introduces an innovative PRE scheme that is meticulously customized for WSNs to enhance the secure communication between nodes within the network and external data server. The proposed PRE scheme optimizes efficiency by integrating lightweight symmetric and asymmetric cryptographic techniques, thereby minimizing computational costs during PRE operations and conserving energy for resource-constrained nodes. In addition, the scheme incorporates sophisticated key management and digital certificates to ensure secure key generation and distribution, which in turn, facilitates seamless authentication and scalable data sharing among the entities in WSN. This scheme maintains sensor-node data encryption and delegates secure re-encryption tasks exclusively to cluster heads, thereby reinforcing data privacy and integrity. Comprehensive evaluations of security, performance, and energy consumption validated the robustness of the scheme. The results confirm that the proposed PRE scheme significantly enhances the security, efficiency, and overall network lifetime of WSNs.

INDEX TERMS Proxy re-encryption (PRE), lightweight encryption, wireless sensor network (WSN), secure data sharing, network security.

I. INTRODUCTION

Wireless sensor networks (WSNs) represent a pivotal technological advancement in an increasingly interconnected world. These networks comprise a multitude of resource-constrained small sensor devices that collaborate to collect and exchange data from their immediate surroundings. This collaborative capability enables WSNs to find applications in diverse fields ranging from environmental monitoring and surveillance to industrial automation and healthcare systems [1]. However, sensor nodes (SNs) inherently face limitations, such as constraints in computational power, energy resources, memory, and bandwidth. These limitations give rise to multifaceted challenges in the intricate task of sharing information within a network, amplifying the significance of ensuring data security and confidentiality [2].

In addition, SNs are vulnerable to various types of attacks, including physical tampering, data interception, node compromise, and denial-of-service (DoS) attacks [3]. These SNs which are deployed remotely and left unmonitored, are particularly susceptible to these threats. Attackers may tamper with SNs to compromise their functionality, steal valuable

The associate editor coordinating the review of this manuscript and approving it for publication was Md. Arafatur Rahman.

data, or disable them, to disrupt network operations. Data interception attacks can lead to breaches of data confidentiality, exposing sensitive information to unauthorized entities. Node-compromise attacks can compromise data integrity, and DoS attacks can disrupt network communication and availability [4].

Information privacy and integrity are paramount concerns during communication and sharing among SNs, cluster heads (CHs) and base stations (BSs). Traditional security mechanisms deployed in WSNs often rely on intricate cryptographic calculations. Unfortunately, these mechanisms impose a considerable energy burden on the SNs, severely hindering communication efficiency [1]. Given the intrinsic energy limitations of SNs, this excessive energy consumption has the potential to cause nodes to deplete their power, potentially leading to premature failure, thus curtailing the network's operational lifetime [5]. In particular, real-time applications are highly sensitive to these energy inefficiencies because they require low latency for rapid decision-making [6].

The CHs, acting as intermediaries between SNs and the overarching network infrastructure, are not immune to security vulnerabilities. Compromised CHs can inadvertently serve as gateways for cyberattacks, potentially resulting in the exposure of aggregated data. These breaches pose a significant risk to data privacy and integrity, emphasizing the critical importance of establishing trust in CHs as a fundamental element of network security [7]. Energy-usage efficiency has emerged as a central concern in WSNs, necessitating the development of energy-efficient security mechanisms. To strike a harmonious balance between data security and energy conservation, innovative approaches, such as lightweight encryption techniques, must be explored [8]. Secure data sharing between nodes located in different clusters introduces additional complexities, requiring the implementation of centralized management systems to effectively address a multitude of concerns, including security, delay, and scalability [9].

Proxy re-encryption (PRE) technology enables secure data communication and sharing within a network, whereby a semi-trusted proxy is employed to convert encrypted data from one device to another without exposing the actual content or any private keys. This seamless transformation is achieved using a re-encryption key provided by a trusted third party that ensures that the data remain confidential and secure throughout the entire transfer process [10]. However, PRE is most effective when large resource-rich devices are employed. and significantly less efficient when deployed on resource-constrained devices, such as SNs. The primary reason for this reduced efficiency stems from the substantial computational costs associated with the complex cryptographic calculations required by the PRE process. These resource-intensive computations render PRE less suitable for devices with limited computational capabilities and energy resources. Additionally, as data-sharing volumes increase and involve a larger number of devices, the computational workload of the proxy escalates, potentially leading to delays in the re-encryption process, which could affect the overall network efficiency and real-time data transmission [11].

In this study, we address these limitations by introducing a new PRE scheme specifically tailored for CHs within WSNs. This innovative scheme leverages lightweight encryption techniques to significantly enhance secure WSN communication and data sharing. The proposed scheme effectively mitigates the security challenges that a CH may encounter, such as physical attacks or data interception, when handling aggregated data during multi-hop transmissions between intermediary CHs on route to AP. The scheme also ensures that data remain encrypted at all times, thereby preventing unauthorized access to or viewing of the data by the CHs. Furthermore, it plays a pivotal role in reducing communication latency and optimizing energy consumption.

The main contributions of this study are summarized as follows:

- In this study, an innovative PRE scheme explicitly designed for WSNs is introduced. The scheme is tailored to address the unique challenges posed by resource-constrained devices in WSNs, whereby lightweight cryptography is leveraged to optimize the encryption, re-encryption, and decryption processes. This optimization enhances communication efficiency among network entities while significantly reducing overhead and mitigating transmission delays.
- Energy consumption during PRE operations was optimized for both SNs and CHs. The proposed scheme seamlessly enhances the secure data exchange within and between clusters while conserving energy resources. This energy-efficient approach significantly improves network-wide security levels and prolongs the operational lifetime of resource-constrained WSNs.
- The effectiveness of the proposed scheme was evaluated by conducting comprehensive security and performance analyses. The results validate the robustness of the proposed PRE scheme in ensuring data security, confidentiality, and integrity while also highlighting the benefits of energy efficiency.

The remainder of this paper is organized as follows: Section II provides an overview of related work. Section III introduces the preliminaries of the study. Section IV presents the details of the proposed scheme. In Section V, the analyses and experimental results are discussed. Finally, Section VI presents the conclusions.

II. RELATED WORK

Numerous PRE schemes, each characterized by distinct features and capabilities, have been introduced in the literature. These schemes are designed to offer a variety of properties, including unidirectionality, non-transitivity, non-transferability, non-interactivity, collusion resistance, proxy invisibility, original access, and key optimality [12]. These attributes play a pivotal role in assessing the scheme's suitability for specific applications and have been extensively examined in academic research.

Recent PRE schemes have often been developed based on combinations of these properties, with the evaluations focusing on the presence of these specific attributes, to ensure that the chosen scheme aligns with the desired security objectives [13]. Researchers have incorporated conventional cryptographic methods such as identity-based encryption (IBE) [14], role-based encryption (RBE) [15], attribute-based encryption (ABE) [16], and certificate-based encryption (CBE) [17], to enhance the scope of PRE solutions. These cryptographic techniques have been integrated into PRE frameworks, providing versatile solutions for addressing a wide range of security and data-sharing requirements. This approach promotes the diversification of security mechanisms within PRE, empowering researchers with a broader set of tools to tailor their solutions to specific scenarios and constraints [10].

However, the computational efficiency of these PRE cryptographic techniques can vary, depending on various factors. In certain scenarios, particularly those involving complex access policies or large data, these techniques may incur high computational costs during decryption. These costs are primarily associated with pairing operations and policy enforcement [18]. In addition, the management of cryptographic keys and access policies can become cumbersome, especially as the system scales up, potentially leading to administrative complexities and security vulnerabilities [13], rendering them inefficient for implementation in resource-constrained devices in which computational resources and energy conservation are paramount.

To address the aforementioned limitations, researchers have embarked on efforts to improve PRE solutions for devices with limited resources. In this context, an ABE-based PRE scheme was introduced by researchers in [19] to bolster the security on IoT platforms, whereby the cryptographic overhead was mitigated by employing elliptic curve encryption, for encryption, re-encryption, and decryption operations. Furthermore, the issue of variable-length ciphertexts was addressed in [20], with the ciphertext expanding as the attributes increased. This PRE scheme is valuable in scenarios where compromised user decryption keys can be invalidated, resulting in a collusion-resistant CP-ABE scheme. Additionally, an improved approach is introduced to ensure constant-length ciphertexts through PRE, thereby reducing computational and communication overhead while maintaining security against the decisional bilinear Diffie-Hellman (DBDH) problem. In [21], researchers proposed a scheme that relies on the complexity of solving the bilinear inverse Diffie-Hellman problem tailored to IoT devices. This bidirectional scheme supports multi-hop functionality, allowing the seamless transformation of uploaded ciphertexts into multiple distinct forms within IoT networks without decryption. A PRE scheme was also designed in [22] to transform ciphertexts between keys without requiring complete trust in the proxy or computationally intensive operations, realizing this outcome through an effective authenticated key-agreement procedure enabled by a proxy re-encryptor designed for IoT applications. This scheme enables the establishment of a shared secret key between the devices and employs a symmetric cipher for data encryption. Another study introduced the key-insulated attribute-based PRE scheme for resource-constrained devices [23]. This approach labels ciphertexts with attributes and adopts a structured approach for user access privileges. Delegators have the ability to generate re-encryption keys using their private keys and entrust this task to a semi-trusted data server. The system's lifespan is partitioned into distinct time intervals, each marked by regular updates of private keys, which in turn control access privileges. Other studies in [24], [25], and [26] conducted integrated blockchain into PRE approaches to enhance data integrity and security. This integration guarantees transparent and tamper-proof data transactions, adding an additional layer of protection to the overall security of the system.

Lightweight encryption, well-suited for resource-constrained environments, is a cryptographic approach designed to minimize computational and memory overhead. Its primary goal is to prioritize efficiency while maintaining an acceptable level of security, rendering it an ideal choice for deployment in networks with limited processing power and memory [13], [27]. Researchers, including those in [28] and [29], have incorporated lightweight encryption into PRE schemes. These schemes play a vital role in ensuring secure data sharing and communication in distributed and decentralized systems. However, traditional PRE methods relying on symmetric ciphers frequently require the distribution of unique pre-shared secret keys, potentially introducing security vulnerabilities. To address these concerns, PRE schemes employing lightweight asymmetric encryption using elliptical curve cryptography (ECC) were introduced [30] and [31] for IoT. These approaches strike a balance between security and efficiency, making them suitable for constrained IoT networks.

Nevertheless, it is important to note that when simultaneously sharing outsourced data with numerous parties, the computational load on the proxy may increase substantially, potentially resulting in computational costs and delays in responding to network devices [32]. Therefore, although lightweight encryption and its application in PRE schemes offer promising venues for enhancing the security and efficiency in networks with resource constraints, challenges related to scalability and computational load management must be effectively addressed.

Despite substantial improvements in PRE security and efficiency, particularly in IoT contexts, resource-constrained devices pose challenges that need to be recognized, and certain critical limitations tied to the unique architecture and constraints of WSNs have yet to be adequately addressed. Previous studies have not fully considered the intricacies of WSNs, including their requirements for efficient routing, data aggregation, and self-organization. Consequently, the practicality and effectiveness of these PRE schemes may be compromised in real-world WSN deployments.

In addition, the integration of blockchain and other attributes into PRE approaches, while enhancing data integrity and security, may introduce challenges related to resource overhead, latency, and scalability, which are critical concerns in WSNs. Therefore, an effective solution is required to address the integration challenges of PRE into WSNs and ensure the seamless alignment of these technologies.

III. PRELIMINARIES

A. OVERVIEW OF WSN ARCHITECTURE

The architecture of a WSN consists of three fundamental components: SNs, CHs, and data aggregation, governed by communication protocols, as illustrated in Figure 1. SNs equipped with specialized sensors serve as the foundational nodes of the network and are strategically positioned across the target area to form a distributed data-collection network. Efficient data management in WSNs is accomplished through cluster formation, wherein the SNs are organized into clusters based on their physical proximity. Each cluster consists of multiple SNs under the leadership of a CH. These CHs have a critical function in collecting the data generated by member SNs and transmitting them to a central base station, utilizing either a single-hop or multi-hop approach, commonly known as the Sink or BS. This aggregation process minimizes redundant data transmissions, resulting in significant energy conservation.

Wireless sensor networks often exhibit a hierarchical structure in which multiple levels of CHs may exist, further enhancing scalability and efficient data management. In addition, the resilience of WSNs is bolstered through redundancy and self-organization mechanisms, ensuring continued operation even in the presence of node failures or adverse conditions.

Periodic updates of CHs as determined by factors such as energy levels and network traffic, ensure efficient network operation. The CHs also serve as the primary connection points to the BS and other CHs in different clusters, fostering information exchange between intercluster nodes, thereby enhancing network scalability. To facilitate seamless communication and data transmission, WSNs employ various wireless protocols and routing algorithms. These methods incorporate data aggregation techniques, error correction mechanisms, and energy-efficient routing strategies that are intricately designed to prolong the lifetime of the network. Protocol selection, routing decisions, and the implementation of security measures are customized to align with the unique demands of specific applications and network requirements.

Notably, security measures such as encryption and authentication, have gained increased significance considering the inherent vulnerabilities and efficiency overheads associated with the existing security protocols in WSNs [33].

B. INTEGRATED LIGHTWEIGHT ENCRYPTION METHODS

1) LIGHTWEIGHT SYMMETRIC ENCRYPTION

In the proposed study, Speck was selected as a superior lightweight symmetric encryption algorithm to achieve high

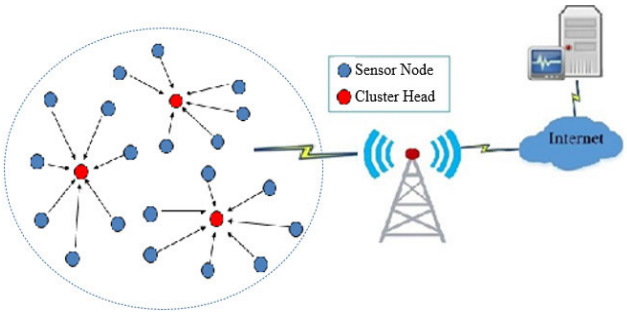


FIGURE 1. WSN architecture.

performance in resource-constrained environments, making it an excellent choice for WSN implementation. Speck, originally developed by the National Security Agency (NSA), excels in both hardware and software implementations. Using block (b) sizes of 64 or 128 bits and supporting symmetric key (Sk) sizes of 128,192, and 256 bits, Speck flexibly adapts to specific encryption requirements. The number of rounds (r) employed in Speck, typically ranges from 22 to 34, depending on the chosen b and Sk sizes, allowing precise tuning to achieve the desired security and efficiency levels [34].

Speck's design principles prioritize simplicity and efficiency, delivering robust encryption capabilities while minimizing computational overhead and memory usage, which are crucial factors in WSNs. Its internal architecture relies on straightforward operations, including bit shifts, additions, and XOR operations. This streamlined and efficient design ensures that Speck encrypt data within WSNs without incurring significant computational or memory burden. A feature of Speck that stands out is its ability to encrypt complete messages without complex modes of operation, simplifying the encryption process and reducing vulnerability risks associated with larger blocks or intricate methods. Moreover, Speck exhibits robust security characteristics such that even a single-bit change in the input data can result in a significantly different ciphertext. This inherent property enhances security by mitigating the risk of cut-and-paste attacks, thereby enhancing data integrity within the WSN [35].

In terms of resource consumption, empirical studies have consistently demonstrated Speck's superiority over resource-intensive encryption algorithms, including the advanced encryption standard (AES), the data encryption standard (DES), and other traditional symmetric ciphers [36]. The coordination between efficiency, security, and adaptability to resource-constrained environments renders Speck highly suitable for secure communication within constrained networks, seamlessly aligning with the demands of WSNs.

2) LIGHTWEIGHT PUBLIC KEY ENCRYPTION

In the proposed scheme, we utilize ellipticcurve cryptography (ECC) as a lightweight public-key cryptographic method

inspired by ElGamal pioneering work on public-key encryption [37]. This approach involves concealing m through two values, $\alpha\hat{}$k and $\beta\hat{}$k, with β. resulting from α raised to the power of a. In this context, α is a primitive root of a large prime p, and k is an integer selected at random. Significantly, the parameters α, β, and p are publicly known. The sending entity utilizes the value k to compute $\left(\alpha\hat{}\mathrm{k}, \beta\hat{}\mathrm{k}\right)$ before transmitting them to the intended recipient. With this secret knowledge, the recipient can decrypt the original message using $m = \left(\alpha^{\mathrm{k}}\right)^{-\mathrm{a}} * \left(\beta^{\mathrm{k}} m\right) = \left(\alpha^{\mathrm{a}}\right)^{-\mathrm{k}} * \left(\beta^{\mathrm{k}} m\right) = \left(\beta^{-\mathrm{k}}\right) * \left(\beta^{\mathrm{k}} m\right)$ [38].

The advent of ECC, independently introduced by Koblitz [39] and Miller [40], marked a significant shift in public-key encryption. ECC utilizes elliptic curve groups over a finite field to implement ElGamal's public-key cryptosystem and operates on points of an elliptic curve over finite fields, rather than directly encrypting messages. This involves essential cryptographic functions, such as encoding messages into points, decoding points into messages, and validating public keys. Key generation in ECC is a crucial process that involves the following steps:

i Selecting a prime curve: An elliptic curve (denoted as E) is defined by a nonsingular cubic polynomial equation with two unknowns within the finite field $\mathbb{F}_p$, where $\mathbb{F}_p$ represents integers operating under the modulo p. The elliptic curve E over $\mathbb{F}_p$ is expressed as $y^2 = x^3 + ax + b(mod\ p)$, where $a, b \in \mathbb{F}_p$. A secure cryptosystem is ensured when $4a^3 + 27b^2 \neq 0(mod\ p)$. The finite field comprises integers ranging from 0 to $(p - 1)$, and the strategic choice of p guarantees the existence of a finite number of points on E, thereby ensuring security [41].

ii Defining key parameters: In this phase, parameters α, β, p, and the curve C are publicly disclosed. Here, both α and β represent points located on E and hold essential significance within the public key infrastructure.

Key generation involves creating both private and public keys. The private key, denoted as d, is calculated as a random integer in the interval $[1, n-1]$, where n represents the prime order of the cyclic subgroup P of the elliptic curve E. The corresponding public key Q is produced as $Q = d \times P$, establishing a unique and secure pairing between the keys.

The fundamental cryptographic operations in ElGamal's ECC follow a defined procedure. During encryption, the sender initially divides m into smaller blocks and represents each block as an integer modulo of p. Subsequently, a random k is chosen to calculate two distinct points (s, w) on the elliptic curve. Specifically, the sender calculates $s = (x_s, y_s) = \mathrm{k} \times \alpha$ and determines w as $w = (x_w, y_w) = (m + k \times \beta)$, where β is derived from α and k. These pair of points (s, w) collectively represents the encrypted form of message m, which is then transmitted to the intended destination for further processing. In the decryption process, upon receiving encrypted points (s, w), the destination node initiates the decryption process to recover the message m. It calculates m using $m = y_w - \mathrm{a} \times y_s$, where a is a secret parameter exclusively known to the recipient, and y_s and y_w are derived from the received points s and w. This decryption process ensures secure message retrieval.

IV. PROPOSED PRE ARCHITECTURE FOR WSNs

In this section, the architectural design of the proposed PRE-based WSN is presented, whereby we delve into the intricacies of the cryptographic algorithms employed and elaborate on the construction of the security model within the network.

A. ARCHITECTURE DESIGN

In this section, the design aspects of the proposed PRE-based WSN are explored. The architectural design consists of three pivotal phases, as illustrated in Figure 2. Table 1 provides a compilation of the symbols used in the proposed scheme along with descriptions.

TABLE 1. List of symbols and their descriptions in this study.

Symbol	Description
SN	Wireless sensor node
CH	Cluster head
ID	Node identity
C	Network cluster
Pk	Entity public key
Prk	Entity private key
Sk	Symmetric encryption key
rk	Re-encryption key
TAN	Trusted authority node
Crt	Node certificate
Sprm	System parameters
DS	Node digital signature
K	Node symmetric key and digital signature
m	Node plaintext message
C	Ciphertext
RC	Re-encrypted ciphertext
ΔT	Total processing time
Pw	Computed power consumption
b	Encryption block size
E	Elliptic curve
r	Random number $\in \mathrm{F}_p^*$
v	Secret value $\in \mathrm{F}_p^*$

In the initial phase, keys and certificates are generated for each node in the network. Subsequently, a combination of lightweight symmetric and asymmetric encryption techniques was employed to secure the data generated by the SNs and their associated encryption keys. In the second stage, a PRE mechanism is implemented at the CH level to facilitate secure data transmission. Finally, in the third stage, an effective management approach is incorporated to ensure secure communication and ciphertext sharing among entities within the WSNs.

In the proposed scheme, the network architecture is organized into clusters, each comprising SNs connected to a CH. During the node setup process, each node is assigned a

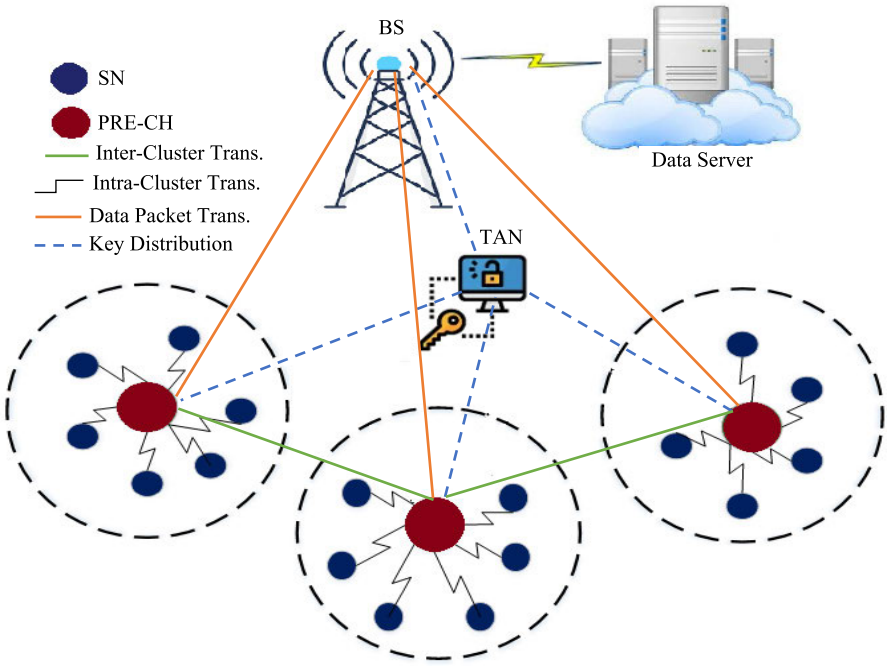


FIGURE 2. Architectural design of the proposed PRE-based WSN.

unique identifier (ID) registered with its corresponding CH. Every SN in the network, including CH, possesses a distinctive public and private key pair, denoted as $(Pk, P\ rk)$. The scheme incorporates a dedicated group of CH nodes serving as proxy servers to enable seamless connectivity and communication among nodes, spanning within and across clusters.

Given the resource-constrained nature of the CH, where resource-intensive tasks such as key generation, encryption, and re-encryption may deplete the power reserves, a specific fog/edge server with higher processing capabilities connected to all CHs, is designated as a fully trusted authority node (TAN). The TAN plays a pivotal role in overseeing the critical functions within the network. Its responsibilities include SN registration, generation of public system parameters, and the secure creation of cryptographic keys for each CH and its associated SNs. In addition, it is responsible for generating digital signatures to ensure the authentication of each node within the network. Notably, although TAN plays a central role in upholding network security, it remains entirely uninvolved in any aspect of PRE functionality.

During the SN registration process within the network, a certificate (Crt) is allocated to each SN that contains vital information. This Crt includes a cluster identifier (CID) that signifies the specific cluster (C) with which the node is affiliated. Additionally, each SN is assigned a unique identifier (SID) within its respective C, which provides precise and exclusive identification. Finally, the certificate Crt generation stage encompasses the creation of a distinct certificate (Crt_{SN}) for every SN. This Crt includes essential information such as CID, SID, Pk_{SN}, and DS_{SN}. It is then securely disseminated and stored in the SN, ensuring authentication and secure transmission of information. The registration procedure comprises the following stages:

1) Generation of cluster identifier (CID): To create a distinctive CID for enrolling new SNs into C, a unique random number is generated for each C. Each CH is equipped with a distinct identifier ($CHID$) and a publicprivate key pair ($Pk_{CH}, P\ rk_{CH}$). This information is securely exchanged among all network's CHs.
2) Generation of a unique SN identifier (SID), digital signature (DS_{SN}), and a public-private key pair (Pk_{SN}, Prk_{SN}): These components serve to uniquely distinguish and authenticate each SN within its designated C. To achieve this, a unique serial number is assigned to each SID, and DS_{SN} is generated using the hash of the SN's Pk. Additionally, each SN is allocated an EC public-private key pair (Pk_{SN}, Prk_{SN}).
3) Symmetric key (Sk) creation: Each time a legitimate SN transmits data across the network, a fresh Sk is created for this specific purpose. The creation of this Sk involves a lightweight one-way hash function as proposed [42]. This function is preferred because of its computational efficiency and resilience to inversion. Subsequently, the Sk is used to encrypt the data originating from SN using a lightweight Speck symmetric encryption method.
4) Certificate generation (Crt_{SN}): Every SN receives its unique Crt_{SN}. The structure of Crt_{SN} incorporates key information, including CID, SID, DS_{SN}, and Pk_{SN}. Subsequently, Crt_{SN} is securely disseminated and

stored in the SN. Its primary function encompasses the dual purpose of authentication and ensuring secure transmission of information.

B. SECURITY MODEL IMPLEMENTATION

The proposed PRE scheme comprises a set of five algorithms, each meticulously defined according to specific input and output parameters, thereby establishing a clear delineation of their respective functions and interactions within the system.

1) SYSTEM INITIALIZATION

Assume that $\mathrm{E}\left(\mathbb{F}_q\right)$ is an elliptic curve defined over the finite field $\mathbb{F}_q$, where q is a significant prime number, and G represents a point on E with order p. Additionally, two multiplicative groups of prime order p are identified as G1 and G2. In this context, a bilinear map is a function, denoted as e, which maps elements from G1 $\times$ G1 $\rightarrow$ G2, and s is an element in e(G1, G1) belonging to G2. The TAN initiates the setup algorithm, using security parameter a as input to produce the public system parameter *Sprm*, which encompasses information about E, q, p, e, G, and s. The details of system initialization are presented in Algorithm 1.

Algorithm 1 System Initilaization

Input a
Output $Sprm_{SN}$
Begin
  for $\forall C_i \in WSN$ **do**
    $Compute\_ID() \rightarrow CID$
    $Identify\_CH() \rightarrow CHID$
    for $\forall SN_i \in C$
      $Compute\_ID() \rightarrow SID$
      $Generate\_Sprm() \rightarrow \mathrm{E}, q, p, e, \mathrm{G}, \mathrm{s}$
      $Send\ \left(Sprm_{SN}\right) \rightarrow SN_i$
    end for
  end for
End

2) KEY GENERATION

During this procedure, the TAN utilizes the public system parameter Sprm to compute the key pairs (Pk, Prk) and certificate (Crt) for nodes A (sender) and B (recipient), where B can represent various entities. These entities may include an SN within the same cluster as A, an SN located within another cluster within the network, or even a base station or data server responsible for receiving the data. The procedure also involves the creation of the re-encryption key (rk), which is used by a CH to re-encrypt a message between A and B. This flexibility in recipient types underscores the scalability and adaptability of the system, enabling secure data transmission and data sharing across a wide range of network entities. The details of the keygeneration procedure are presented in Algorithm 2.

Algorithm 2 Key Generation

Input *Sprm*
Output $Crt, r\ k, (Pk, P\ rk)$
Begin
  $ChooseRandom() \rightarrow r \in \mathrm{F}_p^*$
  $Compute\ (Prk_A) \rightarrow Prk_A = (\mathrm{a}r) \in \mathrm{F}_p^*$
  $Compute\ (Pk_A) \rightarrow Pk_A = (\mathrm{a}rG) \in \mathrm{F}_p^*$
  $Compute\ (Prk_B) \rightarrow Prk_A = (\mathrm{b}r) \in \mathrm{F}_p^*$
  $Compute\ (Pk_B) \rightarrow Pk_A = (\mathrm{b}r\mathrm{G}) \in \mathrm{F}_p^*$
  $Compute\ (rk) \rightarrow rk = (\mathrm{a}r)^{-1}\mathrm{b}r\mathrm{G} = (\mathrm{a})^{-1}\mathrm{b}\mathrm{G}$
  $Compute\ (\mathrm{DS}) \rightarrow \mathrm{DS}_{SN} = Hash\,(Pk_{SN})$
  $Create\ (Crt) \rightarrow Crt_{SN}\ (CID,\ SID,\ \mathrm{DS}_{SN},\ Pk_{SN})$
End

3) SENSOR NODE ENCRYPTION

The sender node initiates the data encryption procedure to secure the message and cryptographic keys. This procedure takes m, K, and Pk of A as inputs. The algorithm then uses Speck to encrypt the divided blocks (b) of m with the computed Sk, generating a ciphered message (C_m). Next, ElGamal's ECC is employed to encrypt Sk and the DS, referred to as K, which is then used to encrypt the node's message during that specific round. Subsequently, an encrypted version of the encryption key, known as C_K, is generated.

Utilizing Speck's lightweight design ensures robust data security without imposing excessive computational overhead. Additionally, ElGamal's ECC is specifically chosen for encrypting cryptographic keys and certificates. Although characterized by a relatively slower nature [43], asymmetric ciphers excel in securing smaller data sizes and facilitating cryptographic key exchange. In ElGamal's ECC encryption, the public key holds significant importance as it serves as the base point for concealing secret values through scalar multiplication, ensuring robust data confidentiality and security throughout the encryption process. This hybrid approach, employing Speck for data encryption and ECC for key and certificate encryption, effectively optimizes both security and efficiency in resource-limited WSN environments. The integration of this dual encryption method transforms messages and their associated keys into secure ciphertext representations. Algorithm 3 delineates the encryption procedure at the sensor node level by utilizing this hybrid combination of symmetric and asymmetric encryption.

4) CLUSTER HEAD RE-ENCRYPTION

The re-encryption procedure is initiated when the target CH receives a transmitted packet from the SN containing the node's Crt, encrypted data blocks C_m, encrypted cryptographic keys C_K, and the recipient's identity SID_B. The CH begins by verifying the authenticity of the SN through the Crt_{SN}. Once authentication is confirmed, the corresponding rk is retrieved from TAN.

The CH then selectively re-encrypts the portion of C_K that was originally encrypted by node A, generating a new

Algorithm 3 Sensor Node Encryption

Input Pk_A, m, K
Output C_m, C_K
Begin
  $OneWayHash\ () \longrightarrow Sk$
  $Create\_Blocks(m) \longrightarrow b_1, .., b_n$
  $Speck\_Enc\ (m, S\ k//b_1, .., b_n//r) \longrightarrow C_m$
  $Generate\_SecretValue() \longrightarrow v \in F_p^*$
  $ECC\_Enc\ (k//Pk_A) \longrightarrow C_{k_A} = (\alpha, \beta)$
    $= (vPk_A, s^v\mathrm{G} + K)$
  $A \leftarrow Return\ (C_m, C_K)$
End

Algorithm 5 Entity Re-Encryption

Input RC_K, C_m, Prk_B
Output m
Begin
  $ECC\_Dec\ (RC_k//Prk_B) \longrightarrow K = \beta' - (\alpha')^{\frac{1}{rb}}\ \mathrm{G}$
  $Compute\ (\beta') \longrightarrow \beta' = s^v\mathrm{G}$
  $Compute\ (\alpha') \longrightarrow \alpha' = s^{vrb}$
  $Compute\ (K) \longrightarrow k = s^v\mathrm{G} + K - (s^{vrb})^{\frac{1}{rb}}\ \mathrm{G} = K$
  $Speck\_Dec\ (C_m, r\|Sk) \longrightarrow m$
  $B \leftarrow Return\ (m)$
End

re-encrypted ciphered key denoted as RC_k. This RC_K can only be decrypted by node B. Notably, this re-encryption is limited to C_K, which is considerably shorter in length compared to the size of C_m. Consequently, CH incurs minimal power consumption during this process. Algorithm 4 provides a detailed outline of this procedure.

Algorithm 4 Cluster Head Re-Encryption

Input C_K, SID_B, rk, Crt_A
Output RC_K
Begin
  $Check\_Authentication\ (Crt_A)$
  $ECC\_Enc\ (C_k//rk) \longrightarrow RC_k = (\alpha', \beta')$
  $Compute\ (\alpha') \longrightarrow \alpha' = e(\alpha, r\ k) = e(var\mathrm{G}, rk)$
  $Compute\ (rk) \longrightarrow rk = a^{-1}b\mathrm{G}$
  $Compute\ (\beta') \longrightarrow \beta' = s^v\mathrm{G} + Pk_B$
  $Compute\ (RC_K) \longrightarrow RC_K = (s^{vrb}, s^v\mathrm{G} + K)$
  $CH \leftarrow Return\ (RC_K)$
End

5) ENTITY DECRYPTION

The decryption procedure begins when recipient node B receives the data packet that includes C_m and RC_K from the CH. Note that B can represent an SN within the cluster, a different cluster, an AP, or a data server. By utilizing the private key Prk_B of B, RC_K is decrypted to recover K which includes $Sprm$ and Sk. These keys are subsequently employed to decrypt C_m and retrieve the original message m. Algorithm 5 outlines the decryption procedure performed by entity B.

C. SECURE COMMUNICATION AND SHARING

When a registered SN within a specific C initiates communication or data-sharing with other SN in the same cluster, different clusters, or data servers, a secure connection is established through the associated CH. During this process, the sending SN transmits its Crt and recipient ID to the CH for authentication. If the Crt is successfully verified, the CH permits data transmission; otherwise, authentication is denied.

After successful SN authentication, the CH communicates with TAN to obtain the required cryptographic keys and $Sprm$. Subsequently, SN encrypts the payload in the transmitted data packet using the generated Sk. In addition, it encrypts a K using its own Pk_{SN}, and attaches the C_k to the data packet.

Upon reception of the data packet by the CH, it uses the acquired rk to re-encrypt the C_K and appends a new RC_K to the data packet before forwarding it to the target destination node based on the unique ID. In scenarios involving crosscluster communication, the recipient's corresponding CH or AP initiates communication with the TAN, to obtain the recipient's Crt, Prk, $_B$ and $Sprm$. This step serves the crucial purpose of authenticating the recipient's identity. Subsequently, the CH or AP transmits the ciphered message C_m, along with the associated keys, to the intended destination node. Upon receiving the ciphered data packets, the recipient utilizes its Prk_B to decrypt K, thereby retrieving the Sk to decrypt C_m, using the Speck cipher.

In the proposed scheme, the SNs undergo registration and certification facilitated by their respective CHs. When communicating SNs belong to the same cluster, their identities and certificates are stored within that specific CH. This allows the CH to perform centralized authentication of SNs within its cluster.

For SNs belonging to different clusters, the registration process occurs at the respective CHs. These CHs can communicate with the TAN, enabling them to authenticate SNs from other clusters. This mechanism effectively facilitates information-sharing among multiple SNs spanning different clusters within the WSN. Notably, in scenarios involving communication between clusters or with the data server, CHs are not entrusted with the authority to access data and encryption keys. Their role is strictly limited to the management of communication, facilitation of authentication procedures, interaction with the TAN, and execution of the PRE process for the encrypted symmetric key.

V. EXPERIMENTS AND DISCUSSION

This section presents the simulation environment and parameters used, including a performance evaluation of the proposed PRE scheme in terms of execution time,

computational cost, and power consumption. Finally, the security analysis of the scheme considers common attacks targeting WSNs.

A. SIMULATION AND PARAMETER SETTINGS

A simulated WSN environment was established utilizing the NS2 simulator to implement and assess the proposed PRE scheme. The specifications of this simulated environment are detailed in Table 2, where we outline various parameters, including WSN area size, number of sensor nodes, simulation time, modulation standard, and other key factors influencing the simulation. Moreover, the simulations were executed on hardware equipped with an Intel Core i5-2450M 2.5 GHz CPU, 3 MB Cache, and 4 GB RAM. The WSN, covering a square area of 400 × 400 m^2, comprised varying numbers of SNs.

TABLE 2. Simulation parameter specifications.

Parameter	Value
WSN area size	400m × 400m
Number of sensor nodes	50 to 250 SNs
Simulation time	250 sec
Modulation standard	Zigbee/IEEE 802.15.4
Max data rates	250 kbps
Packet size	6400 bits
Control message size	200 bits
Initial power	3 J (joule)
Transmit/receive power level	50 nJ/bit
Power consumption per block size	0.001 for 32 bits
Power consumption per round	0.001 J
Data aggregation power	5 nJ/bit/signal
Free space loss	10 J/bit

In these experiments, all SNs were configured to transmit data to the CHs using Zigbee/IEEE 802.15.4 communication protocol. For consistency, we adopted the default simulation parameters with specific parameter values. To ensure robustness, the recorded results represent the averages obtained from 30 distinct runs of the proposed method.

The proposed PRE scheme places significant emphasis on enhancing the security of SNs, data transmission, and sharing within networks, further prioritizing energy efficiency improvement and extension of WSN's lifetime. To assess the performance of the proposed scheme, the following key metrics were employed:

- Cryptographic efficiency: Rigorous evaluation involved measuring and comparing execution times of the proposed lightweight encryption, re-encryption, and decryption methods against traditional encryption algorithms. This comparison enabled a detailed understanding of the scheme's computational overhead and processing efficiency.
- Node power consumption: Simulations were conducted across diverse timeframes to assess the scheme's impact on power consumption across SNs and CHs, juxtaposing these results with standard operating scenarios. The analysis included considerations of power consumption patterns concerning different data packet volumes and transmission durations.
- Network throughput and lifetime: Aiming to elevate WSN throughput while streamlining encryption processes, our assessment evaluated the scheme's influence on WSN lifetime, thoroughly comparing it with full encryption, re-encryption, and decryption approaches across generated data. Additionally, varying initial power settings were meticulously considered to scrutinize their impact on the network lifetime, effectively representing the duration of nodes' power consumption.

B. PERFORMANCE EVALUATION

In our evaluation, a sequence of simulation experiments was carried out to evaluate the proposed PRE scheme. In the initial simulation scenario, we investigated the impact of the encryption, re-encryption, and decryption methods on processing times when employing the proposed PRE scheme, comparing them with those of full data encryption using standard ciphers, such as AES-256 and RSA-1024. The analysis included measuring cryptographic execution times, keeping the encryption parameters constant while gradually increasing the data size. The simulation was initiated at 30 s, involving 50 SNs and 4 CHs.

In the initial data exchange, a 16 KB data message was transmitted between an SN and its corresponding CH, with the data size incrementally increased afterward. The total processing time for the SN, denoted as ΔT_{SN}, encompasses multiple components, including the time required for the SN to generate a transmission request, transmit the data packet, perform symmetric encryption of m, and execute asymmetric encryption of k, as expressed in Equation (1).

$$\Delta T_{SN} = T(SymEnc(m)) + T(AsymEnc(K)) + T(TranDP) \tag{1}$$

For the CH, the total time includes the time required to authenticate the SN, communicate with the TAN, reencrypt K, and transmit the data packet to the next entity, as expressed in Equation (2). During the communication with TAN, encryption keys and parameters are acquired.

$$\Delta T_{CH} = T(Auth(SN) + (TranTAN) + T(ReEnc(K)) + T(TranDP) \tag{2}$$

Figure 3 presents an overview of the total processing time associated with the cryptographic processes in the proposed scheme using different payload data sizes. The SN consistently demonstrates remarkable efficiency, maintaining an average ΔT_{SN} of 171 ms in executing the operations detailed in Equation (1). This achievement remains unaffected by potential network latency considerations. Meanwhile, the CH exhibits commendable performance, maintaining an almost constant ΔT_{CH} of 28 ms while executing the tasks outlined in Equation (2).

By contrast, the recipient entity requires an average processing time of 126 ms to retrieve messages of the same data size. The throughput performance of the proposed PRE scheme was further evaluated for transactions per second (TPS) rates, ranging from 20 to 200. The evaluation began at a throughput rate of 20 TPS using a 16 KB payload for a duration of 60 s. Subsequently, the send rate was gradually increased to 200 TPS. This comprehensive evaluation allowed benchmarkng the proposed scheme's performance against standard TPS transmission, which served as the baseline without encryption. Figure 4 illustrates the evaluation outcomes. On average, the proposed scheme exhibits approximately 42% lower throughput than standard transmission.

These results emphasize the substantial impact of the encryption and re-encryption processes on data transmission efficiency with the proposed scheme. They also highlight the inherent tradeoff between security enhancement and data throughput, particularly in data-intensive applications within WSNs.

As part of the comparative analysis, we introduced the AES and Rivest-Shamir-Adleman (RSA) ciphers into the simulation network, to simulate the conventional encryption scenario commonly used in most studies not involving PRE. This allowed assessing the respective execution times in comparison to those of the proposed PRE method. In this non-proxy re-encryption approach, the SN uses AES-256 to encrypt the complete message before transmission. Additionally, RSA-1024 is used at the same node to re-encrypt the entire symmetrical ciphertext for intracluster communication. Subsequently, at the destination node, both RSA and AES ciphers were employed for decryption, and AES decrypted the symmetric ciphertext and RSA to recover the original message. Figure 5 presents a comparison of the execution times for the proposed PRE scheme with that of the conventional non-proxy re-encryption approach across various data payload sizes.

From the results, it is evident that the proposed PRE scheme significantly reduces the processing time by approximately 64% compared to the non-proxy re-encryption approach that utilizes standard ciphers. This remarkable reduction in processing time can be attributed to the efficient performance of the lightweight ciphers employed in cryptographic operations.

Moreover, the proposed scheme significantly minimizes the computational and communication burden on the CH during the re-encryption process, focusing solely on encrypting the symmetric key. Consequently, our approach is more resource efficient considering the extensive workload associated with the complete re-encrypting of payload data.

Another important aspect to consider is the power consumption of the SNs during PRE operations. The overall power consumption, denoted as Pw, is obtained by multiplying the power usage of a node by the time required to complete each operation, as outlined in Equation (1) for SNs, and Equation (2) for CHs when transmitting a message m to the destination node. The total Pw of an SN in our scheme was calculated by simulating the operation for 30 s across

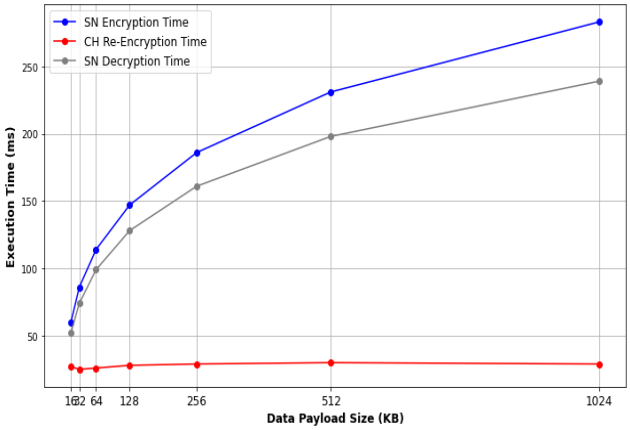


FIGURE 3. Analysis of total execution time for cryptographic processes in the proposed PRE scheme.

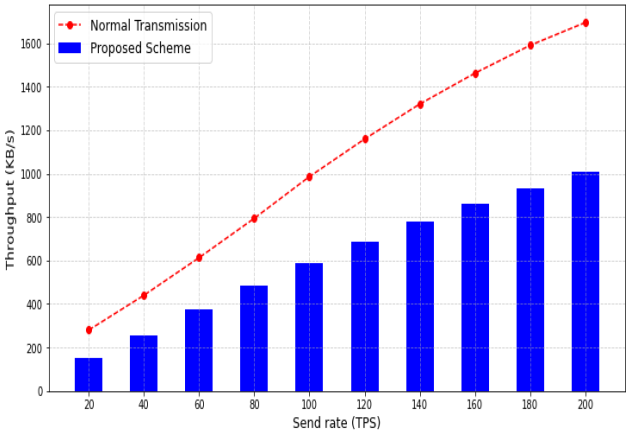


FIGURE 4. Analyzing throughput rates of the proposed PRE scheme vs. standard transmission without encryption under various TPS settings.

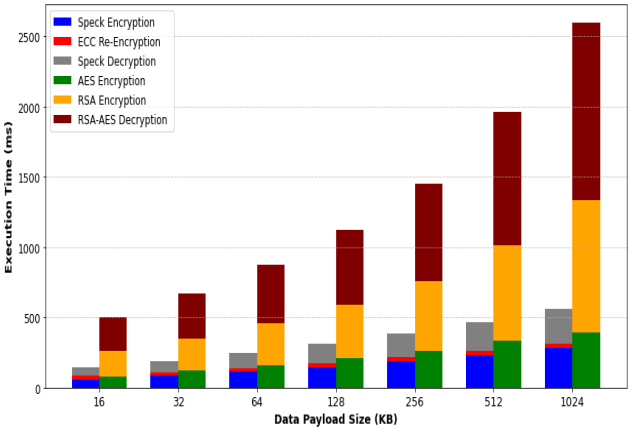


FIGURE 5. Comparative execution times of proposed PRE scheme vs. non-proxy re-encryption approach.

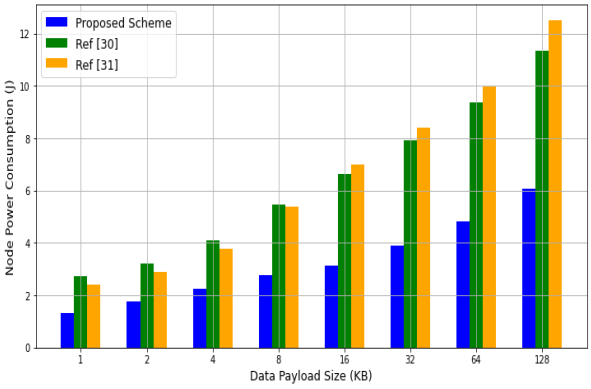
various payload sizes. These results were then compared with those obtained from the related PRE schemes, as illustrated in Figure 6(a).

The proposed PRE scheme demonstrates a significantly reduced *Pw* compared to related schemes. On average, our scheme consumes 3.32 J, with 46% of the total power used by SN for data encryption and transmission within the simulation timeframe. The CH incurs an average *Pw* of 13% for the re-encryption process, with an average *Pw* expenditure of 41% during the SN decryption process. Notably, these power-consuming processes exhibit a direct correlation with the number of data packets involved. In contrast, IoT nodes that follow the PRE schemes in [30] and [31], exhibit average *Pw* levels of 6.28 J and 6.23 J, respectively, during data exchange with destination nodes. These schemes require more power because of the significant resource investment necessary for asymmetric PRE.

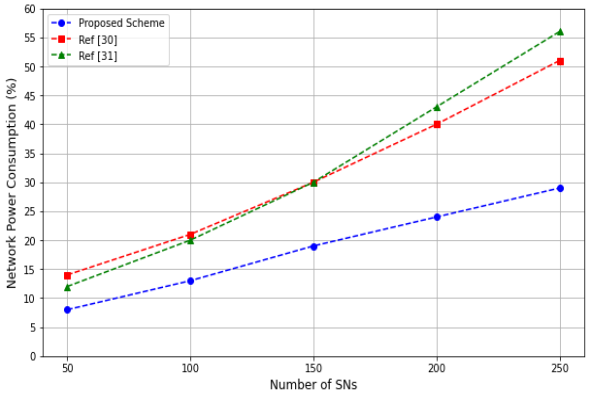
In the following simulation, the network's *Pw* and lifetime are analyzed using the proposed scheme and then compared with those of the schemes presented in [30] and [31]. This analysis involved variations in the number of SNs, simulation times, and the number of data sharings between SNs, as depicted in Figures 6 (b), (c), and (d), respectively. The results in Figure 6(b) indicate that the proposed scheme can effectively reduce the network *Pw* by approximately 40% for all SNs as compared to the schemes in [30] and [31]. Next, the simulation time was gradually increased from 30 s to 150 s to allow for full power consumption at some SNs, and then the impact on the network *Pw* was analyzed.

The results in Figure 6 (c) indicate that the proposed scheme reduces network power consumption by approximately 31.5% and 33% compared with the schemes in [30] and [31], respectively. Subsequently, we analyzed the impact of increasing the amount of data sharing between SNs in different clusters on the network lifetime using the proposed PRE scheme and compared it with those of related PRE schemes. The results in Figure 6(d) show that the network lifetime changes from 11 s to 29 s as the number of data shares is increased from 50 to 250, regardless of any network latency issues. The change in network lifetime is almost doubled in schemes [30] and [31], when the number of sharings reaches 250. This is attributed to the increased power consumption during PRE operations, which escalates as the amount of data shared among the nodes increases.

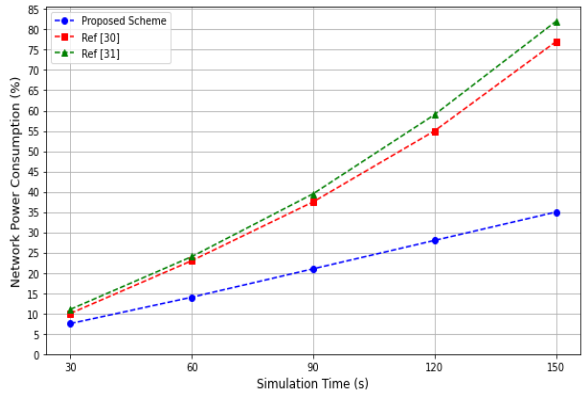
The proposed PRE scheme enhances scalability through the use of lightweight cryptographic methods, ensuring data integrity while conserving CHs′ power resources. The integration of a TAN streamlines key distribution, accommodating increased node counts and data transmissions within the WSN. Unique key implementation for each session among SNs fortifies security and averts network-wide risks associated with key compromise, allowing for network expansion without vulnerabilities from shared or static keys.



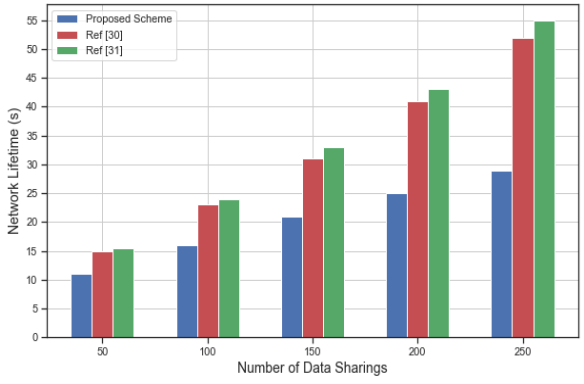
(a): Node power consumption for different data sizes·



(b): Percentage of network power consumption vs. number of SNs.



(c): Percentage of network power consumption vs. simulation time.



(d): Network lifetime vs. number of sharings between SNs.

FIGURE 6. Analyzing the impact of the proposed PRE scheme on SN network power consumption and lifetime, compared to related schemes.

Dynamic key management tailored to session or data contexts reduces distribution overhead, efficiently managing larger node counts. Additionally, the adoption of hierarchical or distributed key management systems reinforces scalability, handling cryptographic operations across expanding node networks for secure communications amid evolving WSN demands.

With the innovative design of assigning the responsibility for PRE tasks to different CHs across the WSN, our scheme effectively mitigates limitations inherent in existing schemes that rely on a single connected cloud server. This decentralized approach addresses concerns related to load balancing and single points of failure, diverging from centralized designs. Our scheme offers a more scalable and fault-tolerant solution, especially as the number of connected sensors increases. Unlike centralized cloud servers, our approach allocates the computational load across the network, enhancing scalability and resilience with the lowest impact on overall system performance.

C. SECURITY ANALYSIS

In this section, the security robustness of the proposed PRE scheme is explored to evaluate its resilience to common attacks targeting WSNs. The evaluation focuses on its effectiveness in establishing secure communication and data sharing within the network while meeting stringent security requirements.

To provide comprehensive insights into our system's security, our analysis prioritized addressing prevalent threats such as Sybil attacks, data tampering, eavesdropping, and man-in-the-middle attacks. Our methodologies revolved around employing cryptographic verification, implementing end-to-end encryption, validating signatures, and generating unique cryptographic keys. Through systematic evaluation, these measures were rigorously tested against potential vulnerabilities. Through systematic evaluation, these measures underwent rigorous testing against potential vulnerabilities.

In the proposed PRE scheme, each SN within a cluster is assigned a unique ID associated with a CH. This ID serves as a means of verifying the authenticity of a node. In addition, the trustworthiness of the SN identity is maintained through its corresponding verification process.

To ensure the security of the data shared between the SNs, we implemented end-to-end encryption and utilized cryptographic keys. These keys are uniquely generated by the TAN and securely transmitted to the specific nodes involved in each transmission session. In addition, a dual-phase authentication process was employed. In the first phase, SN and its associated CH are authenticated to ensure that each SN is validated before any data transmission takes place. In the second phase, the CH verifies the authenticity of the destination SN or AP before initiating re-encrypted data transmission.

The encryption keys and authentication parameters are exclusively owned by authorized entities, and their legitimacy is confirmed by the recipient's ability to decrypt the K linked to each data packet. Data confidentiality is protected using asymmetric encryption through the public key of the data owner, thereby preventing unauthorized access by the CH and other entities. Moreover, only the verified CHs with unique IDs receive the rk from the TAN. This prevents unauthorized CHs from accessing the keys or engaging in re-encryption for transmission. Consequently, as messages are transmitted exclusively through authenticated nodes, it is extremely challenging for an attacker to impersonate legitimate SNs or CHs in potential data transmissions involving tampered or falsified data.

Each SN has a single registered ID along with a Crt and key pair. The message signing process requires both DS and the sender's Crt to be utilized. Because SN identities are inherently linked to their respective CH and TAN, this design effectively prevents adversaries from creating new identities to initiate Sybil attacks. Ensuring data integrity in our WSN transmission is crucial for preventing tampering with malicious nodes. This is achieved through a DS_{SN} generated using the hash of the sender's Pk_{SN}. These verification codes are attached to encrypted data packets. At the destination node, hash-based verification is used to validate the authenticity codes and ensure data integrity. The matching signatures not only confirm the integrity of the data but also verify whether they match the expected values. The receiver cannot generate a valid signature without knowledge of the hash value. Any incorrect DS is detected, signifying unauthorized changes to the data by the receiving entity, thus demonstrating the robust maintenance of data integrity within the proposed scheme.

Every data transmission in our scheme is combined with the Crt, thereby preventing SNs from denying message authenticity or falsely attributing actions to others with authorized SNs using their unique $Crts$ to exclusively sign their messages, allowing recipients to verify the sender's identity for non-repudiation.

In addition, because the TAN is the sole authority responsible for generating encryption keys and parameters for various nodes, and each encryption session employs a unique random value r within the $Sprm$, the creation of redundant key components becomes meaningless. Thus, collusion attempts involving malicious SNs or CHs cannot lead to the acquisition of the decryption key. Consequently, our scheme effectively resists collusion and repudiation attempts.

In case of an adversary attempting to recover the encryption keys and parameters of the transmitted data from an SN through brute-force attacks, each piece of data, transmitted or shared, undergoes encryption and reencryption using a distinct set of keys generated by the TAN. Moreover, each Sk is encrypted using a unique Pk associated with a specific SN. As a result, it becomes computationally infeasible for an adversary to deduce the correct values of the $Sk, r\ k, P\ k$, and Prk keys necessary to recover other data associated with the same SN or any other node using brute-force attacks. The complexity of guessing the random values of the keys required to decrypt the data makes

TABLE 3. Comparative analysis of proposed and related PRE schemes for constrained networks.

Feature	Ref [30]	Ref [31]	Ref [32]	Ref [24]	Proposed Scheme
PRE-cryptography	Lightweight asymmetric encryption	Lightweight asymmetric encryption	lightweight Asymmetric encryption	Lightweight asymmetric encryption	Lightweight symmetric and asymmetric encryption
Scheme environment	IoT networks	IoT networks	IoT-enabled smart grid	IoT-based Blockchain	WSNs
Authentication effectiveness	Moderate	Moderate	Strong	Strong	Strong
Data integrity	No	No	Yes	Yes	Yes
Network attack resistance	Moderate	Moderate	Moderate	Strong	Strong
Collusion and repudiation resistance	Moderate	Poor	Moderate	Moderate	Strong
Execution performance	Moderately efficient	Moderately efficient	Moderately efficient	Low efficiency	Highly efficient
Energy efficiency	Moderately expensive	Moderately expensive	Moderately expensive	Relatively expensive	Inexpensive

this exceptionally challenging. Consequently, the proposed PRE scheme demonstrates robust security against brute-force attacks. Considering the possibility of an adversary eavesdropping or acting as a man-in-the-middle to intercept communication traffic between SN, CH, and AP, even a malicious adversary would encounter significant challenges in achieving their objectives. Deciphering secret parameters, including the random r and secret v values, presents a formidable challenge. Furthermore, the retrieval of the Prk and ECC points of an entity is considered impossible for malicious adversaries because of their inability to compute randomly generated high-entropy ECC points for this purpose. Thus, our scheme is robust in protecting against eavesdropping and man-in-the-middle attacks.

Data freshness involves verifying that a received message is recent and has not been subject to reuse or replay by a potential threat. To safeguard a network from potential replay attacks, message freshness must be authenticated within a transmission counter or a defined timeframe. In our scheme, a monotonically increasing counter is employed for communication between SNs and a CH, as well as between CHs and the AP. This counter guarantees that messages have been sent recently and prevents adversaries from replaying old messages from SNs or re-encrypting data from CHs, thereby preserving the freshness of the data. Table 3 presents a comparative analysis of the security and efficiency features of the proposed PRE scheme and those of other PRE schemes designed for constrained networks.

This comprehensive assessment unequivocally confirms the system's robustness in mitigating significant security threats commonly encountered during data exchange in WSN environments. It strongly affirms the efficacy of our strategies in fortifying the system against vulnerabilities. Furthermore, the implementation of these measures underscores the system's adeptness in preserving data integrity and confidentiality, demonstrating resilience even in diverse and challenging scenarios.

VI. CONCLUSION

This paper presented an innovative PRE scheme designed to address the unique challenges encountered in WSNs. The PRE is tailored between CHs to facilitate secure intra- and inter-cluster communication, data sharing, and authentication among WSN nodes. To optimize efficiency and conserve resources, the proposed design is adept in managing the cryptographic computational overhead through a balanced combination of lightweight symmetric and asymmetric encryption techniques. The Speck symmetric encryption was employed to secure the SN data, whereas re-encryption relied on ECC to handle the symmetric encryption keys attached to the ciphertext. Moreover, an efficient key management technique was designed to ensure secure key generation, distribution, and freshness in the dynamic WSN environment.

The evaluation results robustly validate the efficacy of our tailored PRE scheme in WSNs, demonstrating its ability to significantly enhance encryption, re-encryption, and decryption performance while minimizing the strain on the constrained resources of SNs. Moreover, our scheme exhibits remarkable scalability, effectively addressing challenges commonly associated with centralized-based PRE approaches. Additionally, by distributing PRE tasks across the WSN, our design adeptly mitigates the risk of a single point of failure, enhancing the overall robustness and reliability of the system. The evaluation results demonstrate a notable 40% reduction in SN power consumption and a 32% decrease in overall network power consumption compared to existing PRE solutions designed for resource-constrained environments. The substantial processing time reduction in our PRE scheme, attributed to lightweight and proxy re-encryption methods, amplifies CH efficiency while maintaining robust security measures. Security analyses confirmed the scheme's proficiency in meeting essential security requirements, including confidentiality, authentication, integrity, and resilience against collusion and repudiation.

The proposed scheme exhibits robustness against common WSN threats, such as replay, Sybil, man-in-the-middle, and brute-force attacks.

Future research will focus on further enhancing the applicability of the proposed PRE scheme to resource-constrained WSNs, which would involve exploring real-world deployment scenarios and investigating the scalability and performance of the scheme in specific WSN environments.

ACKNOWLEDGMENT

The authors gratefully acknowledge the Rabdan Academy for their invaluable support and resources provided throughout this research, which significantly contributed to its successful completion.

REFERENCES

[1] O. A. Khashan, R. Ahmad, and N. M. Khafajah, "An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks," *Ad Hoc Netw.*, vol. 115, Apr. 2021, Art. no. 102448.

[2] O. A. Khashan, S. Alamri, W. Alomoush, M. K. Alsmadi, S. Atawneh, and U. Mir, "Blockchain-based decentralized authentication model for IoT-based E-learning and educational environments," *Comput., Mater. Continua*, vol. 75, no. 2, pp. 3133–3158, 2023.

[3] I. Mashal, O. A. Khashan, M. Hijjawi, and M. Alshinwan, "The determinants of reliable smart grid from experts' perspective," *Energy Informat.*, vol. 6, no. 1, pp. 1–23, Apr. 2023.

[4] O. A. Khashan and N. M. Khafajah, "Efficient hybrid centralized and blockchain-based authentication architecture for heterogeneous IoT systems," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 35, no. 2, pp. 726–739, Feb. 2023.

[5] A. Sufyan, K. B. Khan, O. A. Khashan, T. Mir, and U. Mir, "From 5G to beyond 5G: A comprehensive survey of wireless network evolution, challenges, and promising technologies," *Electronics*, vol. 12, no. 10, p. 2200, May 2023.

[6] F. H. El-Fouly, M. Kachout, Y. Alharbi, J. S. Alshudukhi, A. Alanazi, and R. A. Ramadan, "Environment-aware energy efficient and reliable routing in real-time multi-sink wireless sensor networks for smart cities applications," *Appl. Sci.*, vol. 13, no. 1, p. 605, Jan. 2023.

[7] Z. A. Zukarnain, O. A. Amodu, C. Wenting, and U. A. Bukar, "A survey of Sybil attack countermeasures in underwater sensor and acoustic networks," *IEEE Access*, vol. 11, pp. 64518–64543, 2023.

[8] O. A. Khashan, N. M. Khafajah, W. Alomoush, M. Alshinwan, S. Alamri, S. Atawneh, and M. K. Alsmadi, "Dynamic multimedia encryption using a parallel file system based on multi-core processors," *Cryptography*, vol. 7, no. 1, p. 12, Mar. 2023.

[9] K. Jain, P. S. Mehra, A. K. Dwivedi, and A. Agarwal, "SCADA: Scalable cluster-based data aggregation technique for improving network lifetime of wireless sensor networks," *J. Supercomput.*, vol. 78, pp. 13624–13652, Mar. 2022.

[10] O. A. Khashan, "Parallel proxy re-encryption workload distribution for efficient big data sharing in cloud computing," in *Proc. IEEE 11th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2021, pp. 554–559.

[11] M. Su, B. Zhou, A. Fu, Y. Yu, and G. Zhang, "PRTA: A proxy re-encryption based trusted authorization scheme for nodes on CloudIoT," *Inf. Sci.*, vol. 527, pp. 533–547, Jul. 2020.

[12] S. M. Patil and B. R. Purushothama, "Non-transitive and collusion resistant quorum controlled proxy re-encryption scheme for resource constrained networks," *J. Inf. Secur. Appl.*, vol. 50, Feb. 2020, Art. no. 102411.

[13] O. A. Khashan, "Hybrid lightweight proxy re-encryption scheme for secure fog-to-things environment," *IEEE Access*, vol. 8, pp. 66878–66887, 2020.

[14] G. Kan, C. Jin, H. Zhu, Y. Xu, and N. Liu, "An identity-based proxy re-encryption for data deduplication in cloud," *J. Syst. Archit.*, vol. 121, Dec. 2021, Art. no. 102332.

[15] N. H. Sultan, V. Varadharajan, L. Zhou, and F. A. Barbhuiya, "A role-based encryption (RBE) scheme for securing outsourced cloud data in a multi-organization context," *IEEE Trans. Services Comput.*, vol. 16, no. 3, pp. 1647–1661, Jun. 2023.

[16] H. Deng, Z. Qin, Q. Wu, Z. Guan, and Y. Zhou, "Flexible attribute-based proxy re-encryption for efficient data sharing," *Inf. Sci.*, vol. 511, pp. 94–113, Feb. 2020.

[17] Y. Lu and J. Li, "A pairing-free certificate-based proxy re-encryption scheme for secure data sharing in public clouds," *Future Gener. Comput. Syst.*, vol. 62, pp. 140–147, Sep. 2016.

[18] D. Nuñez, I. Agudo, and J. Lopez, "Proxy re-encryption: Analysis of constructions and its application to secure access delegation," *J. Netw. Comput. Appl.*, vol. 87, pp. 193–209, Jun. 2017.

[19] N. Doshi and R. Patel, "An improved approach in CP-ABE with proxy re-encryption," *e-Prime-Adv. Electr. Eng.*, vol. 2, Jan. 2022, Art. no. 100042.

[20] N. Doshi, "An enhanced approach for CP-ABE with proxy re-encryption in IoT paradigm," *Jordanian J. Comput. Inf. Technol.*, vol. 8, no. 3, p. 1, 2022.

[21] H.-Y. Lin and Y.-M. Hung, "An improved proxy re-encryption scheme for IoT-based data outsourcing services in clouds," *Sensors*, vol. 21, no. 1, p. 67, Dec. 2020.

[22] K. T. Nguyen, N. Oualha, and M. Laurent, "Authenticated key agreement mediated by a proxy re-encryptor for the Internet of Things," in *Proc. Eur. Symp. Res. Comput. Secur.*, Heraklion, Greece, 2016, pp. 339–358.

[23] H. Hong and Z. Sun, "Sharing your privileges securely: A key-insulated attribute based proxy re-encryption scheme for IoT," *World Wide Web*, vol. 21, no. 3, pp. 595–607, May 2018.

[24] K. O. O. Agyekum, Q. Xia, E. B. Sifah, C. N. A. Cobblah, H. Xia, and J. Gao, "A proxy re-encryption approach to secure data sharing in the Internet of Things based on blockchain," *IEEE Syst. J.*, vol. 16, no. 1, pp. 1685–1696, Mar. 2022.

[25] A. Manzoor, A. Braeken, S. S. Kanhere, M. Ylianttila, and M. Liyanage, "Proxy re-encryption enabled secure and anonymous IoT data sharing platform based on blockchain," *J. Netw. Comput. Appl.*, vol. 176, Feb. 2021, Art. no. 102917.

[26] Y. Chen, B. Hu, H. Yu, Z. Duan, and J. Huang, "A threshold proxy re-encryption scheme for secure IoT data sharing based on blockchain," *Electronics*, vol. 10, no. 19, p. 2359, Sep. 2021.

[27] Z. Qin, H. Xiong, S. Wu, and J. Batamuliza, "A survey of proxy re-encryption for secure data sharing in cloud computing," *IEEE Trans. Services Comput.*, early access, Apr. 6, 2016, doi: 10.1109/TSC.2016.2551238.

[28] L. Ferretti, M. Marchetti, and M. Colajanni, "Fog-based secure communications for low-power IoT devices," *ACM Trans. Internet Technol.*, vol. 19, no. 2, pp. 1–21, Mar. 2019.

[29] A. Vishwanath, R. Peruri, and J. He, *Security in Fog Computing Through Encryption*. Kennesaw, GA, USA: DigitalCommons@ Kennesaw State Univ., 2016.

[30] A. A. Diro, N. Chilamkurti, and Y. Nam, "Analysis of lightweight encryption scheme for fog-to-things communication," *IEEE Access*, vol. 6, pp. 26820–26830, 2018.

[31] S. Kim and I. Lee, "IoT device security based on proxy re-encryption," *J. Ambient Intell. Humanized Comput.*, vol. 9, no. 4, pp. 1267–1273, Aug. 2018.

[32] S. Hussain, I. Ullah, H. Khattak, M. Adnan, S. Kumari, S. S. Ullah, M. A. Khan, and S. J. Khattak, "A lightweight and formally secure certificate based signcryption with proxy re-encryption (CBSRE) for Internet of Things enabled smart grid," *IEEE Access*, vol. 8, pp. 93230–93248, 2020.

[33] O. A. Khashan, "Secure outsourcing and sharing of cloud data using a user-side encrypted file system," *IEEE Access*, vol. 8, pp. 210855–210867, 2020.

[34] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, "The Simon and SPECK lightweight block ciphers," in *Proc. 52nd Annu. design Autom. Conf.*, 2015, pp. 1–6.

[35] I. Batra, S. Verma, Kavita, and M. Alazab, "A lightweight IoT-based security framework for inventory automation using wireless sensor network," *Int. J. Commun. Syst.*, vol. 33, no. 4, Mar. 2020, Art. no. e4228.

[36] Y. Al-Aali and S. Boussakta, "Lightweight block ciphers for resource-constrained devices," in *Proc. 12th Int. Symp. Commun. Syst., Netw. Digit. Signal Process. (CSNDSP)*, Jul. 2020, pp. 3–25.

[37] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inf. Theory*, vol. IT-31, no. 4, pp. 469–472, Jul. 1985.

[38] A. J. Menezes and S. A. Vanstone, "Elliptic curve cryptosystems and their implementation," *J. Cryptol.*, vol. 6, no. 4, pp. 209–224, Sep. 1993.

[39] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comput.*, vol. 48, no. 177, pp. 203–209, 1987.

[40] V. S. Miller, "Use of elliptic curves in cryptography," in *Proc. Conf. Theory Appl. Cryptograph. Techn.*, 1985, pp. 417–426.
[41] D. Freeman, M. Scott, and E. Teske, "A taxonomy of pairing-friendly elliptic curves," *J. Cryptol.*, vol. 23, no. 2, pp. 224–280, Apr. 2010.
[42] S. Sujanthi and S. N. Kalyani, "SecDL: QoS-aware secure deep learning approach for dynamic cluster-based routing in WSN assisted IoT," *Wireless Pers. Commun.*, vol. 114, no. 3, pp. 2135–2169, Oct. 2020.
[43] O. A. Khashan and N. M. Khafajah, "Secure stored images using transparent crypto filter driver," *Int. J. Netw. Secur.*, vol. 20, no. 6, pp. 1053–1060, 2018.

OSAMA A. KHASHAN received the M.Sc. degree in information technology from Utara University Malaysia, in 2008, and the Ph.D. degree in computer science from The National University of Malaysia, in 2014. With a diverse academic background, he has held positions at various universities. He is currently an Associate Professor/Associate Researcher with the Research and Innovation Centers, Rabdan Academy, Abu Dhabi, United Arab Emirates. His research interests include information security, cybersecurity, cryptography, blockchain technology, cloud computing, and machine learning.

NOUR M. KHAFAJAH received the B.S. degree in computer science from Al-Balqa Applied University, Jordan, in 2011, and the M.S. degree in information security and assurance from the Islamic Science University of Malaysia, in 2014. She has worked in various universities in Saudi Arabia and Jordan. Her research interests include information and network security, cybersecurity, cryptology, and machine and deep learning.

WALEED ALOMOUSH received the Ph.D. degree from Universiti Kebangsaan Malaysia (UKM), in 2015. He is currently an Assistant Professor with the School of Information Technology, Skyline University College, Sharjah, United Arab Emirates. He has published many research papers in international journals and conferences of high repute. His research interests include data clustering and optimization, and image processing.

MOHAMMAD ALSHINWAN received the Ph.D. degree from the School of Computer Engineering, Inje University, Gimhae, Republic of Korea, in 2017. He was an Assistant Professor with the Department of Computer and Information Sciences, Amman Arab University, Jordan. He is currently an Associate Professor with Applied Science Private University, Jordan. His research interests include computer networks, mobile networks, information security, AI, and optimization methods.