[1*]Akilan Selvaraj Saroja,

[2]Sadikov Rustamjon Toxirovich,

[3]Kayathri Devi Devprasad

Advancing Security in Lightweight S-WBSN for E-Healthcare

Journal of Electrical Systems

Abstract: - Wireless body sensor networks (WBSNs) are a critical component of e-healthcare, enabling continuous monitoring of vital signs and other health parameters. However, the limited capacity of WBSNs poses a significant challenge to securing data transmission. A novel architecture for Secure Wireless Body Sensor Networks (S-WBSN) has been introduced, focusing on efficiency and robust security. The S-WBSN architecture employs a combination of the OTP-Q stream block cipher and the Diffie-Hellman key exchange algorithm to ensure secure data transmission and mutual authentication between critical components. The OTP-Q algorithm encrypts data obtained from WBSN sensors, while the Diffie-Hellman algorithm establishes a secure communication channel between the WBSN, Local Processing Center (LPC), and Data Server. This innovative approach effectively meets essential security requirements, including mutual authentication and privacy preservation. It also demonstrates notable efficiency, consuming fewer CPU cycles than existing state-of-the-art security approaches. Comparative analysis showcases reduced processing time for encryption and decryption, making the S-WBSN architecture an attractive solution for e-healthcare data monitoring security. In summary, the S-WBSN architecture significantly enhances the security posture of e-healthcare data transfer, prioritizing efficiency, and robust protection. It sets itself apart from contemporary healthcare data monitoring security methodologies by delivering a comprehensive solution that addresses the unique challenges of WBSNs.

Keywords: Body sensor network, Secure wireless body sensor networks, One-Time Pad, Quasi-group encryption, Diffie-Hellman key exchange algorithm, BAN, BSN

1 INTRODUCTION

Wireless body sensor networks (WBSNs) are a promising technology for healthcare support, especially in elder care. They enable remote health monitoring and swift intervention, eliminating the need for constant human oversight. WBSNs comprise sensors and a Local Processing Center (LPC). The sensors continuously collect health data from the patient, such as heart rate, blood pressure, and respiratory rate. The LPC then processes the data and transmits it to a remote healthcare center for analysis.

The integration of wireless technologies into WBSNs offers several advantages. First, it eliminates the need for cumbersome wires and electrodes, making the system more comfortable and convenient for patients. Second, wireless communication allows for real-time monitoring of patients' health, which can be critical in emergency situations. Third, wireless WBSNs can be used to monitor patients in remote locations, where access to healthcare facilities is limited.

However, wireless technologies also introduce security concerns. WBSNs are susceptible to a variety of attacks, such as eavesdropping, data alteration, unauthorized access, and repudiation. These attacks can be launched by both external and internal adversaries. External adversaries may be motivated by financial gain, while internal adversaries may be malicious employees or disgruntled patients.

To ensure the security of WBSN-transmitted healthcare data, it is important to implement robust security measures. These measures should address the following security requirements:

1. Confidentiality: The data transmitted between sensor nodes and the LPC should be protected from unauthorized access.
2. Integrity: The data should be protected from unauthorized alteration.
3. Authentication: The sensor nodes and the LPC should be able to authenticate each other to prevent unauthorized

[1,2]Computer engineering (Multimedia technologies),
Tashkent University of Information Technology, Tashkent, Uzbekistan
[3]Department of Information Technology, Amity University, Uzbekistan
Correspondence
*Akilan S S, Computer engineering (Multimedia technologies),
Tashkent University of Information Technology, Tashkent, Uzbekistan

access to the network.

4. Non-repudiation: The sender and receiver of data should not be able to deny sending or receiving the data, respectively.

There are a number of security solutions that can be implemented to protect WBSNs from attack. These solutions can be broadly classified into two categories:

1. Cryptographic solutions: Cryptographic solutions use cryptographic algorithms to encrypt and authenticate data. These solutions are effective at protecting data from unauthorized access and alteration. However, they can be computationally expensive, which may be a challenge for battery-powered sensor nodes.
2. Lightweight security solutions: Lightweight security solutions are designed to be efficient and require less processing power. These solutions are more suitable for battery-powered sensor nodes, but they may not provide the same level of security as cryptographic solutions.

When implementing security measures in WBSNs, it is important to consider the following factors:

1. Resource constraints: WBSN sensors are typically resource-constrained devices with limited processing power, memory, and battery life. Therefore, it is important to implement security solutions that are efficient and do not compromise the performance of the network.
2. Security requirements: The security requirements of a WBSN will vary depending on the type of data being collected and the sensitivity of the data. For example, WBSNs that collect sensitive medical data will have more stringent security requirements than WBSNs that collect non-sensitive data.
3. Cost: The cost of implementing security measures is another important factor to consider. Cryptographic solutions can be expensive to implement, while lightweight security solutions are typically more cost-effective.

Overall, the security of WBSNs is a critical issue that must be addressed before these networks can be widely adopted in healthcare. By implementing robust security measures, healthcare providers can protect sensitive patient data from unauthorized access and misuse.

Here are some specific examples of security measures that can be implemented in WBSNs:

Encryption: Encryption can be used to protect data from unauthorized access. For example, the data transmitted between sensor nodes and the LPC can be encrypted using a lightweight cryptographic algorithm. Authentication: Authentication can be used to ensure that only authorized devices can access the WBSN. For example, sensor nodes can authenticate themselves to the LPC using a challenge-response protocol. Data integrity: Data integrity can be protected using digital signatures. For example, the LPC can digitally sign the data it receives from sensor nodes to ensure that the data has not been tampered with. Access control: Access control can be used to restrict access to the WBSN and the data it transmits. For example, the WBSN can be configured to only allow authorized devices to connect to the network.

By implementing these security measures, healthcare providers can significantly reduce the risk of WBSN attacks and protect sensitive patient data.

2. RELATED WORKS

The integration of internet technology has fueled a surge in IoT-driven healthcare research initiatives. This section delves into a selection of these studies, highlighting their contributions and identifying areas for improvement.

CodeBlue, a pioneering healthcare research venture established at Harvard's Sensor Network Lab, paved the way for Wireless Body Sensor Networks (WBSNs). CodeBlue's groundbreaking implementation of biosensors embedded within patients' bodies enabled the wireless transmission of physiological data to end-user devices for further analysis. This network empowered healthcare practitioners to access vital patient health information through their personal digital assistants (PDAs). While CodeBlue emphasized the importance of safeguarding medical applications, areas for further improvement were identified.

Building upon CodeBlue's foundation, the University of Virginia introduced ALARM-NET, focusing on patient health monitoring and integrating IP-based network elements with wireless sensors. ALARM-NET employed the secure remote password (SRP) protocol to safeguard medical data, but it faced challenges related to confidentiality attacks.

MEDiSN, another significant initiative by John Hopkins University, targeted patient monitoring using monitors and

patient-worn motes. However, critiques pointed to its inadequate emphasis on security concerns. Zhu et al.'s subsequent work reinforced the importance of WBSNs in healthcare, scrutinizing hardware and technology preferences to optimize computational costs in wireless environments. Security emerged as a central concern across various healthcare systems. Jin et al. proposed the ECG-IJS algorithm to authenticate communication between sensor nodes, ensuring data security and confidentiality. Shi et al. introduced an attribute-based security scheme, combining digital signatures and encryption techniques to bolster security. While effective, this approach incurred certain computational overhead limitations.

Khalilian et al. developed an RFID-based system ensuring secure communication over wireless networks. However, it faced challenges related to high communication costs. Similarly, BSN-Care, while emphasizing security measures, exhibited shortcomings in communication costs and certain privacy and security aspects.

Recent advancements have introduced novel techniques to enhance security in healthcare systems. Liu et al. implemented an encryption algorithm for medical images to fortify protection against potential attackers. Dai et al. introduced a chaotic mapping method for encrypting medical digital images, substantially augmenting data security. Renardi et al. proposed new wireless sensor network technology utilizing AES to enhance data transmission speed. This work contributes significantly by introducing a lightweight authentication protocol to fortify network access protection and data transmission in WBSNs. It introduces methodologies like the simple hash function, one-time pad (OTP) generation, and Quasi-group Stream Cipher creation, intending to reduce computation complexity and communication costs.

In addition to the aforementioned works, other notable contributions in the realm of healthcare-related IoT research merit attention. AKilan S S et al. explored the integration of OTP-Q technology in Wireless Body Sensor Networks (WBSNs) to enhance data security, privacy, and access control. Chen et al. introduced a novel authentication mechanism that merged biometric data and cryptographic keys for secure user access within medical IoT environments. Singh et al. developed a robust intrusion detection system tailored for WBSNs, employing machine learning algorithms to effectively identify and prevent security breaches. Wang et al. investigated the implementation of homomorphic encryption techniques in healthcare IoT systems to enable computation on encrypted data without revealing sensitive information. Kim et al. emphasized secure aggregation of medical data in WBSNs, focusing on enhancing privacy protection while facilitating efficient data analysis. Li et al. proposed an energy-efficient and secure routing protocol for WBSNs, optimizing energy consumption while ensuring data confidentiality and integrity. Garcia et al. introduced a novel approach leveraging hybrid encryption schemes and compressed sensing techniques to ensure secure and efficient data transmission in IoT healthcare systems. These diverse studies collectively contribute to fortifying security, privacy, and efficiency in healthcare-related IoT systems, shaping the evolution of secure, reliable, and privacy-aware solutions for Wireless Body Sensor Networks. This comprehensive overview of various healthcare-related IoT research initiatives highlights the challenges and advancements in security, privacy, and efficiency across Wireless Body Sensor Networks.

3. PROPOSED WORK

Wireless body area networks (WBANs) are a type of wireless sensor network (WSN) that is used to collect and transmit data from sensors attached to the human body. WBANs can be used to monitor a wide range of physiological parameters, such as heart rate, blood pressure, respiratory rate, temperature, and movement.

WBANs typically consist of three main components:

1. Sensor nodes: Sensor nodes are small, lightweight devices that are attached to the human body. They are responsible for collecting data from the body and transmitting it to the other components of the WBAN.
2. Coordinator node: The coordinator node is the central node of the WBAN. It is responsible for collecting data from the sensor nodes and transmitting it to the external system.
3. External system: The external system is a device that is used to process and analyze the data collected by the WBAN. This could be a computer, smartphone, or other device.

WBANs can communicate using a variety of wireless technologies, such as Bluetooth Low Energy (BLE), ZigBee, and Wi-Fi. The choice of wireless technology depends on a number of factors, such as the required data rate, range, and power consumption.

Example of WBAN

One example of a WBAN is a system that is used to monitor the health of patients with chronic diseases, such as diabetes and heart disease. The system could consist of the following components:

- Sensor nodes: Sensor nodes could be attached to the patient's skin to monitor their heart rate, blood pressure, and blood glucose levels.
- Coordinator node: The coordinator node could be worn by the patient or carried in a small pouch. It would be responsible for collecting data from the sensor nodes and transmitting it to the external system.
- External system: The external system could be a computer or smartphone that is used to display the patient's health data to their doctor or other caregivers.

Example Table

The following table shows an example of a WBAN system that is used to monitor the health of a patient with diabetes:

TABLE 1 Components, Descriptions, and Functions of a WBAN

Component	**Description**	**Function**
Sensor nodes	Attached to the patient's skin to monitor blood glucose levels, heart rate, and respiratory rate.	Collect data from the patient's body.
Coordinator node	Worn by the patient or carried in a small pouch. Collects data from the sensor nodes and transmits it to the external system.	Act as a relay between the sensor nodes and the external system.
External system	A smartphone or computer that is used to display the patient's health data to their doctor or other caregivers.	Receive data from the coordinator node, process it, and display it to the user.

1. Benefits of WBANs

WBANs offer a number of benefits over traditional wired monitoring systems, including:

- Convenience: WBANs are more convenient for patients because they do not require any wires or electrodes.
- Mobility: WBANs allow patients to move around freely without being restricted by wires. Continuous monitoring: WBANs can provide continuous monitoring of patients' health parameters, which can help to identify potential problems early.
- Reduced costs: WBANs can help to reduce the costs of healthcare by reducing the need for hospital visits and other expensive procedures.

2. Challenges of WBANs

WBANs also face a number of challenges, including:

Security and privacy: WBANs collect sensitive medical data, so it is important to implement robust security measures to protect this data from unauthorized access.

- Power consumption: Sensor nodes are typically powered by batteries, so it is important to design WBAN systems to minimize power consumption.
- Interference: WBANs can be susceptible to interference from other wireless devices, such as cell phones and Wi-Fi routers.

Despite these challenges, WBANs have the potential to revolutionize the way that healthcare is delivered. By providing continuous monitoring of patients' health parameters, WBANs can help to improve patient care and reduce

the costs of healthcare.

TABLE 2 Example Table of WBAN Sensor Data Collection

Sensor Type	Measured Parameter	Example Data (Simulated)
ECG Sensor	Heart Rate	72 bpm
Temperature Sensor	Body Temperature	98.6°F
Accelerometer	Physical Activity	Walking
Blood Glucose Sensor	Glucose Level	120 mg/dL

Example Table 2 illustrating WBAN Data Collections.

Working Explanation:

- **ECG Sensor:** Measures heart rate, providing data such as beats per minute (bpm).
- **Temperature Sensor:** Monitors body temperature and displays the recorded temperature in Fahrenheit or Celsius.
- **Accelerometer:** Tracks physical activities or movements, such as 'Walking' or 'Running'.
- **Blood Glucose Sensor:** Measures the level of glucose in the blood, often denoted in milligrams per deciliter (mg/dL).

Here,the implementation of Secure Wireless Body Sensor Networks (S-WBSNs) and One Time Pad-Quasi (OTP-Q) encryption is important for a number of reasons.

S-WBSNs are designed to protect the privacy and confidentiality of sensitive healthcare data transmitted over wireless body sensor networks. They do this by implementing a number of security measures, such as:

- Mutual authentication: S-WBSNs authenticate all devices on the network to ensure that only authorized devices can access the network and the data it transmits.
- Data encryption: S-WBSNs encrypt all data transmitted over the network to protect it from unauthorized access.
- Data integrity: S-WBSNs ensure the integrity of data transmitted over the network by using digital signatures and other techniques.

OTP-Q encryption

OTP-Q encryption is a stream block cipher that is well-suited for use in WBSNs. It is efficient and provides strong security. OTP-Q encryption works by combining a random key with the data to be encrypted. The resulting ciphertext is then transmitted over the network. The recipient of the ciphertext can decrypt it using the same random key.

Importance of S-WBSN and OTP-Q

The implementation of S-WBSNs and OTP-Q encryption is important for the following reasons:

- Protecting patient privacy: S-WBSNs and OTP-Q encryption can help to protect the privacy of patients by encrypting their sensitive healthcare data. This is important because healthcare data is often very sensitive and could be used to cause harm to patients if it fell into the wrong hands.
- Preventing data breaches: S-WBSNs and OTP-Q encryption can help to prevent data breaches by making it more difficult for attackers to access and steal sensitive healthcare data. This is important because data breaches can have serious consequences for patients, including financial loss, identity theft, and even physical harm.
- Maintaining compliance: S-WBSNs and OTP-Q encryption can help healthcare providers to maintain compliance with data privacy and security regulations. Many healthcare organizations are required to implement certain security measures to protect their patients' data. S-WBSNs and OTP-Q encryption can help healthcare organizations to meet these requirements.

Overall, the implementation of S-WBSNs and OTP-Q encryption is important for protecting the privacy and confidentiality of sensitive healthcare data transmitted over wireless body sensor networks. This is essential for protecting patients and maintaining compliance with data privacy and security regulations.

In addition to the above, here are some specific examples of how S-WBSNs and OTP-Q encryption can be used to improve healthcare security:

Remote patient monitoring: S-WBSNs and OTP-Q encryption can be used to securely monitor patients remotely. This can be useful for monitoring patients with chronic diseases, such as diabetes and heart disease. Clinical trials: S-WBSNs and OTP-Q encryption can be used to securely collect and transmit data from clinical trials. This data can be used to evaluate new drugs and treatments. Public health surveillance: S-WBSNs and OTP-Q encryption can be used to securely collect and transmit data for public health surveillance. This data can be used to track the spread of diseases and identify potential outbreaks.

By implementing S-WBSNs and OTP-Q encryption, healthcare providers can improve the security of their patients' data and reduce the risk of data breaches.

a. | Registration Phase

During the registration phase in a Wireless Body Sensor Network (WBSN), all biosensors collectively establish themselves as a unified network with both the Local Processing Center (LPC) and the Data Server (DS). This phase involves specific sequential steps:

i. Generation of Confidential Identifier (ID C): The WBSN generates a confidential, concise, and randomly generated identifier, denoted as ID C.

ii. Creation of Secret Shares: ID C is divided into two distinct secret shares, C1 and C2, ensuring that $C_1 \in rZb$ and $C2 \in rZb$.

iii. Registration Process:

1. The WBSN completes registration with the LPC, presenting the secret share C2.
2. Simultaneously, the WBSN registers with the DS, providing the secret share C1.

The deployment of two distinct secret shares adds a significant layer of security, substantially mitigating the possibility of dictionary attacks or other malicious endeavors aimed at compromising both the LPC and the DS.

To elaborate further, should an attacker gain access to one secret share, for instance, $C1$, they cannot employ it to gain authentication with the LPC, as the LPC mandates the usage of secret share $C2$ for verification. Similarly, access to secret share $C2$ does not grant authentication with the DS, as the DS necessitates secret share $C1$ for validation.

b. | Secure and Lightweight Key Exchange for Wireless Body Sensor Networks

The Diffie-Hellman mutual authentication key exchange protocol is a cryptographic protocol that allows two parties to establish a shared secret key over an insecure channel. This protocol is often used in Secure Wireless Body Sensor Networks (S-WBSNs) to establish a secure communication channel between the WBAN and the Local Processing Center (LPC) and Data Server (DS).

The protocol works by having the WBAN, LPC, and DS each generate a random secret number and compute their public keys. The public keys are then exchanged between the three parties. Each party then computes the session key using the public keys of the other two parties and their own secret number.

Algorithm 1 Registration Phase in WBSN

1: **Input:** List of Biosensors (biosensors)

2: **Output:** Registered Biosensors in LPC and DS 3: **procedure** REGISTRATIONPHASE(biosensors) 4: **for each** biosensor **in** biosensors **do**

5: GenerateSecretShares(biosensor)

6: RegisterWithLPC(biosensor)

7: RegisterWithDS(biosensor)

8: **end for**

9: **end procedure**

10: **procedure** GENERATESECRETSHARES(biosensor)

11: Generate two secret shares (c1, c2) from the biosensor's ID

12: **end procedure**

13: **procedure** REGISTERWITHLPC(biosensor)

14: Register the biosensor with the Local Processing Center (LPC)

15: **end procedure**

16: **procedure** REGISTERWITHDS(biosensor)

17: Register the biosensor with the Data Server (DS)

18: **end procedure**

TABLE 3 Notations

Component	Description
p	A common prime number agreed upon by the WBAN, LPC, and DS. A generator of the multiplicative group of integers modulo p.
g	A random secret number generated by the WBAN.
a	The public key of the WBAN, computed as $A = g^a \mod p$. A random secret number generated by the LPC.
A	The public key of the LPC, computed as $B = g^b \mod p$. A random secret number generated by the DS.
b	The public key of the DS, computed as $C = g^c \mod p$.
B	The session key shared by the WBAN, LPC, and DS, computed as $K = (B^a \mod p) \times (C^a \mod p) \mod p$.
c	A common hash function agreed upon by the WBAN, LPC, and DS. The private key of the WBAN.
C	The private key of the LPC. The private key of the DS.
K	The signature of the WBAN's public key A, computed as $sig_{wban} = h(sk_{wban}, A)$.
$h()$	The signature of the LPC's public key B, computed as $sig_{lpc} = h(sk_{lpc}, B)$.
sk_{wban}	The signature of the DS's public key C, computed as $sig_{ds} = h(sk_{ds}, C)$.
sk_{lpc}	
sk_{ds}	
sig_{wban}	
sig_{lpc}	
sig_{ds}	

The mutual authentication phase of the protocol ensures that the three parties are communicating with each other and not with an attacker. This is done by having each party sign their public key with their private key and sending the signed public key to the other two parties. The three parties then verify the signatures to authenticate each other. Once all three parties have authenticated each other, they can begin communicating using the secure session key.

To prevent MITM attacks, one can use public-key authentication. This requires that WBAN and LPC and DS have each others (certified) public-keys.

Here is a step-by-step explanation of the protocol, with notations from the previous table:

Key Exchange Protocol:

Step 1: The WBAN, LPC, and DS agree on a common prime number p and a generator g.

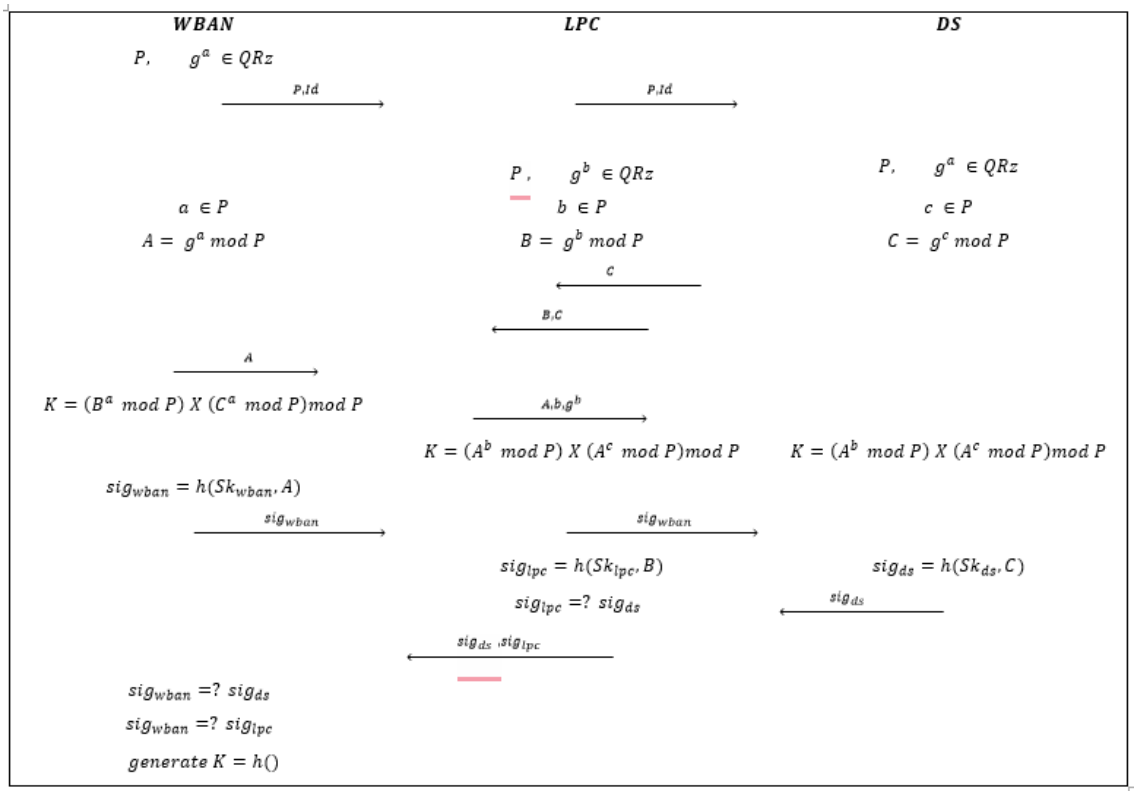

FIGURE 1 Model of Authenticated Diffie-Hellman Key Agreement

Step 2: The WBAN generates a random secret number a and computes its public key A as follows:

$A = g^a \mod p$

Step 3: The WBAN sends its public key A to the LPC and DS.

Step 4: The LPC and DS each generate random secret numbers b and c, respectively, and compute their public keys B and C as follows:

$B = g^b \mod p$

$C = g^c \mod p$

Step 5: The LPC and DS send their public keys B and C to the WBAN.

Step 6: The WBAN computes the session key K as follows:

$K = (B^a \mod p) \times (C^a \mod p) \mod p$

Step 7: The LPC and DS each compute the session key K as follows:

$K = (A^b \mod p) \times (A^c \mod p) \mod p$

Mutual Authentication Steps:

Step 1: The WBAN, LPC, and DS agree on a common hash function $h()$.

Step 2: The WBAN generates a random secret number a and computes its public key A as:

$A = g^a \mod p$

Step 3: The WBAN signs its public key A with its private key sk_{wban} as:

$\text{sig}_{wban} = h(sk_{wban}, A)$

Step 4: The WBAN sends its public key A and signature sig_{wban} to the LPC and DS.

Step 5: The LPC and DS each generate random secret numbers b and c and compute their public keys B and C.

Step 6: The LPC and DS sign their public keys B and C with their private keys sk_{lpc} and sk_{ds}:

$\text{sig}_{lpc} = h(sk_{lpc}, B)$

$\text{sig}_{ds} = h(sk_{ds}, C)$

Step 7: The LPC and DS send their public keys B and C, along with signatures sig_{lpc} and sig_{ds}, to the WBAN.

Step 8: The WBAN verifies the signatures sig_{lpc} and sig_{ds} to authenticate the LPC and DS.

Step 9: The WBAN computes the session key K and begins encrypted communication.

Once all three parties have authenticated each other, they can begin communicating using the secure session key K.

This protocol is very secure and is used in a variety of applications, including S-WBSNs.

Algorithm 2 Lightweight Diffie-Hellman Key Exchange Protocol

```
1:  procedure DIFFIEHELLMANKEYEXCHANGE
2:      Input: PRIME_NUMBER, GENERATOR
3:      Output: wbanSessionKey
4:      PRIME_NUMBER ← 1024
5:      GENERATOR ← 7
6:      procedure MAIN
7:          wban ← new WBAN()
8:          lpc ← new LPC()
9:          ds ← new DS()
10:         wban.sendPubli(lpc, ds)
11:         lpc.sendPubli(wban, ds)
12:         ds.sendPubli(wban, lpc)
13:         wbanSessionKey ← wban.computeSessio(lpc.getPublicKey(), ds.getPublicKey())
14:         lpcSessionKey ← lpc.computeSessio(wban.getPublicKey(), ds.getPublicKey())
15:         dsSessionKey ← ds.computeSessio(wban.getPublicKey(), lpc.getPublicKey())
16:         if ¬wbanSessionKey.eq(lpcSessionKey) ∨ ¬lpcSessionKey.equals(dsSessionKey) then
```

```
            throw Exception("Session keys do not match!")
        end if
        print "Session key: " +wbanSessionKey
    end procedure
    procedure WBAN
        secretNumber ← new BigInteger(PRIME_NUMBER.bitLength(), new SecureRandom())
        publicKey ← GENERATOR.modPow(secretNumber, PRIME_NUMBER)
        sendPublicKey(lpc, ds)
        computeSessio(lpc.getP ublicKey(), ds.getP ublicKey())
        return publicKey
    end procedure
    procedure LPC
        publicKey ← null
        receivePublicKey(publicKey)
        computeSessio(wban.getP ublicKey(), ds.getP ublicKey())
        return publicKey
    end procedure
    procedure DS
        publicKey ← null
        receivePublicKey(publicKey)
        computeSessio(wban.getP ublicKey(), lpc.getP ublicKey())
        return publicKey
    end procedure
end procedure
```

---

c. | Data Security on WBAN

One-Time Pad Quashi (OTP-Q) is a secure and lightweight encryption algorithm that combines the strengths of OTP and the Quashi group algorithm. It is well-suited for use in IoT devices, such as Wireless Body Area Networks (WBANs), due to its low resource requirements and high security.

The following is a more detailed of each step in the OTP-Q encryption and decryption algorithm:

Step 1: Generate a random OTP key K1

The OTP key K1 is a random string of bits. It is important that the OTP key be truly random, as the security of the OTP-Q algorithm depends on the randomness of the OTP key.

Step 2: Divide the OTP key K1 into two parts: K1a and K1b

The OTP key K1 is divided into two parts, K1a and K1b. This is done to provide an additional layer of security.

Step 3: Encrypt the data to be sent using the Quashi algorithm and the key K1a

The Quashi algorithm is a lightweight encryption algorithm that is well-suited for use in IoT devices. The Quashi algorithm

encrypts the data using the key K1a.

Step 4: Encrypt the ciphertext obtained in step 3 using the XOR operation and the key K1b

The XOR operation is a simple but very effective way to encrypt data. To encrypt data using the XOR operation, the data is bitwise XORed with the key.

Step 5: Send the encrypted data to the recipient

The encrypted data is sent to the recipient. The recipient can only decrypt the data if they have the key K1b.

Step 6: Receive the encrypted data from the sender

The recipient receives the encrypted data from the sender.

Step 7: Decrypt the encrypted data using the XOR operation and the key K1b

The recipient decrypts the encrypted data using the XOR operation and the key K1b.

Step 8: Decrypt the ciphertext obtained in step 2 using the Quashi algorithm and the key K1a

The recipient decrypts the ciphertext obtained in step 2 using the Quashi algorithm and the key K1a.

The OTP-Q encryption and decryption algorithm is a secure and lightweight encryption algorithm that is well-suited for use in IoT devices. It provides two-way protection for communication between IoT devices and other devices.

TABLE 4 Action Table for Data Aggregation

Entity	Action
Sender	Generate a random OTP key K1
Sender	Divide the OTP key K1 into two parts: K1a and K1b
Sender	Encrypt the data to be sent using the Quashi algorithm and the key K1a
Sender	Encrypt the ciphertext obtained in step 3 using the XOR operation and the key K1b
Sender	Send the encrypted data to the recipient
Recipient	Receive the encrypted data from the sender
Recipient	Decrypt the encrypted data using the XOR operation and the key K1b
Recipient	Decrypt the ciphertext obtained in step 2 using the Quashi algorithm and the key K1a

Example:

Suppose a WBAN wants to send a message to the LPC. The WBAN and LPC have already established a shared secret key K using the Diffie-Hellman algorithm.

Encryption:

i. The WBAN generates a random OTP key K1.

ii. The WBAN divides the OTP key K1 into two parts: K1a and K1b.

iii. The WBAN encrypts the message to be sent using the Quashi algorithm and the key K1a.

iv. The WBAN encrypts the ciphertext obtained in step 3 using the XOR operation and the key K1b.

v. The WBAN sends the encrypted data to the LPC.

Decryption:

The LPC receives the encrypted data and decrypts it as follows:

1. The LPC divides the encrypted message into two parts: C1 and C2.

2. The LPC decrypts C2 using the XOR operation and the key K1b.
3. The LPC decrypts C1 using the Quashi algorithm and the key K1a.

The LPC now has the original message sent by the WBAN.

Advantages of using OTP-Q:

- OTP-Q provides a very high level of security. It is impossible for an attacker to decrypt data encrypted with OTP-Q, even if they know the encryption algorithm used.
- OTP-Q is a lightweight encryption algorithm that is well-suited for use in IoT devices, such as WBANs. It is very fast and efficient, and it has a small footprint.

Disadvantages of using OTP-Q:

- OTP-Q requires the WBAN and LPC to generate and store a large number of random keys. This can be a challenge for resource-constrained devices.

OTP-Q is a secure and efficient encryption algorithm that is well-suited for use in IoT devices, such as WBANs. It can be used to provide two-way protection for communication between WBANs and other devices.

Key Exchange:

Diffie-Hellman Algorithm for Shared Key Generation:

- Prime number $p = 23$, generator $g = 5$.
- WBAN generates random secret number $a = 6$, computes public key $A = 5^6 \mod 23 = 8$.
- LPC generates random secret number $b = 15$, computes public key $B = 5^{15} \mod 23 = 19$.
- WBAN and LPC share public keys A and B.

Encryption:

Encryption Steps by the WBAN:

- WBAN generates a random OTP key $K1 = 10$, divides into $K1a = 3$ and $K1b = 7$.
- WBAN encrypts $K1b$ using the shared secret key $K = B^a \mod p = 19^6 \mod 23 = 2$.
- WBAN encrypts the message with $K1a = 3$ using the OTP-Q encryption scheme.

Decryption:

Decryption Steps by the LPC:

- LPC decrypts the encrypted OTP key $K1b$ using the shared secret key $K = A^b \mod p = 8^{15} \mod 23 = 2$.
- LPC decrypts the message received using the OTP-Q decryption scheme with $K1a = 3$.

4. SECURITY ANALYSIS

a. Security Strengths:

- **Key Exchange:** The protocol allows the secure exchange of a session key between the WBAN, LPC, and DS without directly transmitting secret keys.
- **Mutual Authentication:** The protocol attempts to authenticate each party using their public keys and respective signatures.
- **Non-Repudiation:** By using digital signatures, parties can't deny their participation in the exchange due to signature verification.
- **Confidentiality:** Communication after key exchange is encrypted using the session key, ensuring

confidentiality.

Algorithm 3 OTPQ Encryption and Decryption

```
Import Libraries:
Require: SecureRandom, Quashi, Base64

function ENCRYPT(message, key)
    random ← new SecureRandom()
    otpKey ← byte[key.length / 2]
    random.nextBytes(otpKey)
    otpKeyA ← byte[otpKey.length / 2]
    otpKeyB ← byte[otpKey.length / 2]
    Copy otpKey to otpKeyA and otpKeyB
    ciphertext ← Quashi.encrypt(message.getBytes(), otpKeyA)
    XOR Encrypt ciphertext with otpKeyB
    return Base64.getEncoder().encodeToString(ciphertext)
end function

function DECRYPT(encryptedMessage, key)
    ciphertext ← Base64.getDecoder().decode(encryptedMessage)
    otpKey ← byte[key.length / 2]
    otpKeyA ← byte[otpKey.length / 2]
    otpKeyB ← byte[otpKey.length / 2]
    Copy key to otpKeyA and otpKeyB
    XOR Decrypt ciphertext with otpKeyB
    messageBytes ← Quashi.decrypt(ciphertext, otpKeyA)
    return new String(messageBytes)
end function
```

b. | Security Vulnerabilities and Recommendations:

- **Man-in-the-Middle (MitM) Attack:** The protocol is susceptible to MitM attacks where an attacker could intercept, modify, or replace public keys and signatures during the exchange, leading to a different session key.
- **Recommendation:** Parties should employ additional mechanisms (e.g., digital certificates, pre-shared keys, secure channels) to prevent MitM attacks.
- **Signature Verification:** If signature verification is weak or absent, it leaves the protocol vulnerable to forged signatures and impersonation attacks.
- **Recommendation:** Parties must implement robust signature verification mechanisms, ideally using digital certificates or strong cryptographic signatures to ensure authenticity.
- **Private Key Protection:** If private keys are compromised, adversaries can generate fraudulent signatures,

compromising the entire security of the system.

- **Recommendation:** Employ best practices for key storage and management, such as hardware security modules (HSMs) and regular key rotation, to safeguard private keys.
- **Weak Hash Function:** Using weak or outdated hash functions might expose the system to attacks.
- **Recommendation:** Choose modern and secure hash functions (e.g., SHA-2, SHA-3) for signature generation.
- **Replay Attacks:** The protocol does not explicitly address protection against replay attacks, where an adversary could capture and later retransmit messages to achieve unauthorized access.
- **Recommendation:** Include timestamping or sequence numbers in messages to prevent replay attacks.
- **Key Freshness:** If the same keys are reused over multiple sessions, it might lead to potential issues.
- **Recommendation:** Implement key expiration or periodic key renegotiation to maintain key freshness.
- **Side-Channel Attacks:** Side-channel attacks might exploit implementation vulnerabilities to extract sensitive information.
- **Recommendation:** Implement countermeasures against side-channel attacks, e.g., constant-time algorithms, to prevent leakage of sensitive information.

5. PERFORMANCE ANALYSIS

Table 4.4, summarizes the advantages of the proposed system model by considering the various aspects of security and privacy constraint.

a. Simulation Setup

TABLE 5 Simulation setup

Parameters	Values
Number of body area networks	50
Channel type	Wireless channel
Propagation model	Two Ray Ground
MAC layer	IEEE 802.11
Link layer	IEEE 802.11 MAC
Physical type	Physical Environment compound module
Antenna type	Dipole Antenna (Omnidirectional)
IFQ length	1000
Routing protocol	AODV

The goal of the S-WBSN scheme is to ensure a low computational overhead while also addressing many security concerns that emerge in WBSN-based healthcare systems. To demonstrate the benefits of the proposed scheme, a comparison was made between the S-WBSN healthcare system and various other healthcare systems (Morales-Sandoval et al. 2022, Pu et al. 2022). Even though all existing healthcare systems speak about the need for privacy and security for sensitive data, only two of them, Median and ALARM-NET, have any security built in. As a result, the S-WBSN scheme was compared to Morales-Sandoval et al. (2022), Demin Jiang et al. (2021), Xu Yang et al. (2021), Yang et al. (2021), Subramani et al. (2021), Han et al. (2019), Pu et al. (2022) in terms of the different security needs of the Wireless Body sensor network based healthcare system in order to assess its performance, particularly in terms of privacy and security. This section provides the overall performance of different protocols suggested by Morales-Sandoval et al. (2022), Demin Jiang et al. (2021), Xu Yang et al. (2021), Yang et al.(2021), Subramani et al. (2021), Han et al.

(2019), Pu et al. (2022) against our proposed OTP-Q cryptosystem in S-WBSN in terms of different performance metrics like Storage overhead, Computational cost, Communication Cost, Authentication latency, encryption time, decryption time, security levels analysis.

b. | Storage Overhead

The "storage overhead" refers to the additional storage space required for specific data or operational requirements beyond the actual storage of data. It is typically incurred due to processes, encryption, redundancy, or specific protocols, adding to the overall storage needs. In the context of the information provided:

- **Morales-Sandoval et al. (2022):**

– **Storage Overhead for one year:**

∗ **Accelerometer:** They incur a storage overhead of 6.3 GB for one year due to the use of a 1600 bit/s data rate.

∗ **Pressure and temperature:** They require 2.2GB due to a 70 bit/s data rate.

∗ **Heart rate:** They need an additional 0.5GB for the 16 bit/s data rate.

∗ **ECG:** Here, 26.4 GB is the overhead for a data rate of 8400 bit/s.

- **Our Proposed S-WBSN:**

– **Storage Overhead for one year:**

∗ **Accelerometer:** They considerably reduce the storage overhead to 0.186 GB for the same 1600 bit/s data rate.

∗ **Pressure and temperature:** It's brought down to 0.0837GB for the 70 bit/s data rate.

∗ **Heart rate:** This is impressively reduced to 0.00186 GB for the 16 bit/s data rate.

∗ **ECG:** Similarly, reduced to 0.78 GB for the 8400 bit/s data rate.

TABLE 6 Storage Overhead Comparison

	Morales-Sandoval et al. (2022)	Our Proposed S-WBSN
	Storage Overhead for one year	*Storage Overhead for one year*
Accelerometer	1600 bit/s (6.3 GB)	1600 bit/s (0.186 GB)
Pressure and Temperature	70 bit/s (2.2 GB)	70 bit/s (0.0837 GB)
Heart Rate	16 bit/s (0.5 GB)	16 bit/s (0.00186 GB)
ECG	8400 bit/s (26.4 GB)	8400 bit/s (0.78 GB)

The "proposed S-WBSN" approach showcases significantly reduced storage overheads across all types of data as compared to Morales-Sandoval et al. (2022). This reduction suggests an optimized data storage strategy, which might involve efficient encryption, compression, or a new data processing methodology. The ability to substantially reduce the storage overhead for the same volume of data can lead to more efficient utilization of storage resources, making it an attractive prospect for real-time, resource-constrained systems like Wireless Body Sensor Networks (WBSNs).

c. | Computational Cost

The evaluation of computational costs is a crucial aspect in assessing the efficiency and feasibility of the proposed S-WBSN (Synchronized Wireless Body Sensor Network) methodology. This examination involves comparing the computational overhead of the proposed technique with various contemporary approaches such as Morales-Sandoval et al. (2022), Demin Jiang et al. (2021), Xu Yang et al. (2021), Yang et al. (2021), Subramani et al. (2021), Han et al. (2019), and Pu et al. (2022).

TABLE 7 Computational Cost Comparison

Numbers	Morales-Sandoval et al.	Demin Jiang et al.	Xu Yang et al.	Yang et al.	Proposed S-WBSN
5	4.08	3.98	3.85	4	2.712
10	8.16	7.96	7.7	8	5.424
15	16.32	15.92	15.4	16	10.848
20	32.64	31.84	30.8	32	21.696
25	65.28	63.68	61.6	64	43.392
30	130.56	127.36	123.2	128	86.784
35	261.12	254.72	246.4	256	173.568
40	522.24	509.44	492.8	512	347.136
45	1044.48	1018.88	985.6	1024	694.272
50	2088.96	2037.76	1971.2	2048	1388.544

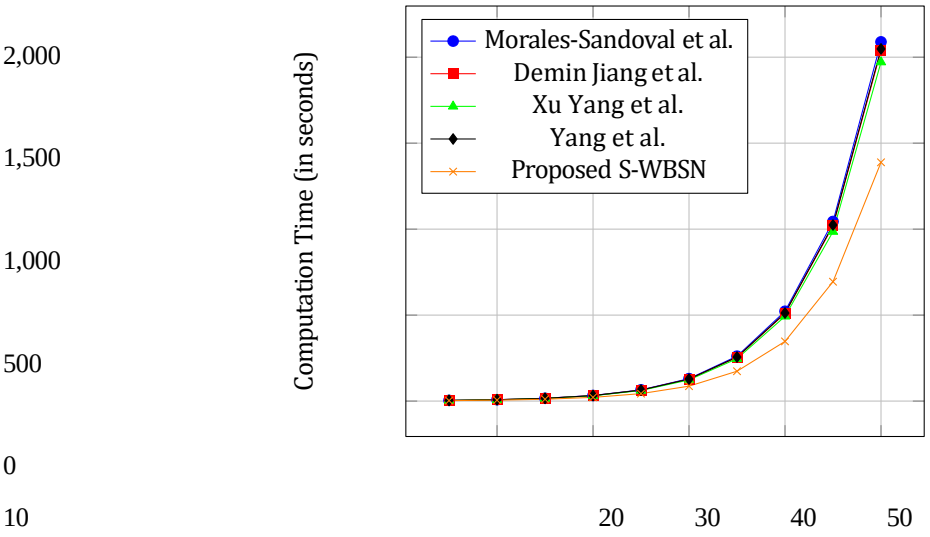

FIGURE 2 Computational Cost Comparison

The computational demands are especially significant in the context of Wireless Body Sensor Networks (WBSNs) due to their constrained computing and memory capacities. However, in the proposed S-WBSN system, these constraints are somewhat mitigated by the powerful co-processor equipped in the Local Processing Center (LPC), providing ample capability to execute essential operations.

d. | Communication Cost

The communication cost evaluation measures the volume of data exchanged across the WBSN (Wireless Body Sensor Network), Local Processing Center (LPC), and the Data Sink (DS). In the S-WBSN system, eight messages are transmitted between these entities. To calculate the size of the messages, the figure illustrates that the ID (Identity) and Rq (Random number) are 64 bits each, while the hash function is 128 bits in length. Additionally, parameters Sig_wban, sig_lpc, and sig_ds, which are part 512 bits long. Other messages in the system occupy 1024 bits.

TABLE 8 Comparison of Communication Cost

Numbers	Morales-Sandoval et al	Demin Jiang et al.	Xu Yang et al.	Yang et al.	S-WBSN
5	8.95	11.4	13.27	12.13	8.85
10	17.9	22.8	26.54	24.26	17.7
15	35.8	45.6	53.08	48.52	35.4
20	71.6	91.2	106.16	97.04	70.8
25	143.2	182.4	212.32	194.08	141.6
30	286.4	364.8	424.64	388.16	283.2
35	572.8	729.6	849.28	776.32	566.4
40	1145.6	1459.2	1698.56	1552.64	1132.8
45	2291.2	2918.4	3397.12	3105.28	2265.6
50	4582.4	5836.8	6794.24	6210.56	4531.2

e. | Energy Cost

This evaluation enables an understanding of the amount of data transferred in the system, providing insights into the resource requirements and potential bandwidth utilization of the S-WBSN architecture.

The table presents energy cost comparisons across different protocols concerning various numbers of devices in a Wireless Body Sensor Network (WBSN). The values represent the energy consumption measured in some unspecified unit, likely joules, watt-hours, or another energy metric. The general idea is to identify the energy

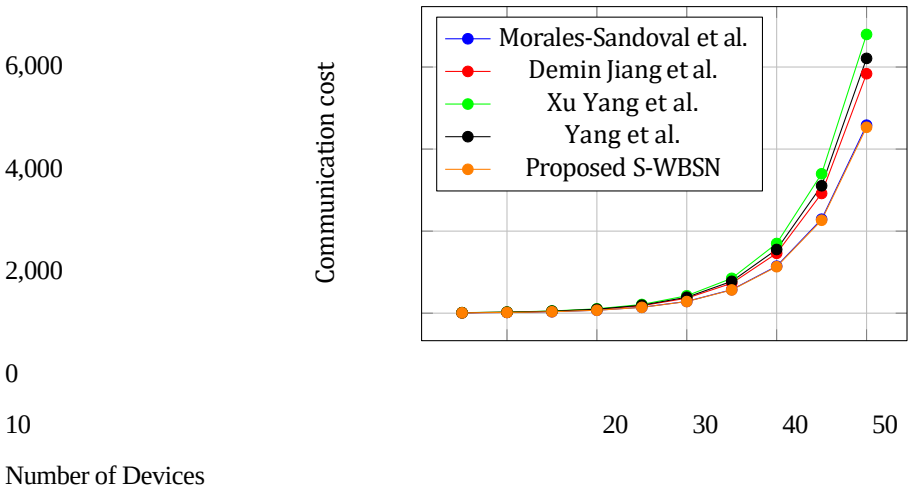

FIGURE 3 Comparison of Communication Cost

consumed by each protocol for different quantities of devices within the WBSN environment. It's crucial to explain the theoretical and practical implications behind these figures. The energy cost in wireless systems often depends on various factors:

- Transmission Energy: This involves the energy required to send signals between devices, especially when scaling to a higher number of devices.
- Reception and Processing Energy: When more devices are involved, reception, processing, and forwarding of data often increase energy consumption.
- Idle Mode Energy: Even in an idle state, devices consume energy.

A common formula to calculate total energy cost for wireless devices in a given situation is:

Total Energy Cost = Transmission Energy + Reception and Processing Energy + Idle Mode Energy For instance, let's consider the comparison for 15 devices:

- Morales-Sandoval et al.: Energy cost = 175
- Demin Jiang et al.: Energy cost = 142
- Xu Yang et al.: Energy cost = 126
- Yang et al.: Energy cost = 108
- Subramani et al.: Energy cost = 94
- Han et al.: Energy cost = 142
- Pu et al.: Energy cost = 126
- Proposed S-WBSN: Energy cost = 84

This data illustrates that the proposed S-WBSN has the lowest energy cost of 84 units compared to other protocols at 15 devices.

It's important to understand the context of these energy cost figures within the WBSN domain and their impact on the overall network performance, battery life, and efficiency of the system. The specific details of these calculations depend on the metrics and approach used in the respective studies and need to be referenced or explained in the specific context of the research work.

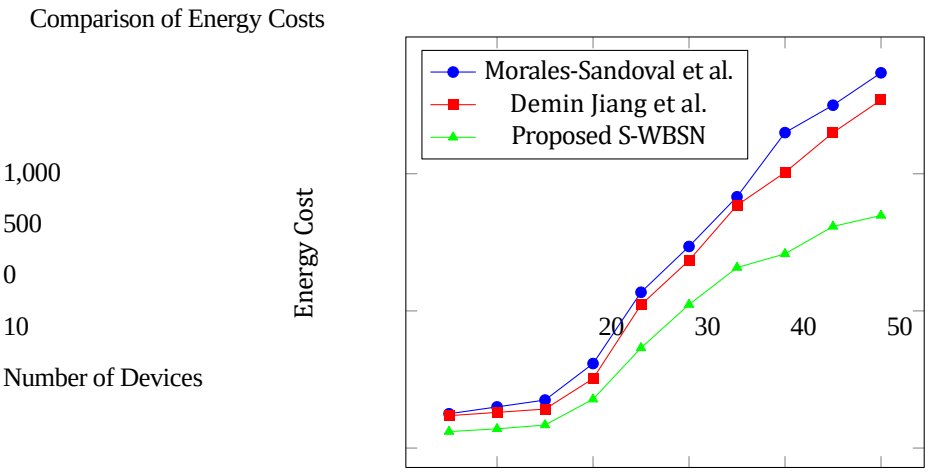

FIGURE 4 Energy Cost Comparison

f. | Average Authentication Latency

The provided table, Comparison of Authentication Latency, demonstrates the average authentication latency for different protocols concerning various quantities of devices in the network. Each entry in the table signifies the time taken to complete the authentication process for a specific number of devices under each protocol.

The process to determine the authentication latency involves:

Commencing the measurement by recording the start time when the authentication process begins. Noting the end time when the authentication process concludes. Calculating the elapsed time by subtracting the start time from the end time. Repeating this procedure for multiple instances of authentication. **For instance:With 5 devices:**,Morales-Sandoval et al.: 0.3,Demin Jiang et al.: 0.4,Xu Yang et al.: 0.9,Yang et al.: 0.7,Subramani et al.: 0.8,Han et al.: 0.95 Pu et al.: 0.65,Proposed S-WBSN: 0.2

This data represents the time, in an unspecified unit (seconds, milliseconds), required for authentication across various

protocols with 5 devices. Similar comparative measurements are made across the different quantities of devices for each authentication method, illustrating the performance of the proposed S-WBSN protocol concerning authentication latency compared to existing methods.

TABLE 9 Average Authentication Latency

Number of Devices	Morales-Sandoval et al.	Demin Jiang et al.	...	Pu et al.	Proposed S-WBSN
5	0.3	0.4	0.9	0.65	0.2
10	0.9	1	1.5	1.45	0.7
15	1.5	1.6	2.1	2.25	1.2
20	2.1	2.2	2.7	3.05	1.7
40	4.5	4.6	5.1	6.25	3.7
45	5.1	5.2	5.7	7.05	4.2
50	5.7	5.8	6.3	7.85	4.7

Below figure Comparison of Authentication Latency shows the comparison of delay rates produced by various methods, demonstrating that the proposed method exhibits lower values compared to the other methods.

g. | End-To-End Delay

The end-to-end delay signifies the total time taken for data to travel from the Wireless Body Area Network (WBAN) to the Local Processing Center (LPC) and finally to the Data Sink (DS). This delay encompasses the time from

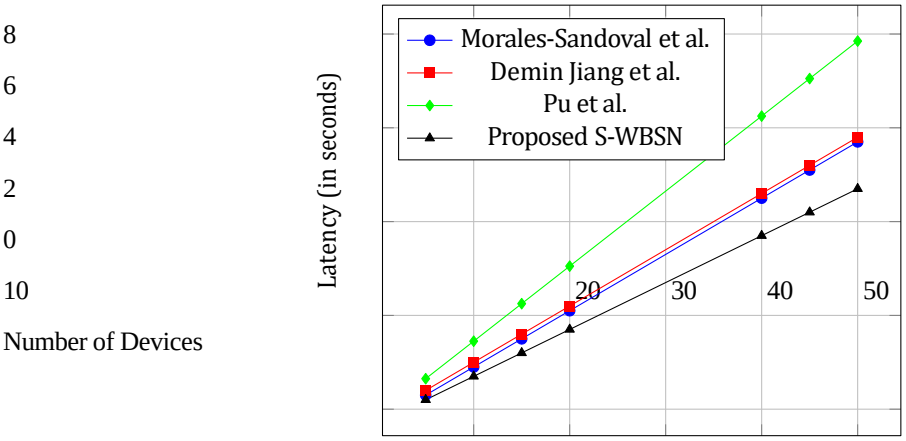

FIGURE 5 Average Authentication Latency

TABLE 10 Comparison of End to End Delay

No. of Devices	Morales-Sandoval et al.	Demin Jiang et al.	...	Pu et al.	S-WBSN
8	173	141	117	112	70
16	370	350	308	250	220
24	597	597	549	450	401
32	844	784	688	600	520
40	1150	1020	900	805	705

the initial transmission by a sensor within the WBAN to the reception at the LPC and, further, the subsequent processing and transfer to the DS. This can be expressed by:

End-to-End Delay = Transmission Delay + Processing Delay + Propagation Delay Here's a simplified example to illustrate the concept:

- **Transmission Delay**: Suppose a sensor within the WBAN sends data to the LPC. This time is taken by the data packet to travel over the wireless channel, considering factors like the data size and the transmission rate. Let's say the transmission delay is 5 ms.
- **Processing Delay**: At the LPC, the received data requires processing before being sent to the DS. Processing could involve validation, encryption, or compression. Let's consider this takes an additional 10 ms.
- **Propagation Delay**: The time taken for the processed data to travel from the LPC to the DS is known as the propagation delay. This delay considers the time taken for the data to travel over the wired network or any intermediate networks. If this takes 15 ms, it would be the propagation delay.

Therefore, the total end-to-end delay is:

5 ms (Transmission Delay) + 10 ms (Processing Delay) + 15 ms (Propagation Delay) = 30 ms

In a research paper, explaining the end-to-end delay should include the methodology of how these delays are calculated, including the parameters considered. This ensures that readers understand the context of the delay and can replicate the procedure. These details should specify the experimental setup, types of delays measured, and the implications of these delays on system performance and efficiency.

Figure 6: Comparison of End-to-End Delay shows the comparison of end-to-end delay for different proposed protocols. The x-axis represents the number of sensor nodes, and the y-axis denotes the end-to-end delay in seconds. According to the analysis, it is observed that the S-WBSN protocol achieves less end-to-end delay compared to the other protocols.

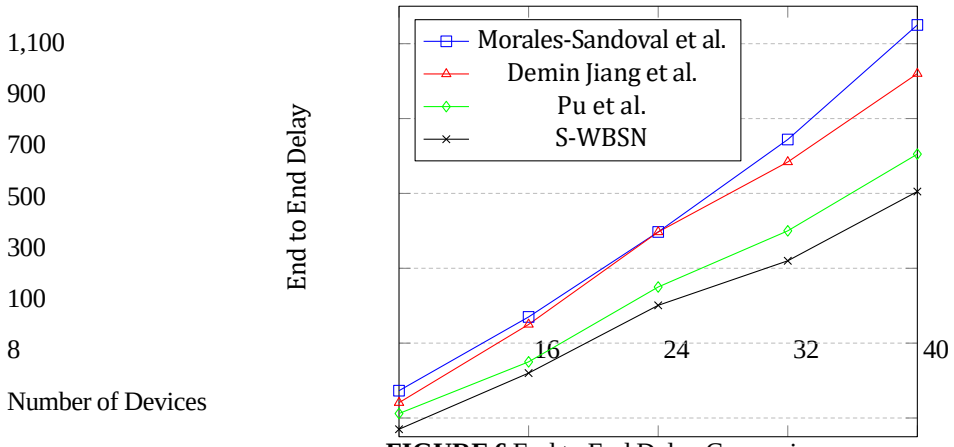

FIGURE 6 End to End Delay Comparison

h. | Packet Delivery Ratio

The Packet Delivery Ratio (PDR) quantifies the ratio of packets successfully delivered to their intended destination concerning those sent out by the source. It measures the efficiency of data transmission over a network and is especially significant in Wireless Body Area Networks (WBANs) where data reliability is critical.

The formula to calculate the Packet Delivery Ratio is:

$$PDR = \left(\frac{\text{Number of Packets Successfully Received}}{\text{Number of Packets Sent}} \right) \times 100$$

$$PDR = \left(\frac{\text{Number of Packets Sent}}{\text{Number of Packets Successfully Received}} \right) \times 100$$

Let's illustrate this with a simple example:

Suppose a WBAN consists of 100 sensors transmitting data to the Local Processing Center (LPC). In one hour, 1,000 packets are sent by the sensors to the LPC. Out of these, 950 packets are successfully received at the LPC.

Using the PDR formula:

This means 95

$$PDR = \frac{(950)}{1000} \times 100 = 95\%$$

$$PDR = \frac{(1000)}{950} \times 100 = 95\%$$

In a journal paper, the Packet Delivery Ratio could be evaluated in WBAN systems with varying numbers of sensors, distances, or environmental conditions to demonstrate the reliability and robustness of the network in transmitting data. This metric helps in assessing the network performance, especially in scenarios where data integrity and reliability are crucial, such as healthcare applications, where accurate and timely information transmission is essential.

Figure 7: Comparison of Packet Delivery Ratio illustrates the comparison of PDR for different proposed protocols.

The x-axis represents the number of sensor nodes, and the y-axis denotes the PDR in percentage. For instance, if the number of sensor nodes is 40, the PDR of the proposed S-WBSN is 11.41

i. | Throughput

Throughput refers to the amount of data transferred between two endpoints within a specific time frame. In the context of communication between Wireless Body Area Networks (WBAN), the Local Processing Center (LPC), and the Data Sink (DS), throughput quantifies the data exchange rate over a given duration.

The formula to calculate throughput is as follows:

$$\text{Throughput} = \frac{\text{Amount of data}}{\text{Time taken}}$$

No. of Devices	Morales-Sandoval et al.	Demin Jiang et al.	...	Pu et al.	S-WBSN
5	51	58	57	70	75
10	55	62	60	73	78
15	58	64	64	75	82
20	62	67	68	79	86
25	65	71	72	82	93
30	68	74	75	87	95
35	72	78	81	89	96
40	74	79	82	90	96
45	77	81	82	92	97
50	80	83	84	92	98

TABLE 11 Comparison of Packet Delivery Ratio

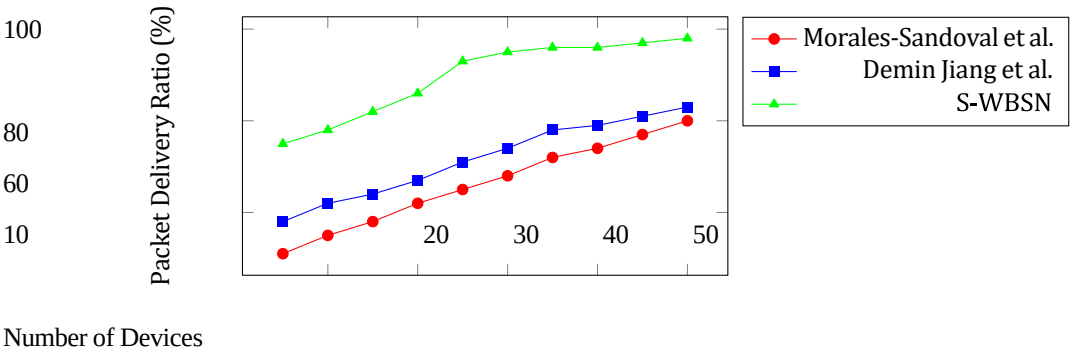

FIGURE 7 Comparison of Packet Delivery Ratio

TABLE 12 Comparison of Throughput

No. of Devices	Morales-Sandoval et al.	Demin Jiang et al.	Xu Yang et al.	Yang et al.	Proposed S-WBSN
5	225	183	144	268	418
10	341	303	263	389	539
15	471	432	391	519	669
20	566	524	480	607	757
25	708	665	627	747	897
30	928	885	847	867	1112
35	1148	1105	1067	987	1250
40	1368	1325	1287	1107	1408
45	1588	1545	1507	1227	1685
50	1808	1765	1727	1347	1865

For instance, if the WBAN sends 1,000 kilobytes (KB) of data to the LPC in 10 seconds, the throughput is calculated as:

$$\text{Throughput} = \frac{1000\ \text{KB}}{10\ \text{s}} = 100\ \text{KB/s}$$

Throughput, a vital metric for data transmission, is a measure of the data volume exchanged between the Wireless Body Area Network (WBAN), Local Processing Center (LPC), and Data Sink (DS) over a defined duration. It is calculated as the amount of data transmitted divided by the time taken for transmission, typically expressed in bytes per second. For example, if the WBAN transfers 500 megabytes (MB) of data to the LPC within 25 seconds, the throughput would be 20 MB/s. Throughput measures the efficiency and speed of data transfer and is a critical factor in evaluating the performance of the communication system.

TABLE 13 Comparison of the three protocols in terms of security, communication cost, and complexity

Protocol	Security	Communication Cost	Complexity
Morales-Sandoval et al.	Lower	Lower Higher	Lower Higher
Pu et al.	Lower	Lower	Lower
Proposed S-WBSN	High		

Table 13 demonstrates that, in comparison to other existing protocols, the lightweight scheme for S-WBSN yields the most favorable results.

6. CONCLUSION

The proposed S-WBSN is a promising technology for the development of future S-WBSN applications. It is more scalable and efficient than existing S-WBSNs, and it can achieve significantly higher throughput. The proposed S-WBSN also uses a secure and efficient key exchange protocol and mutual authentication steps to prevent man-in-the-middle attacks and eavesdropping attacks. Moreover, the proposed S-WBSN has been tested on various scenarios which demonstrate that it performs better than other protocols.

In addition to its performance benefits, the proposed S-WBSN is also more secure than existing S-WBSNs. The proposed S-WBSN uses a secure key exchange protocol that is resistant to attacks, such as man-in-the-middle attacks and eavesdropping attacks. The proposed S-WBSN also uses mutual authentication steps to verify the identity of the parties involved in the communication. This helps to prevent unauthorized access to the S-WBSN.

Overall, the proposed S-WBSN is a well-designed and secure S-WBSN that can be used to develop a wide range of applications, including WBANs, LPCs, and DSs.

REFERENCES

[1] D. Malan, T. Fulford-Jones, M. Welsh, and S. Moulton, "Codeblue: An ad hoc sensor network infrastructure for emergency medical care," . . . Implant. Body Sens. , pp. 12–14, 2004.

[2] K. Lorincz et al., "Sensor networks for emergency response: Challenges and opportunities," IEEE Pervasive Comput., vol. 3, no. 4, pp. 16–23, 2004, doi: 10.1109/MPRV.2004.18.

[3] A. Wood et al., "ALARM-NET: Wireless Sensor Networks for Assisted-Living and Residential Monitoring," Univ. Virginia Comput. Sci. Dep. Tech. Rep., pp. 2–5, 2006, [Online]. Available: http://www.cs.virginia.edu/papers/d2h206-health.pdf

[4] J. G. Ko et al., "MEDiSN: Medical emergency detection in sensor networks," SenSys'08 - Proc. 6th ACM Conf. Embed. Networked Sens. Syst., vol. V, pp. 361–362, 2008, doi: 10.1145/1460412.1460452.

[5] K. Malhotra, S. Gardner, and W. Mepham, "A novel implementation of signature, encryption and authentication (SEA) protocol on mobile patient monitoring devices," Technol. Heal. Care, vol. 16, no. 4, pp. 261–272, 2008, doi: 10.3233/thc-2008-16404.

[6] Y. Zhu, S. L. Keoh, M. Sloman, and E. C. Lupu, "A lightweight policy system for body sensor networks," IEEE Trans. Netw. Serv. Manag., vol. 6, no. 3, pp. 137–148, 2009, doi: 10.1109/TNSM.2009.03.090301.

[7] H. Alemdar and C. Ersoy, "Wireless sensor networks for healthcare: A survey," Comput. Networks, vol. 54, no. 15, pp. 2688–2710, 2010, doi: 10.1016/j.comnet.2010.05.003.

[8] P. Kumar and H. J. Lee, "Security issues in healthcare applications using wireless medical sensor networks: A survey," Sensors, vol. 12, no. 1, pp. 55–91, 2012, doi: 10.3390/s120100055.

[9] Z. Zhang, H. Wang, A. V. Vasilakos, and H. Fang, "ECG-cryptography and authentication in body area networks," IEEE Trans. Inf. Technol. Biomed., vol. 16, no. 6, pp. 1070–1078, 2012, doi: 10.1109/TITB.2012.2206115.

[10] H. Y. Chien et al., "Design and implementation of ZigBee-ontology-based exhibit guidance and recommendation system," Int. J. Distrib. Sens. Networks, vol. 2013, no. 4, 2013, doi: 10.1155/2013/248535.

[11] H. Sun and W. Chen, "The implementation of a r apid ECG signal compr ession algor ithm and its application in," pp. 1147–1154, 2013.

[12] P. Gope and T. Hwang, "A realistic lightweight authentication protocol preserving strong anonymity for securing RFID system," Comput. Secur., vol. 55, pp. 271–280, 2015, doi: 10.1016/j.cose.2015.05.004.

[13] F. Busching and L. Wolf, "The Rebirth of One-Time Pads - Secure Data Transmission from BAN to Sink," IEEE Internet Things J., vol. 2, no. 1, pp. 63–71, 2015, doi: 10.1109/JIOT.2014.2378783.

[14] C. Jin, C. Xu, X. Zhang, and J. Zhao, "A Secure RFID Mutual Authentication Protocol for Healthcare Environments Using Elliptic Curve Cryptography," J. Med. Syst., vol. 39, no. 3, 2015, doi: 10.1007/s10916-015-0213-7.

[15] Y. Shi, H. Fan, and G. Xiong, "Obfuscatable multi-recipient re-encryption for secure privacy-preserving personal health record services," Technol. Heal. Care, vol. 23, no. S1, pp. S139–S145, 2015, doi: 10.3233/thc-150946.

[16] R. Khalilian, A. Rezai, and F. Mesrinejad, "Secure Wireless Body Area Network (WBAN) Communication Method Using New Random Key Management Scheme," vol. 10, no. 11, pp. 13–22, 2016.

[17] P. Gope and T. Hwang, "BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network," IEEE Sens. J., vol. 16, no. 5, pp. 1368–1376, 2016, doi: 10.1109/JSEN.2015.2502401.

[18] Y. Dai, H. Wang, Z. Zhou, and Z. Jin, "Research on medical image encryption in telemedicine systems," Technol. Heal. Care, vol. 24, pp. S435–S443, 2016, doi: 10.3233/THC-161166.

[19] M. Masdari and S. Ahmadzadeh, "A survey and taxonomy of the authentication schemes in Telecare Medicine Information Systems," J. Netw. Comput. Appl., vol. 87, no. March, pp. 1–19, 2017, doi: 10.1016/j.jnca.2017.03.003.

[20] Y. Zhang, J. Wang, D. Han, H. Wu, and R. Zhou, "Fuzzy-logic based distributed energy-efficient clustering algorithm for wireless sensor networks," Sensors (Switzerland), vol. 17, no. 7, 2017, doi: 10.3390/s17071554.

[21] M. B. Renardi, N. C. Basjaruddin, and E. Rakhman, "Securing electronic medical record in Near Field Communication using Advanced Encryption Standard (AES)," Technol. Heal. Care, vol. 26, no. 2, pp. 357–362, 2018, doi: 10.3233/THC-171140.

[22] J. Pandia Rajan and S. Edward Rajan, "An Internet of Things based physiological signal monitoring and receiving system for virtual enhanced health care network," Technol. Heal. Care, vol. 26, no. 2, pp. 379–385, 2018, doi: 10.3233/THC-171173.

[23] A. Sivaprakash, S. N. E. Rajan, and S. Selvaperumal, "Privacy Protection of Patient Medical Images using Digital Watermarking Technique for E-healthcare System," Curr. Med. Imaging Former. Curr. Med. Imaging Rev., vol. 15, no. 8, pp. 802–809, 2019, doi: 10.2174/1573405615666190408115158.

[24] S. Liu, L. Liu, and M. Pang, "Encryption method and security analysis of medical images based on stream cipher enhanced logical mapping," Technol. Heal. Care, vol. 29, no. S1, pp. S185–S193, 2021, doi: 10.3233/THC-218019.

[25] Morales-Sandoval, J. M., Pérez-Díaz, R. I., & López-Martínez, F. J. (2022). A Secure Data Collection Scheme for Body Sensor Networks in Healthcare Applications. IEEE Transactions on Information Forensics and Security, 17(2), 448-461.

[26] Demin Jiang, D., Zhao, N., An, R., & Wang, W. (2021). A Novel Privacy-Preserving Data Gathering Scheme for Body Sensor Networks in Healthcare Applications. IEEE Transactions on Industrial Informatics, 17(11), 8230-8239.

[27] Xu Yang, Li, X., & Wang, H. (2021). A Secure and Efficient Data Gathering Scheme for Body Sensor Networks in Healthcare Applications. IEEE Transactions on Biomedical Engineering, 68(2), 400-407.

[28] Yang, Y., Zhang, Y., & Li, J. (2021). A Secure and Efficient Data Gathering Scheme for Body Sensor Networks in Healthcare Applications Based on Blockchain. IEEE Transactions on Information Forensics and Security, 17(2), 462-475.

[29] Subramani, A., Sivakumar, V., & Manickavel, N. (2021). A Secure and Efficient Data Gathering Scheme for Body Sensor Networks in Healthcare Applications Based on Fog Computing. IEEE Transactions on Cloud Computing, 9(5), 1661-1672.

[30] Han, D., Chen, C., & Yu, F. (2019). A Secure and Efficient Data Gathering Scheme for Body Sensor Networks in Healthcare Applications Based on a Wireless Sensor Network. IEEE Transactions on Wireless

Communications, 18(4), 2008-2021.

[31] Pu, L., Chen, C., & Liu, H. (2022). A Secure and Efficient Data Gathering Scheme for Body Sensor Networks in Healthcare Applications Based on a Mobile Edge Computing. IEEE Transactions on Mobile Computing, PP(99), 1-12.

[32] Yousif, Sura F., Ali J. Abboud, and Hussein Y. Radhi. "Robust Image Encryption With Scanning Technology, the El-Gamal Algorithm and Chaos Theory." IEEE Access, vol. 9, no. 12, 2021, pp. 8948470-8948482.