INTERNATIONAL JOURNALS OF ACADEMICS & RESEARCH
(IJARKE Science & Technology Journal)

Secure and Efficient Certificateless Signcryption Protocol for Wireless Body Area Networks (WBANs)

King'ang'i Misheck Murimi, Tharaka University, Kenya
Kirima Daniel Mukathe, Tharaka University, Kenya
Makembo John Majira, Tharaka University, Kenya

Abstract

In WBANs, security and efficiency are critical concerns. Devices communicate via an insecure short-range communication standard, exposing patients' sensitive data to security breaches. Additionally, WBAN entities are resource-constrained devices that demand lightweight computations. Meanwhile, researchers have designed numerous schemes to combat the above-mentioned problems. Nevertheless, several schemes rely on bilinear pairing and certificate management, which are heavy cryptographic operations, thus suffering computational inefficiencies. To resolve security and efficiency issues, we design and validate a secure and efficient certificateless signcryption scheme using elliptic curve cryptography and general hash functions to signcrypt and unsigncrypt messages. Besides, we conduct formal security proof using the Random Oracle Model (ROM) to demonstrate Indistinguishability under Chosen Ciphertext Attack (IND-CCA) and Existential Unforgeability under Chosen Message Attack (EUF-CMA). From the formal security proof, the proposed scheme has proven to be IND-CCA and EUF-CMA secure against adversaries of Type I and Type II. Finally, we conduct efficiency evaluation in terms of computation and communication costs. During performance evaluation, we analyzed the computational and communication costs and compared them with state-of-the-art works, where the proposed scheme showed computation efficiency improvements and communication efficiency improvement against other schemes. Compared to existing schemes, the scheme from this study has better performance in terms of computation and communication cost, thus its applicability in WBANs environment.

Key words: *Certificateless, Signcryption, Confidentiality, Unforgeability*

1. Introduction

The remarkable progress of the Internet of Things (IoT) in recent years has given rise to the wireless body area networks (WBANs), a cutting-edge healthcare system that enables the monitoring of patients' health conditions without the need for constant physician supervision and aids in the diagnosis of diseases. WBAN refers to a wireless network involving the human body, biosensors, application provider, and network manager (as depicted in Figure 1), (Mandal, 2023).

The human body avails physiological data (i.e., body temperature, blood pressure, heart rate, blood sugar level, and Electrocardiogram (ECG)) to biosensors implanted inside or outside the human body. Upon receiving physiological data, the biosensors transmit the data to the application provider for immediate diagnosis and treatment. In addition, WBAN contains an aggregator, such as a mobile device, which is responsible for collecting and aggregating data from multiple biosensors and transmitting it to the application provider (Almuhaideb, 2022).

The network manager acts as a trusted authority mandated for the entire network management, including registration and revocation of entities. The biosensors connect with the aggregator in a star or multi-hop topology, and their communication occurs via the short-range communication standard called IEEE 802.15.6 (Cornet et al., 2022).

WBAN provides numerous benefits to patients and medical service providers, such as real-time and remote health monitoring of patients' conditions for early detection of abnormalities. For instance, WBANs ensure automated health care for people with diabetes by detecting the glucose level and stimulating the insulin pump to release insulin, thus providing automatic dosing in diabetics (Jahan et al., 2023). As a result, the patients and medical service providers save time and resources. Despite the numerous benefits provided by WBANs, the network is coupled with several challenges, some of which are life-threatening.

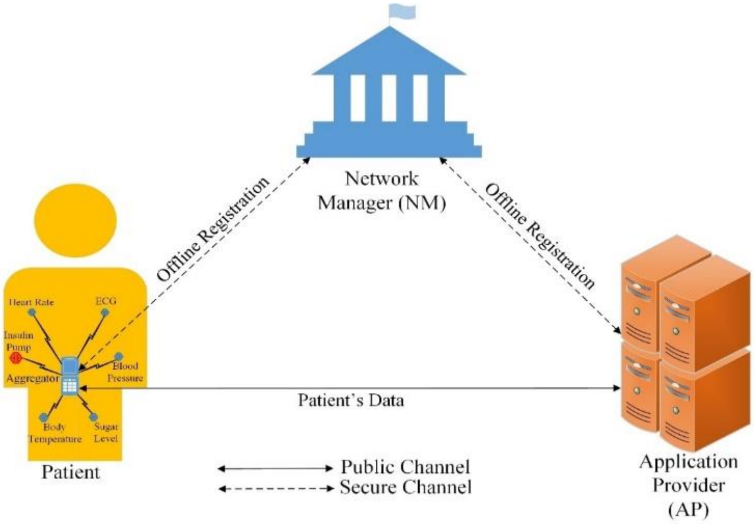

Figure 1: The Propose System Model

1.1 Motivation and Contribution

Firstly, in WBANs, data is transmitted through insecure public channels exposing sensitive data to security risks such as message injection, eavesdropping, message replay, spoofing, and compromise to the integrity of the message (Sama et al., 2022). For instance, data may be altered, leading to wrong diagnosis, posing a risk to patient's safety, and potentially leading to catastrophic consequences. Secondly, the confidentiality of patients' data is required to protect against unauthorized access, which could result in ill purposes such as cybercrimes. Finally, biosensors in WBANs are resource-constrained due to their tiny-size nature, thus limiting their ability to handle highly complex computations while providing efficiency, which is a critical requirement (Mandal, 2022).

Several schemes have been presented to achieve secure communication through an insecure channel. However, many schemes experience security issues coupled with performance overheads. To achieve security for instance, several authors have used heavy cryptographic operations such as those involving bilinear pairing and certificate management, exposing WBAN resource constrained devices to complex computations thus compromising efficiency. On the other hand, several schemes presented to achieve WBAN efficiency lacks confidentiality of patient's data, and identity privacy. Motivated by the above-mentioned challenges, this paper therefore proposes a secure and efficient protocol to signcrypt and unsigncrypt health related messages for WBANs.

Below is a summary of the major challenges facing existing WBAN schemes:

- Certificate management problems
- Bilinear pairing complexities
- Confidentiality issues
- Forgeability problem
- Key escrow problems
- Lack of forward secrecy
- Lack of anonymity
- Vulnerability to common attacks

2. Related Work

Researchers have made significant progress in addressing security issues in WBANs by utilizing public key cryptography (PKC) to design various authentication schemes, which may fall under public key infrastructure (PKI), identity-based cryptography (IBC), and certificateless cryptography (CLC). Zhou (2019) proposed a protocol for mobile health systems based on certificateless signcryption as an improvement to Zhang et al.'s scheme. The author applied certificateless elliptic curve cryptography to achieve confidentiality and unforgeability, as well as improving a little on computation and communication costs compared to the original scheme. However, the scheme is relatively expensive in terms of computation and lacks a conditional anonymity security feature. Liu et al., (2020) designed a streamlined data access control scheme by leveraging the signcryption technique for improved efficiency.

A pairing-free RSA cryptosystem is applied to make the scheme more applicable in the industry in terms of efficiency. Formal analysis proves the scheme resilient to typical security attacks. The scheme, however, lacks anonymity. Ullah et al. (2021) designed a signcryption scheme for the internet of health things based on hyper-elliptic curve certificateless cryptography to achieve anonymity and forward secrecy at the same time. The scheme further proves to achieve confidentiality and unforgeability through formal security analysis in the ROM. Nonetheless, the scheme lacks sender authentication and is a little more expensive computationally.

Xiong et al., (2022) presented a signcryption scheme for flexible heterogeneous WBAN environment. The security of the scheme is achieved by enabling body sensors to encrypt sensitive data using the PKI's management system public key and then uploading it to a server in the cloud, which conducts an equivalence test on the ciphertext. Despite the security achievements of the above-discussed schemes, they suffer from one common problem, i.e., certificate management complexity, which makes them unsuitable for WBANs.

Ramadan et al. (2023) presented an identity-based signcryption protocol for telemedicine systems with an equality test feature. The scheme achieves confidentiality and unforgeability in the ROM. Nevertheless, the scheme suffers from the key escrow problem, high computation and communication costs due to bilinear pairing operations, and a lack of sender authentication. Zhang et al. (2024) proposed a certificateless signcryption scheme for internet of medical things (IoMT) safe data communication based on zero knowledge proof. Their scheme achieves confidentiality and unforgeability, as well as improved communication efficiency compared to other relevant schemes. However, Zhang et al.'s scheme lacks a sender authentication security feature and is expensive in terms of communication and computation.

In summary, the schemes proposed by various authors experience certificate management problem, key escrow problem, and reduced efficiency. To be precise, the major gaps identified from the existing literature include: complex computations due to bilinearly and certificate management, lack of conditional anonymity, key escrow problem, lack of sender authentication, lack of forward secrecy, and lack of unforgeability. Table 1 provides a summary of identified gaps for the literature:

Table 1: Summary of Strengths and Weaknesses of Related Schemes

Scheme	**Approach**	**Strength**	**Weakness**
Xiong et al. 2022	PKI-IBC, bilinear pairing	Achieves message authentication, confidentiality, unforgeability, and forward secrecy.	Lacks sender authentication, conditional anonymity, and incurs high computational and communication cost due to bilinear pairing. Has key-escrow problem.
Zhou 2019	CLC, ECC	Achieves both sender and message authentication, confidentiality, and unforgeability	High computation cost, lacks conditional anonymity.
Liu et al. 2020	CLC, bilinear pairing	Achieves message authentication, confidentiality, and solves key escrow issue	Lacks unforgeability, sender authentication, forward secrecy, and conditional anonymity. Incurs high computation cost due to bilinear pairing operation.
Ullah et al. 2021	CLC, ECC	Achieves message authentication, confidentiality, unforgeability, and solves key-escrow problem.	Lacks sender authentication, relatively high computation cost
Ramadan et al. 2023	IBC, bilinear pairing	Achieves message authentication, confidentiality, unforgeability, and forward secrecy.	Lacks sender authentication, Key-escrow resistance, and conditional anonymity. High computation and communication cost due to bilinear pairing approach.
Zhang et al. 2024	CLC, ECC	Achieves both sender and message authentication, confidentiality, unforgeability, forward secrecy, and solves key-escrow problem.	Lacks conditional anonymity, relatively high computational cost.

2.1 Mathematical Preliminaries

The fundamental mathematical concepts used in the proposed scheme are discussed below:

2.1.1 Elliptic Curve Group

An elliptic curve E over a prime finite field F_P is defined by an equation $y^2 = x^2 + ax + b$ where $a, b \in F_P$ and $4a^3 + 27b^2 \neq 0$. Then $G = \{(x, y): x, y \in F_P, E(x, y) = 0\} \cup \{O\}$ is the additive elliptic curve where O is the point at infinity (Mandal, 2022). Figure 2 shows an elliptic curve.

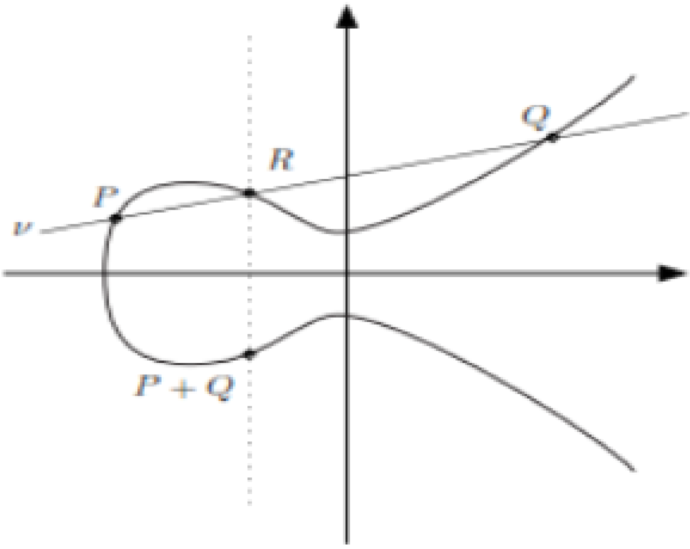

Figure 2: Elliptic Curve
Source: (Kasyoka, 2022)

2.1.2 Point Addition

Taking P, Q as two points on the curve, such that $P + Q = R$, and $-R$ is a third point where the line joining P and Q intersects the curve, then point R is the reflection of $-R$ on x-axis (Mandal, 2022).

2.1.3 Scalar Multiplication

If point P is a generator of cyclic additive group G. Then, $kP = P + P + \cdots + P(k \text{ times})$ where $k \in \mathbb{Z}_q^*$ (Ali et al., 2021).

2.1.4 Computationally Hard Problems

The security of ECC relies on the computational difficulty of solving the discrete logarithm problem, which entails determining the exponent (scalar) when given a base point and the resulting point on the curve, and computational Diffie-Helman Problem (CDHP) which involves computing a third point from two given points as demonstrated below:

i. Elliptic Curve Discrete Logarithm Problem (ECDLP)

Given points $P, Q \in G$, to find an integer $x \in Z_q^*$ such that $Q = xP$. It is hard to compute x from P and Q by an algorithm that is polynomial time bounded. (Yang et al., 2022).

ii. Computational Diffie-Hellman Problem (CDHP)

Given an elliptic curve E defined over a finite field $GF(p)$, a point $P \in E$ of order n, $A = aP$, $B = bP$, it is computationally hard to find to find the point $C = abP$ (Zhang et al., 2021). The problems are believed to be computationally infeasible to solve efficiently.

3. The Proposed Signcryption Scheme

In this section, the proposed ECC-based secure and efficient certificateless signcryption protocol for a wireless body area network is presented. The protocol entails four major algorithms, i.e., setup, registration and key generation, message signcryption, and message unsigncryption. Table 2 provides a description of the notations used in the proposed scheme.

Table 2: Notations used in the Proposed Scheme

NOTATION	DESCRIPTION
p and q	Large prime numbers
$\boldsymbol{G}$	Group of elliptic curve points
$\boldsymbol{E}$	Non-singular elliptic curve
$\{\boldsymbol{s_{NM}}, \boldsymbol{PK_{NM}}\}$	NM's master and public keys
$\{\boldsymbol{H_0}(.),\boldsymbol{H_1}(.),\boldsymbol{H_2}(.),\boldsymbol{H_3}(.)\}$	General One-way hash functions
$\boldsymbol{PD_i}$	Patient's device
$\{\boldsymbol{RID}_{\boldsymbol{PD_i}}, \boldsymbol{PID}_{\boldsymbol{PD_i}}\}$	$PD's$ real identity and pseudo identity
$\{\boldsymbol{\omega_i}, \boldsymbol{\theta_i}\}$	Secret key for PD_i and AP
$\{\boldsymbol{T_i}, \boldsymbol{t_i}\}$	Valid time periods
$\oplus$	XOR operation
$\{\boldsymbol{d_{PD_i}}, \boldsymbol{d_{AP}}\}$	NM's secret key for PD_i and AP PPK generation
$\{\boldsymbol{PPK_{PD_i}}, \boldsymbol{PPK_{AP}}\}$	Partial private keys for PD_i and AP
$\{\boldsymbol{x_{PD_i}}, \boldsymbol{x_{AP}}\}$	PD_i and AP secret key for private key generation
$\boldsymbol{r_{PD_i}}$	PD_i's secret key for message signcryption
$\{\boldsymbol{SK_{PD_i}}, \boldsymbol{PK_{PD_i}}\}$	Private and Public key for PD_i
$\{\boldsymbol{SK_{AP}}, \boldsymbol{PK_{AP}}\}$	Private and public key for AP
$\boldsymbol{\varrho}$	Signcryption
$\perp$	Error
$\{\boldsymbol{m_{PD_i}}, \boldsymbol{m_{AP}}\}$	PD_i and AP message

3.1 Setup

The Network Manager(NM) solely initializes the system by performing the following.

i. Inputs $\lambda \in Z^+$as security parameter, randomly picks two large prime numbers p and q, and non-singular elliptic curve E defined by the equation $y^2 = x^2 + ax + b$, where $a, b \in F_P$ and $4a^3 + 27b^2 \neq 0$.

ii. Selects a generator P for group G, where G are elliptic curve points with prime order q. P and q are supposed to be large prime numbers to enhance security.

iii. Randomly picks $s_{NM} \in \mathrm{Z}_q^*$ as its master secret key, and computes its public key as $PK_{NM} = s_{NM}P$.

iv. Randomly picks four one-way hash functions: $H_0: \{0,1\}^* \to \mathrm{Z}_q^*$, $H_1: G \times G \times G \to \mathrm{Z}_q^*$, $H_2: G \to \mathrm{Z}_q^*$, $H_3: G \times \{0,1\}^* \times G \times G \times G \to \mathrm{Z}_q^*$.

v. Finally, the NM publicly publishes system parameters $params$ as $\{p, q, G, P, PK_{NM}, H_0, H_1, H_2, H_3\}$

3.2 Registration and Key Generation

3.2.1 PD Registration

The guide for PD registration is outlined below.

i. The PD randomly chooses $\omega_i \in \mathrm{Z}_q^*$ and computes $PID_{i1} = \omega_i P$.

ii. The PD picks its real-identity RID_{PD_i} and sends tuple $\{PID_{i1}, RID_{PD_i}\}$ to NM.

iii. Upon successfully scrutinizing RID_{PD_i}, the NM computes $PID_{i2} = RID_{PD_i} \oplus H_0(s_{NM} PID_{i1})$ and submits pseudo-identity $PID_i = \{PID_{i1}, PID_{i2}, T_i\}$ to PD. Meanwhile, the NM records tuple $\{PID_i, RID_{PD_i}\}$ in a secure database.

After PID_i generation, the NM continues to compute a partial private key for the PD using the steps below.

iv. The NM randomly chooses $d_{PD_i} \in \mathrm{Z}_q^*$ and computes $D_{PD_i} = d_{PD_i}P$.

v. The NM computes $\beta_{PD_i} = H_1(PID_i, D_{PD_i}, PK_{NM})$

vi. The NM computes $k_{PD_i} = (d_{PD_i} + \beta_{PD_i} . s_{NM}) mod\ q$

vii. The NM sends PPK_{PD_i}=$\{k_{PD_i}, D_{PD_i}\}$ to PD as a partial private key

viii. Upon receiving PPK_{PD_i}, the PD checks for its authenticity by verifying the equation $k_{PD_i}P = D_{PD_i} + \beta_{PD_i}PK_{NM}$.

Proof of Correctness

$$\begin{aligned} k_{PD_i}P &= (d_{PD_i} + \beta_{PD_i} . s_{NM})P \\ &= d_{PD_i}P + \beta_{PD_i} . s_{NM} P \\ &= D_{PD_i} + \beta_{PD_i}PK_{NM} \end{aligned}$$

After successful verification of the PPK_{PD_i}, the PD generates its secret and public key pair using steps below.

ix. The PD randomly chooses $x_{PD_i} \in Z_q^*$ and sets its secret key as $SK_{PD_i} = \{x_{PD_i}, k_{PD_i}\}$.
x. The PD computes $X_{PD_i} = x_{PD_i} PK_{NM}$ and $Y_{PD_i} = k_{PD_i} PK_{NM}$.
xi. Finally, the PD sets its full public key as $PK_{PD_i} = (X_{PD_i}, Y_{PD_i})$.

3.2.2 AP Registration

The steps for PD registration are outlined below.

i. The AP randomly chooses $\theta_i \in Z_q^*$ and computes its public key $PK_{AP} = \theta_i P$.
ii. The AP sends tuple $\{RID_{AP}, PK_{AP}\}$ to NM, where RID_{AP} is the real identity for AP.
iii. Upon successfully scrutinizing RID_{AP}, the NM randomly chooses $d_{AP} \in Z_q^*$ and computes $D_{AP} = d_{AP} P$.
iv. The NM computes $\beta_{AP} = H_1(D_{AP}, PK_{AP}, PK_{NM})$.
v. Next, the NM computes $k_{AP} = (d_{AP} + \beta_{AP} . s_{NM}) mod\ q$ and sends partial private key $PPK_{AP} = \{k_{AP}, D_{AP}\}$ to AP.
vi. Upon receiving PPK_{AP}, the AP checks for its authenticity by verifying the equation $k_{AP} P = D_{AP} + \beta_{AP} PK_{NM}$.

Proof of Correctness

$$\begin{aligned} k_{AP}P &= (d_{AP} + \beta_{AP} . s_{NM})P \\ &= d_{AP}P + \beta_{AP} . s_{NM} P \\ &= D_{AP} + \beta_{AP} PK_{NM} \end{aligned}$$

After successful verification of the PPK_{PD_i}, the AP generates it's secret and public key pair using the steps below.

vii. The AP randomly chooses $x_{AP} \in Z_q^*$ and sets its secret key as $SK_{AP} = (x_{AP}, k_{AP})$.
viii. Next, the AP computes $X_{AP} = x_{AP} PK_{NM}$ and $Y_{AP} = k_{AP} PK_{NM}$, and sets its full public key as $PK_{AP} = (X_{AP} + Y_{AP})$.

3.3 Message Signcryption

Every health-related message should be signcrypted before transmission to enhance authenticity.

3.3.1 PD to AP Signcryption

On input of health-related message $m_{PD_i} \in \{0,1\}^*$, system parameters $params$, pseudo identity PID_{PD_i}, private key SK_{PD_i}, and AP's public key PK_{AP}, the PD outputs a signcrypted message ϱ_i. The steps for signcryption are outlined as follows.

i. The PD selects a random value $r_{PD_i} \in Z_q^*$ and computes $R_{PD_i} = r_{PD_i} PK_{AP}$.
ii. The PD computes $b = H_2(R_{PD_i})$ and $c = b \oplus m_{PD_i}$ and $e = H_3(PID_{PD_i}, m_{PD_i}, R_{PD_i}, PK_{PD_i}, PK_{AP}, t_i)$.
iii. Next, the PD computes $s = r_{PD_i}{}^{-1}(e + SK_{PD_i})$. If $s = 0$, return to step (i). Otherwise, output a signcrypted message $\varrho_i = (c, e, s)$, and send it to AP.

3.3.2 AP to PD Signcryption

When the AP needs to send a diagnostic message $m_{AP} \in \{0,1\}^*$ to PD, the AP will use its secret key SK_{AP} and PD's public key PK_{PD_i} to signcrypt message m_{AP} in the same manner that PD to AP signcryption is done.

3.4. Message Unsigncryption

Before acting on the signcrypted message, the receiver must run an unsigncryption algorithm to ensure the sender's and message's integrity.

3.4.1 PD to AP Unsigncryption

Upon receiving the signcrypted message $\varrho_i = (c, e, s)$ from PD, the AP extracts pseudo-identity's validity period T_i and timestamp t_i and checks their expiry. If the message is fresh, the AP runs the unsigncryption algorithm by taking system parameters $params$, its private key SK_{AP} and PD's public key PK_{PD_i} as inputs and outputs the original message m_{PD_i}. The steps for unsigncryption are outlined as follows.

i. The AP takes message $\varrho_i = (c, e, s)$ and computes $y = s^{-1}$.
ii. The AP computes $V_{AP} = eyPK_{AP} + yPK_{PD_i} SK_{AP}$.
iii. The AP computes $b' = H_2(V_{AP})$.
iv. The AP computes $m_{PD_i} = b' \oplus c$.
v. Finally, the AP computes $e' = H_3(m_{PD_i}, V_{AP}, PK_{PD_i}, PK_{AP}, PID_{PD_i}, t_i)$.
vi. If $e' = e$, AP returns original message m_{PD_i}, otherwise returns error message $\perp$

3.4.2 AP to PD Unsigncryption

The PD will perform the unsigncryption process in the same manner that PD to AP unsigncryption is done.

Proof of Correctness

Given $s = {r_{PD_i}}^{-1}(e + SK_{PD_i})$, we have $s^{-1} = r_{PD_i}(e + SK_{PD_i})^{-1}$

Therefore, the following correctness holds;

$$\begin{aligned} V_{AP} &= eyPK_{AP} + yPK_{PD_i}SK_{AP} \\ &= es^{-1}PK_{AP} + s^{-1}PK_{PD_i}SK_{AP} \\ &= es^{-1}SK_{AP}P + s^{-1}SK_{PD_i}SK_{AP}P \\ &= (e + SK_{PD_i})s^{-1}SK_{AP}P \\ &= (e + SK_{PD_i})r_{PD_i}(e + SK_{PD_i})^{-1}SK_{AP}P \\ &= r_{PD_i}SK_{AP}P \\ &= r_{PD_i}PK_{AP} \\ &= R_{PD_i} \end{aligned}$$

Thus, it is clear that $b' = b$, implying that the receiving device can obtain the original message m_{PD_i} from the sender through the decryption process. Additionally, $e' = e$, which means the receiving device can validate the sender's signature's correctness. Consequently, the proposed signcryption protocol is correct.

4. Security Analysis

4.1 Security Model

We consider two adversary types: Type-1 and Type-2. The two types of adversaries model the typical WBAN attackers in real-life scenario. Type-1 adversary is defined as an outsider attacker or a regular user who can replace the node's public key with a choice value without accessing the NM's master secret key. This type of adversary can perform eavesdropping and impersonation attacks in WBANs. Type-2 adversary on the other hand is characterized as an insider attacker, specifically a trusted but curious NM who possesses the master secret key. The NM is expected to be honest and should not replace the node's public key with a choice value. Type-2 adversary can tamper with data and perform session hijacking.

4.2 Security Proof

Security proof is conducted using Game-1 and Game-2. The players of Game-1 are Type-1 adversary Adv_1 and the challenger $\mathcal{C}$, which involves Adv_1 asking $\mathcal{C}$ some queries and $\mathcal{C}$ answering them correctly. The target of Adv_1 is to compromise the proposed scheme using the answers given by $\mathcal{C}$.

Definition 1: If the advantage of Adv_1 in winning Game-1 is negligible, the study argues that the proposed scheme is secure against Adv_1.

The players of Game-2 are type-2 adversary Adv_2 and the challenger $\mathcal{C}$, which involves Adv_2 asking $\mathcal{C}$ some queries and $\mathcal{C}$ answering them correctly. The target of Adv_2 is to compromise the proposed scheme using the answers given by $\mathcal{C}$.

Definition 2: If the advantage of Adv_2 in winning Game-2 is negligible, the study argues that the proposed scheme is secure against Adv_1.

Theorem 1: Assume that adversary Adv_1 can win Game 1 with a non-negligible advantage $\mathcal{E}' \geq \frac{\varepsilon}{(q_{H_0}+q_{H_1}+q_{H_2}+q_{H_3}+q_{Sig}+q_{Unsig})}$, in ROM after $q_{H_i}(i = 0, \dots, 3)$ hash queries, q_{Sig} signcryption query and q_{Uns} unsigncryption query. Then, there exists a challenger $\mathcal{C}$ who can solve CDH problem with a minimum advantage $\mathcal{E}'$ as defined at the end of the proof.

Proof: Suppose (P, aP, bP) is an instance of CDH problem, where $a, b \in \mathbb{Z}_q^*$. We show how challenger $\mathcal{C}$ in Game 1 interacts with adversary Adv_1 to compute $C = abP$.

Setup: The challenger $\mathcal{C}$ executes the setup algorithm to generate the system parameters $params$ as $\{p, q, G, P, PK_{NM}, H_0, H_1, H_2, H_3\}$ and a master secret key s_{NM}. Note, the challenger $\mathcal{C}$ shares the $params$ with Adv_1 but keeps s_{NM} a secret. To ensure consistency of the queries and responses to ROM, the challenger $\mathcal{C}$ maintains lists $L_{H_i}(i = 0, \dots, 3)$ for hash queries, and lists L_{PPK}, L_{SK}, L_{PK}, L_{Sig} and L_{Unsig} for partial private key query, secret key query, public key query, signcryption query, and unsigncryption query, respectively. Note all the lists are initially set to empty.

i. Phase-I

The challenger $\mathcal{C}$ randomly chooses PID_i^* as the target pseudo identity to be challenged. At this point, the study adopts the irreflexivity assumption (Li, 2018), i.e., given two pseudo identities PID_1 and PID_2, if $PID_1 = \mathrm{PID}_i^*$, then $PID_2 \neq \mathrm{PID}_i^*$ and vice versa.

a. H_0 query: Adversary Adv_1 submits a query on (α_i, T_i) to the challenger $\mathcal{C}$. $\mathcal{C}$ searches for the tuple (α_i, T_i, h_0) in the list L_{H_0} and returns h_0 if the tuple exists. Otherwise, $\mathcal{C}$ chooses hash value $h_0 \in \mathrm{Z}_q^*$ at random and returns h_0 to Adv_1. Then, challenger $\mathcal{C}$ updates L_{H_0} with tuple (α_i, T_i, h_0).

b. H_1 query: Adversary Adv_1 submits a query on $(PID_i, D_{PD_i}, PK_{NM})$ to the challenger $\mathcal{C}$. $\mathcal{C}$ searches for the tuple $(PID_i, D_{PD_i}, PK_{NM}, \beta_{PD_i})$ in the list L_{H_1} and returns β_{PD_i} if the tuple exists. Otherwise, $\mathcal{C}$ chooses hash value $\beta_{PD_i} \in \mathrm{Z}_q^*$ at random and returns β_{PD_i} to Adv_1. Then, challenger $\mathcal{C}$ updates L_{H_1} with tuple $(PID_i, D_{PD_i}, PK_{NM}, \beta_{PD_i})$.

c. H_2 query: Adversary Adv_1 submits a query on (R_{PD_i}) to the challenger $\mathcal{C}$. $\mathcal{C}$ searches for the tuple (R_{PD_i}, b) in the list L_{H_2} and returns b if the tuple exists. Otherwise, $\mathcal{C}$ chooses hash value $b \in \mathrm{Z}_q^*$ at random and returns b to Adv_1. Then, challenger $\mathcal{C}$ updates L_{H_2} with tuple(R_{PD_i}, b).

d. H_3 query: Adversary Adv_1 submits a query on $(PID_{PD_i}, m_{PD_i}, R_{PD_i}, PK_{PD_i}, PK_{AP}, t_i)$ to the challenger $\mathcal{C}$. $\mathcal{C}$ searches for the tuple $(PID_{PD_i}, m_{PD_i}, R_{PD_i}, PK_{PD_i}, PK_{AP}, t_i, e)$ in the list L_{H_3} and returns e if the tuple exists. Otherwise, $\mathcal{C}$ chooses hash value $e \in \mathrm{Z}_q^*$ at random and returns e to Adv_1. Then, challenger $\mathcal{C}$ updates L_{H_3} with tuple $(PID_{PD_i}, m_{PD_i}, R_{PD_i}, PK_{PD_i}, PK_{AP}, t_i, e)$.

e. Partial private key query: Adversary Adv_1 submits partial private key query for PID_{PD_i} to the challenger $\mathcal{C}$. If $PID_i = \mathrm{PID}_i^*$, challenger $\mathcal{C}$ terminates the algorithm. Otherwise, if $PID_i \neq \mathrm{PID}_i^*$, challenger $\mathcal{C}$ performs the following: selects $\eta_i, \phi_i \in \mathrm{Z}_q^*$ at random and computes $D_{PD_i} = \eta_i P - \phi_i P$. Next, challenger $\mathcal{C}$ sets $k_{PD_i} = \eta_i$, $H_1(PID_i, D_{PD_i}, PK_{NM}) = \beta_{PD_i} = \phi_i$ and PPK_{PD_i}=(k_{PD_i}, D_{PD_i}). Finally, Challenger $\mathcal{C}$ returns PPK_{PD_i} to adversary Adv_1 as partial private key and updates list L_{PPK} with the tuple $(PID_i, D_{PD_i}, \beta_{PD_i}, k_{PD_i})$.

f. Public key query: Adversary Adv_1 submits a public key query for PID_i to the challenger $\mathcal{C}$. $\mathcal{C}$ searches for PID_i query in the list L_{PK} and returns PK_{PD_i} if the query exists. Otherwise, $\mathcal{C}$ recovers tuple $(PID_i, D_{PD_i}, \beta_{PD_i}, k_{PD_i})$ from L_{PPK}. Next, $\mathcal{C}$ chooses $x_{PD_i} \in \mathrm{Z}_q^*$ at random and computes $X_{PD_i} = x_{PD_i} PK_{NM}$ and $Y_{PD_i} = k_{PD_i} PK_{NM}$. Finally, $\mathcal{C}$ returns $PK_{PD_i} = (X_{PD_i} + Y_{PD_i})$ to Adv_1 as public key and updates list L_{PK} with the tuple $(PID_i, k_{PD_i}, x_{PD_i}, PK_{PD_i})$.

g. Private key query: Adversary Adv_1 submits private key query for PID_i to the challenger $\mathcal{C}$. If $PID_i = \mathrm{PID}_i^*$, $\mathcal{C}$ terminates the algorithm. Otherwise, if $PID_i \neq \mathrm{PID}_i^*$, challenger $\mathcal{C}$ performs the following: searches for PID_i query in the list L_{PK} and returns SK_{PD_i} to Adv_1 if the query exists. Otherwise, $\mathcal{C}$ runs partial private key and public key queries to output tuple $(PID_i, k_{PD_i}, x_{PD_i}, X_{PD_i}, Y_{PD_i})$. Finally, $\mathcal{C}$ returns $SK_{PD_i} = (k_{PD_i}, x_{PD_i})$ to Adv_1 as the private key.

h. Public key replace query: Adversary Adv_1 submits public key replace query with an input (PID_i, PK'_{PD_i}) to the challenger $\mathcal{C}$, where $PK'_{PD_i} = X'_{PD_i} + Y'_{PD_i}$, $X'_{PD_i} = x'_{PD_i} PK_{NM}$ and $Y'_{PD_i} = k'_{PD_i} PK_{NM}$. Next, $\mathcal{C}$ sets $X_{PD_i} = X'_{PD_i}$, $Y_{PD_i} = Y'_{PD_i}$, $k_{PD_i} = k'_{PD_i}$ and $x_{PD_i} = x'_{PD_i}$. Finally, $\mathcal{C}$ updates list L_{PK} with the tuple $(PID_i, k'_{PD_i}, x'_{PD_i}, PK'_{PD_i})$.

i. Signcryption query: Adversary Adv_1 submits a signcryption query with an input $(PK_{PD_i}, PK_{AP}, m_{PD_i})$ to the challenger $\mathcal{C}$. $\mathcal{C}$ then chooses $r_{PD_i} \in \mathrm{Z}_q^*$ and computes $R_{PD_i} = r_{PD_i} PK_{AP}$. Next, $\mathcal{C}$ computes $b = H_2(R_{PD_i})$ where $H_2(R_{PD_i})$ can be retrieved from list L_{H_2}. Additionally, $\mathcal{C}$ computes $c = b \oplus m_{PD_i}$ and $e = H_3(PID_{PD_i}, m_{PD_i}, R_{PD_i}, PK_{PD_i}, PK_{AP}, t_i)$, where $e = H_3(PID_{PD_i}, m_{PD_i}, R_{PD_i}, PK_{PD_i}, PK_{AP}, t_i)$ can be retrieved from list L_{H_3}. Finally, $\mathcal{C}$ computes $s = r_{PD_i}{}^{-1}(e + SK_{PD_i})$, returns $\varrho_i = (c, e, s)$ to adversary Adv_1 and updates list L_{Sig} with the tuple (c, e, s, ϱ_i).

j. Unsigncryption query: Adversary Adv_1 submits an unsigncryption query with an input $(PK_{PD_i}, PK_{AP}, \varrho_i)$ to the challenger $\mathcal{C}$. $\mathcal{C}$ computes $y = s^{-1}$ and $V_{AP} = eyPK_{AP} + yPK_{PD_i} SK_{AP}$. If $V_{AP} \notin L_{H_2}$, an error message is returned. Otherwise, $\mathcal{C}$ computes $b' = H_2(V_{AP})$, then $m_{PD_i} = b' \oplus c$. If $(m_{PD_i}, V_{AP}, PK_{PD_i}, PK_{AP}, PID_{PD_i}, t_i) \notin L_{H_3}$, an error message is returned. Otherwise, $\mathcal{C}$ computes $e' = H_3(m_{PD_i}, V_{AP}, PK_{PD_i}, PK_{AP}, PID_{PD_i}, t_i)$. If $e' \neq e$, an error message is returned. Otherwise, $\mathcal{C}$ returns m_{PD_i} to Adv_1 and updates list L_{Unsig} with (m_{PD_i})

k. Challenge: Adversary Adv_1 gives two challenge plaintexts $\{ m_{PD_0}, m_{PD_1} \}$ and a target pseudo-identity PID_i^* to challenger $\mathcal{C}$. Next, $\mathcal{C}$ chooses $i \in \{0,1\}$ at random, $b^* \in \{0,1\}^l$, and $e^*, s^* \in \mathrm{Z}_q^*$. $\mathcal{C}$ computes $c^* = b^* \oplus m_{PD_i}$ and $y^* = (s^*)^{-1}$. $\mathcal{C}$ queries values α_i and β_{PD_i} from list $L_{H_0}$and L_{H_1}, respectively. When Adv_1 submits H_2 query with input $R^*_{PD_i} = (e^* y^* + y^* SK_{PD_i}) PK_{AP}$, $\mathcal{C}$ returns b^*. When Adv_1 submits H_3 query with input $(m_{PD_i}$, $R^*_{PD_i} = (e^* y^* + y^* SK_{PD_i}) PK_{AP}$, PK_{PD_i}, $PK_{AP})$, $\mathcal{C}$ returns e^*. Finally, $\mathcal{C}$ returns ciphertext $\varrho_i^* = (c^*, e^*, s^*)$ to Adv_1.

ii. Phase-II

Adversary Adv_1 can execute all queries in phase-I except unsigncryption query on ϱ_i^* to extract plaintext m_{PD_i}.

Guess: Lastly, Adv_1 makes a guess $i' \in \{0,1\}$ for i. If $i' = i$ holds, adversary Adv_1 returns $r_{PD_i} = ey + ySK_{PD_i}$ as the solution to CDH problem. Otherwise, Adv_1 fails to solve CDH. Similar steps are followed during game-2. This theorem proves the scheme's Indistinguishability under Chosen Ciphertext Attack (IND-CCA). Since our scheme is IND-CCA, it implies that no attacker can read the details of the messages sent in this network due to the hardness assumption of the Computational Diffie-Helman problem. Therefore, theorem 1 confirms our scheme has confidentiality security property.

Theorem 2: Assume that adversary Adv_1 can win Game 3 with a non-negligible advantage $\mathcal{E}' \geq \frac{\mathcal{E}}{(q_{H_0}+q_{H_1}+q_{H_2}+q_{H_3}+q_{Sig}+q_{Unsig})}$, in ROM after $q_{H_i}(i = 0, \dots, 3)$ hash queries, q_{Sig} signcryption query and q_{Uns} unsigncryption query. Then, there exists a challenger $\mathcal{C}$ who can solve ECDL problem with a minimum advantage $\mathcal{E}'$ as defined at the end of the proof.

Proof: Suppose $(Q = aP)$ is an instance of ECDL problem, where $a \in Z_q^*$. We show how challenger $\mathcal{C}$ in Game 3 interacts with adversary Adv_1 to compute a from Q and P.

Setup: The challenger $\mathcal{C}$ executes the setup algorithm to generate the system parameters $params$ as $\{p, q, G, P, PK_{NM}, H_0, H_1, H_2, H_3\}$ and a master secret key s_{NM}. Note, the challenger $\mathcal{C}$ shares the $params$ with Adv_1 but keeps s_{NM} a secret. To ensure consistency of the queries and responses to ROM, the challenger $\mathcal{C}$ maintains lists $L_{H_i}(i = 0, \dots, 3)$ for hash queries, and lists L_{PPK}, L_{SK}, L_{PK}, L_{Sig} and L_{Unsig} for partial private key query, secret key query, public key query, signcryption query, and unsigncryption query, respectively. Note all the lists are initially set to empty.

Phase-I

The challenger $\mathcal{C}$ randomly chooses PID_i^* as the target pseudo identity to be challenged. At this point, we adopt the irreflexivity assumption (Li, 2018) i.e., given two pseudo identities PID_1 and PID_2, if $PID_1 = \text{PID}_i^*$, then $PID_2 \neq \text{PID}_i^*$ and vice versa.

Adversary Adv_1 adaptively submits hash queries including H_0 query, H_1 query, H_2 query, H_3 query, partial private key query, private key query, and public key query, to the challenger $\mathcal{C}$, who responds in a similar manner as in Theorem 1 and 2.

Signcryption query: Adversary Adv_1 submits a signcryption query with an input $(PK_{PD_i}, PK_{AP}, m_{PD_i})$ to the challenger $\mathcal{C}$. $\mathcal{C}$ then chooses $r_{PD_i} \in Z_q^*$ and computes $R_{PD_i} = r_{PD_i}PK_{AP}$. Next, $\mathcal{C}$ computes $b = H_2(R_{PD_i})$ where $H_2(R_{PD_i})$ can be retrieved from list L_{H_2}. Additionally, $\mathcal{C}$ computes $c = b \oplus m_{PD_i}$ and $e = H_3(PID_{PD_i}, m_{PD_i}, R_{PD_i}, PK_{PD_i}, PK_{AP}, t_i)$, where $e = H_3(PID_{PD_i}, m_{PD_i}, R_{PD_i}, PK_{PD_i}, PK_{AP}, t_i)$ can be retrieved from list L_{H_3}. Finally, $\mathcal{C}$ computes $s = r_{PD_i}{}^{-1}(e + SK_{PD_i})$, returns $\varrho_i = (c, e, s)$ to adversary Adv_1 and updates list L_{Sig} with the tuple (c, e, s, ϱ_i).

Forgery: After all the queries have been made, adversary adv_1 furnishes challenging pseudo identity PID_i^* i.e., the sender's identity, a message m_{PD}^*, and a challenge signcryption $\varrho_i^* = (c^*e^*s^*)$. Note, the adversary is forbidden from making unsigncryption query for ϱ_i^* using the target identity's private key as this will result to game termination. Otherwise, the challenger $\mathcal{C}$ outputs a message m as the result for unsigncryption with input $(PK_{PD_i}, PK_{AP}, \varrho_i)$. If $m = m_{PD}^*$ and adv_1 did not query for PID_i^* private key and neither did adv_1 submit a replace the public key query for PID_i^* nor did adv_1 issue an extract partial private key query for PID_i^* at some point, the adversary adv_1 wins the game.

Similar steps are followed during game 2. This theorem proves the scheme's Existential Unforgeability under Chosen Message Attacks (EUF-CMA). Since our scheme is EUF-CMA, it implies that no attacker can generate valid signatures without access to the NM's secret key, a value that is randomly generated and difficult to compute due to the hardness of the Elliptic Curve Discrete Logarithm problem. Therefore, theorem 2 confirms our scheme has unforgeability security property.

5. Performance Evaluation

This section evaluates the performance of the proposed scheme in terms of security features, computation cost, and communication cost, and compares it with state-of-art schemes.

5.1 Security Features

Table 3 presents a summary of the security features achieved by the study's scheme and a comparison with other related schemes. The security features considered include: sender authentication, message authentication, confidentiality, unforgeability, non-repudiation, key-escrow resistance, availability, forward secrecy, and conditional anonymity. The study uses the symbols √ to denote that the scheme meets the security property. On contrary, the symbol × denotes that the scheme fails to meet the security property. Notably, the study's scheme meets all the security properties aforementioned, whereas the other six schemes lack various security features, as shown in Table 3.

Table 3: Comparison of Security Features of the Proposed Scheme with Related Schemes

Security Feature	Xiong et al. 2022	Zhou 2019	Liu et al. 2020	Ullah et al. 2021	Ramadan et al. 2023	Zhang et al. 2024	Proposed
Sender authentication	×	√	×	×	×	√	√
Message authentication	√	√	√	√	√	√	√
Confidentiality	√	√	√	√	√	√	√
Unforgeability	√	√	×	√	√	√	√
Non-repudiation	√	√	√	√	√	√	√
Key-escrow resistance	×	√	√	√	×	√	√
Availability	√	√	√	√	√	√	√
Forward secrecy	√	√	×	√	√	√	√
Conditional anonymity	×	×	×	√	×	×	√
Approach	PKI-IBC	CLC	CLC	CLC	IBC	CLC	CLC

5.2 Computation Cost

Here, we evaluate the signcryption and unsigncryption costs for both ECC and bilinear pairing-based cryptographic operations. Table 4 shows the running times for the various cryptographic operations considered in this scheme. We generated the running times from a simulation experiment. The experiment employed Mult-precision Integer and Rational Arithmetic Cryptographic Library for C/C++ (MIRACL CC), a widely recognized encryption toolkit used for conducting various cryptographic operations across different environments. The results were obtained from a set-up with the following specifications: an Intel i7 processor, Windows 10 operating system, 8GB RAM capacity, and a 3.40 GHz CPU.

Table 4: Cryptographic Operations Running Times

Notation	Cryptographic Operation	Run time (ms)
$\boldsymbol{T_{SM\_ecc}}$	Elliptic Curve Scalar Multiplication	0.442
$\boldsymbol{T_{SM\_bp}}$	Bilinear Pairing Scalar Multiplication	1.709
$\boldsymbol{T_{PA\_ecc}}$	Elliptic Curve Point Addition	0.0018
$\boldsymbol{T_{PA\_bp}}$	Bilinear Pairing Point Addition	0.071
$\boldsymbol{T_{IN}}$	Inverse	0.174
$\boldsymbol{T_{h}}$	General Hash Function	0.0001
$\boldsymbol{T_{Bp}}$	Bilinear Pairing	4.211
$\boldsymbol{T_{exp}}$	Exponentiation	3.886

Table 5 presents a summary of the computation costs for the proposed scheme and other related schemes for signcryption and unsigncryption algorithms. From the summary, the computation costs for signcryption and unsigncryption algorithms for the proposed scheme are T_{SM_ecc}+T_{PA_ecc}+T_{IN}+$2T_h$ $= 0.618$ ms and $2T_{SM\_ecc} + T_{PA\_ecc} + T_{IN} + 2T_h = 1.06$ ms, respectively, and the overall computation cost is 1.678 ms. We note that the proposed scheme outperforms the other six related schemes in terms of computational efficiency for both signcryption and unsigncryption algorithms, as well as overall efficiency.

Table 5: Total Computation Cost for both Signcryption and Unsigncryption

Scheme	**Signcryption cost (ms)**	**Unsigncryption cost (ms)**	**Total cost (ms)**
(Xiong et al., 2022)	$4T_{SM\_bp}$+$4T_h$+$2T_{exp}$ =14.6084	$3T_{Bp}+$ $T_{PA\_bp}+5T_h+T_{IN}+T_{exp}=16.7645$	31.3729
(Zhou, 2019)	$5T_{SM\_ecc}$+$4T_{PA\_ecc}+5T_h=2.2177$	$7T_{SM\_ecc}$+$4T_{PA\_ecc}$+$5T_h=3.1017$	5.3194
(Liu et al., 2020)	T_{SM_bp}+$5T_h$+$3T_{IN}+$ $6T_{exp}=25.5295$	T_{SM_bp}+$3T_h$+T_{IN}+$6T_{exp}=25.1993$	50.7288
(Ullah et al., 2021)	$4T_{SM\_ecc}$+$3T_h=1.7683$	$4T_{SM\_ecc}$+$3T_h=1.7683$	3.5366
(Ramadan et al., 2023)	$2T_{SM\_bp}$+T_{PA_bp}+$4T_h+$ $2T_{exp}=11.4944$	$4T_{Bp}$+T_h=16.4401	27.9345
(Zhang et al., 2024)	$3T_{SM\_ecc}$+$4T_{PA\_ecc}$+$6T_h=1.3338$	$4T_{SM\_ecc}$+$4T_{PA\_ecc}$+$2T_h=1.7754$	3.1092
Proposed	T_{SM_ecc}+T_{PA_ecc}+T_{IN}+$2T_h=0.618$	$2T_{SM\_ecc}$+T_{PA_ecc}+T_{IN}+$2T_h=1.06$	1.678

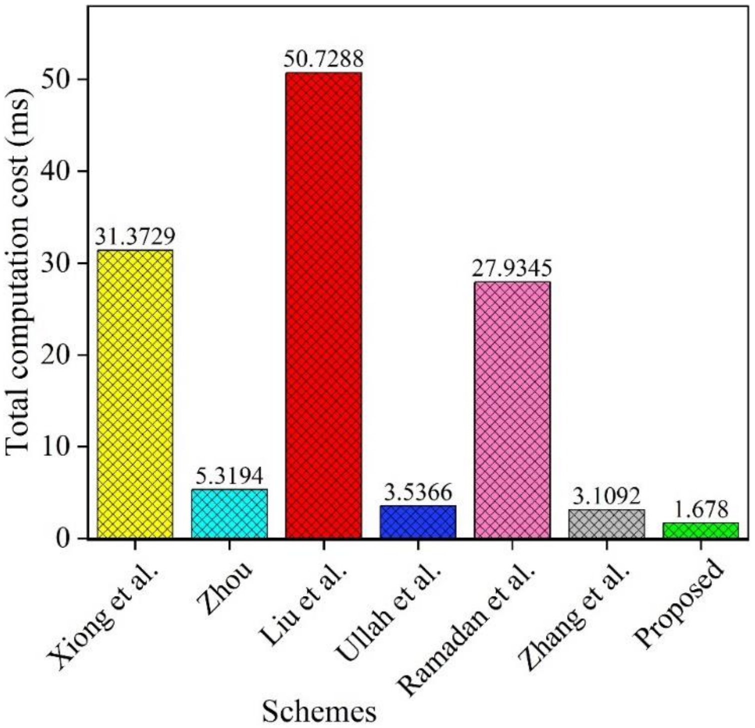

Figure 3: Total Computation Cost for both Signcryption and Unsigncryption

5.3 Communication cost

To evaluate communication cost, we consider the storage cost for transmitting ciphertext, the sender's public key, the receiver's public key, and the timestamp, measured in terms of byte size. For the analysis of bilinear pairing-based schemes, the study adopts a curve Ệ: $y^2 = x^3 + x\ (mod\ ṕ)$, and ṕ is a prime number of size 64 bytes. Curve Ệ contains some points generated by Ṕ which forms an additive group $\mathbb{G}_1$ with order q , a 20-byte prime number. A bilinear pairing operation is thus defined as $\mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$, $\mathbb{G}_1$ and $\mathbb{G}_2$ being the additive and multiplicative groups respectively. Therefore, the length of $\mathbb{G}_1$ is taken as 128 bytes and that of Z_q^* as 20 bytes. For analysis of elliptic curve-based schemes, the study adopts a curve E: $y^2 = x^3 + ax + b\ (mod\ p)$, and $p \in Z_q^*$ is a prime number of size 20 bytes. Curve E contains some points generated by P, which forms a cyclic additive group $\mathbb{G}$ of order q, where $q \in Z_q^*$ is a 20-byte prime number. Therefore, the length of $|\mathbb{G}_1|$ is taken as 40 bytes and that of $|Z_q^*|$ as 20 bytes. The length of the plaintext message $|m|$ and timestamp $|t|$ are assumed to be 20 bytes and 4 bytes, respectively, for both bilinear pairing and elliptic curve-based schemes. From the summary in Table 6, the total communication cost of the proposed scheme is given as $4|G_1|+3|Z_q^*|+|t| = 4 \times 40 + 3 \times 20 + 4 = 224\ bytes$. The total communication costs of other related schemes used to compare our scheme are provided in the table 6.

Table 6: Total communication cost for single message

Scheme	Total communication cost for single message	Total communication cost for *n* messages
(Xiong et al., 2022)	$7\|G_1\|+2\|Z_q^*\| + \|t\| = 944\ bytes$	944n bytes
(Zhou, 2019)	$4\|G_1\|+\|Z_q^*\| + \|t\| = 184\ bytes$	184n bytes
(Liu et al., 2020)	$6\|Z_q^*\| + \|m\| + \|t\| = 792\ bytes$	792n bytes
(Ullah et al., 2021)	$2\|G_1\|+2\|Z_q^*\| + \|m\| + \|t\| = 144\ bytes$	144n bytes
(Ramadan et al., 2023)	$4\|G_1\| + 2\|m\| + \|t\| = 556\ bytes$	556n bytes
(Zhang et al., 2024)	$5\|G_1\|+\|Z_q^*\| + \|m\| + \|t\| = 244\ bytes$	244n bytes
Proposed	$4\|G_1\|+3\|Z_q^*\| + \|t\| = 224\ bytes$	224n bytes

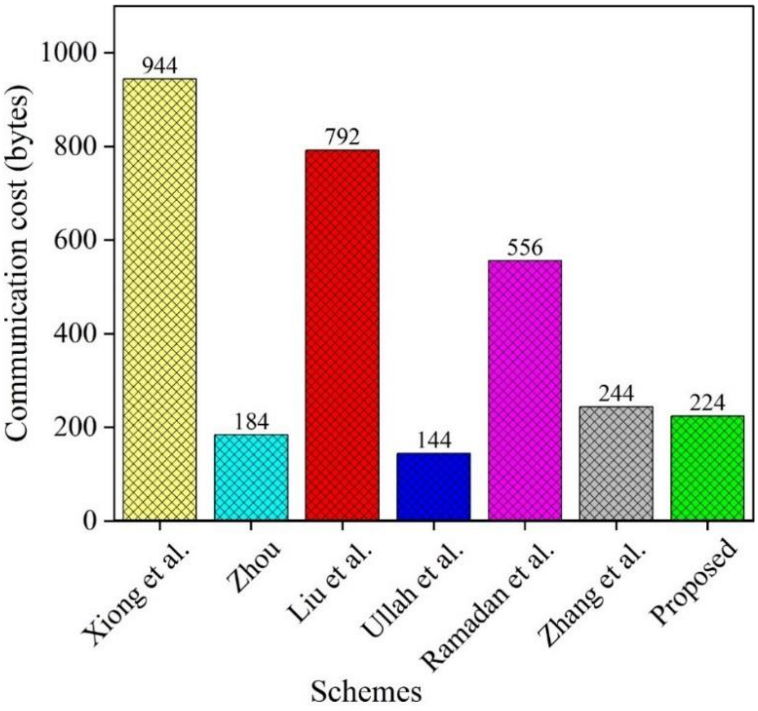

Figure 4: Total communication cost for single message

Table 7 provides comparison of the computational and communication costs between the proposed scheme and other related schemes.

Table 7: Comparison of the Total Computation and Communication Costs of the Proposed Scheme with Existing Schemes

Scheme	Total computation cost (in milliseconds)	Total communication cost for single message (in byes)
(Xiong et al., 2022)	31.3729	944
(Zhou, 2019)	5.31940	184
(Liu et al., 2020)	50.7288	792
(Ullah et al., 2021)	3.53660	144
(Ramadan et al., 2023	27.9345	556
(Zhang et al., 2024)	3.10920	244
Proposed	1.67800	224

5. Conclusion and Future Work

This study has successfully achieved its objective by analyzing, designing and validating secure and efficient certificateless signcryption for wireless body area networks by utilizing elliptic curve cryptography (ECC). The design has achieved significant improvement in terms of performance through optimizing the cost for computational algorithms and that of communication, thus making it suitable for resource constrained WBAN devices.

Through comprehensive performance evaluation, the results have proved the scheme to outsmart the state-of-the art schemes across the key performance metrics i.e., security, computation cost, and communication cost. This validation confirms that the proposed scheme is not only secure but also efficient in terms of resource usage, thereby enhancing WBAN reliability and usability for healthcare applications. In the future, this study intends to improve the proposed scheme by exploring and developing a hybrid cryptographic framework that combines the strengths of ECC with the advanced security features of quantum key distribution (QKD) to create a robust and future-proof cryptographic system that can withstand the capabilities of quantum computers while maintaining the practical benefits of ECC.

References

1. Ali, I., Chen, Y., Ullah, N., Kumar, R., & He, W. (2021). An Efficient and Provably Secure ECC-Based Conditional Privacy-Preserving Authentication for Vehicle-to-Vehicle Communication in VANETs. IEEE Transactions on Vehicular Technology, 70(2), 1278–1291. https://doi.org/10.1109/TVT.2021.3050399
2. Almuhaideb, A. M. (2022). Secure and Efficient WBAN Authentication Protocols for Intra-BAN Tier. J. Sens. Actuator Netw, 11(44). https://doi.org/https://doi.org/ 10.3390/jsan11030044
3. Cornet, B., Fang, H., Ngo, H., Boyer, E. W., & Wang, H. (2022). An Overview of Wireless Body Area Networks for Mobile Health Applications. IEEE Network, 36(1), 76–82. https://doi.org/10.1109/MNET.103.2000761
4. Jahan, M., Zohra, F. T., Parvez, M. K., Kabir, U., Al Radi, A. M., & Kabir, S. (2023). An end-to-end authentication mechanism for Wireless Body Area Networks. Smart Health, 29, 100413. https://doi.org/10.1016/j.smhl.2023.100413
5. Kasyoka, P. N. (2022). Certificateless Signcryption for Wireless Sensor Networks.
6. Li, A. A. O. (2018). Provably Secure Heterogeneous Access Control Scheme for Wireless Body Area Network. J Med Syst, 42(108), 190–198. https://doi.org/https://doi.org/10.1007/s10916-018-0964-z SYSTEMS-LEVEL
7. Liu, X., Wang, Z., Ye, Y., & Li, F. (2020). An efficient and practical certificateless signcryption scheme for wireless body area networks. Computer Communications, 162(February), 169–178. https://doi.org/10.1016/j.comcom.2020.08.014
8. Mandal, S. (2022). Provably secure certificateless protocol for wireless body area network. Wireless Networks, 4. https://doi.org/10.1007/s11276-022-03205-4
9. Mandal, S. (2023). Provably secure certificateless protocol for wireless body area network. Wireless Networks, 29(3), 1421–1438. https://doi.org/10.1007/s11276-022-03205-4
10. Qu, Y., Zheng, G., Ma, H., Wang, X., Ji, B., & Wu, H. (2019). A survey of routing protocols in WBAN for healthcare applications. Sensors (Switzerland), 19(7). https://doi.org/10.3390/s19071638
11. Ramadan, M., Raza, S., & Member, S. (2023). Identity-Based Signcryption for Telemedicine Systems. IEEE Internet of Things Journal, 10(18), 16594–16604. https://doi.org/10.1109/JIOT.2023.3269222
12. Sama, N. U., Zen, K., Humayun, M., Jhanjhi, N. Z., & Rahman, A. U. (2022). Security in Wireless Body Sensor Network: A Multivocal Literature Study. Applied System Innovation, 5(4). https://doi.org/10.3390/asi5040079
13. Ullah, I., Alkhalifah, A., Rehman, S. U., Kumar, N., & Khan, M. A. (2021). An Anonymous Certificateless Signcryption Scheme for Internet of Health Things. IEEE Access, 9, 101207–101216. https://doi.org/10.1109/ACCESS.2021.3097403
14. Xiong, H., Hou, Y., Huang, X., Zhao, Y., & Chen, C. M. (2022). Heterogeneous Signcryption Scheme from IBC to PKI with Equality Test for WBANs. IEEE Systems Journal, 16(2), 2391–2400. https://doi.org/10.1109/JSYST.2020.3048972
15. Yang, X., Yi, X., Khalil, I., Huang, X., & Shen, J. (2022). Efficient and Anonymous Authentication for Healthcare Service with Cloud Based WBANs. IEEE Transactions on Services Computing, 15(5), 2728–2741.
16. Zhang, J., Dong, C., & Liu, Y. (2024). Efficient Pairing-Free Certificateless Signcryption Scheme for Secure Data Transmission in IoMT. IEEE Internet of Things Journal, 11(3), 4348–4361. https://doi.org/10.1109/JIOT.2023.3298840
17. Zhang, J., Zhang, Q., Li, Z., Lu, X., & Gan, Y. (2021). A Lightweight and Secure Anonymous User Authentication Protocol for Wireless Body Area Networks. Security and Communication Networks, 2021. https://doi.org/10.1155/2021/4939589
18. Zhou, C. (2019). An improved lightweight certificateless generalized signcryption scheme for mobile-health system. International Journal of Distributed Sensor Networks, 15(1), 1550147718824465.