Wireless Personal Communications (2020) 111:2605–2623
https://doi.org/10.1007/s11277-019-07005-6

An Improved Authentication Protocol for Wireless Body Sensor Networks Applied in Healthcare Applications

Kakali Chatterjee[1]

Published online: 12 December 2019

Abstract
Wireless body sensor networks are now very popular for modern healthcare applications like health monitoring, remote healthcare, emergency healthcare etc. This healthcare application mainly used for constant monitoring of health specific data while doing regular activities. The wireless body area network is consisted of small wearing sensors which are implanted in human body for capturing medical data and send to a medical server through a network connector to base station. A major issue is secure transmission of patient's medical healthcare information to the medical server through wireless communication. Also the data collected in this network is very sensitive because on the basis of this clinical data, further treatment will be occurred. Therefore, security requirements such as confidentiality, integrity, authenticity should be guaranteed during communication. This paper proposes a strong mutual authentication protocol based on public key cryptography for satisfying all security requirements. The proposed authentication approach resists the major vulnerable attacks in wireless body sensor networks with low computational and communicational load.

Keywords Mutual authentication · Paillier cryptosystem · Body sensor networks

1 Introduction

Recent days healthcare applications are playing a major role for remote health monitoring. These applications are mainly used the patient data which is captured by the wearable sensors. These wearable sensors are the part of a Wireless Body Area Networks for patient monitoring purpose. The implanted sensors will collect the data from the patient body and the smart phone will collect the data from the sensors to supply it to the medical server [1].

Originally the wireless body area network (WBAN) was proposed by Zimmerman [2] uses wireless personal area network (WPAN) technology. In current days, the WBAN has played an important role in research community and health organizations for smart health applications. Normally in this type of networks many low power intelligent sensors are placed in or around the human body for measuring vital parameters such as heart

✉ Kakali Chatterjee
kakali2008@gmail.com

[1] CSE Department, NIT Patna, Patna, India

rate, pulse, blood pressure, and temperature and oxygen saturation etc. Real-time monitoring could be implemented remotely through these sensors. A body sensor based healthcare application can provide many benefits in health sector also. This type of application can provide a convenient environment for monitoring those vital parameters during daily lives activity and medical conditions for long term critically ill (paralyzed patient, cancer patient) person to reduce the huge hospitalization cost. The sensed data is stored in health cloud so that doctors can view these data at anytime from anywhere in the country. In such environment, one of the biggest challenges is to send the data securely to the cloud server because any changes of this sensitive data may cause wrong diagnosis and wrong treatment of the patient. As the data gathered from the sensors will send to the base stations through a personal server (network coordinator), an adversary can easily capture the data from the wireless channels and modify that. This wrong data could endanger patient's life. Also the personal server can be captured by the adversary with wrong intension. Hence strong authentication and secured communication is essential in this scenario. This is the main objective of this research work.

In WBAN, several authentication schemes based on Receiver Signal Strength [3–6] and Proximity [7–9] and Biometric based [10–12] has been found in the literature. The drawback of these schemes is mainly depending upon the distance between devices (sensors) which must be half of the wavelength distance of each other. These drawbacks can be overcome using cryptography based scheme because those schemas mainly depend upon the operational complexity not with signal strength or location. But implementation of suitable cryptographic protocol in this environment is challenging as these sensor devices are constrained in terms of memory, computing power and energy supply.

The traditional public key cryptography based authentication schemes are also found in literature [13–17]. One of the most secure public key cryptographic techniques is Elliptic Curve Cryptography which provides the highest security with smaller key size [14]. Compared to traditional techniques, ECC is more suitable for sensor networks due to the constraints like limited computing capabilities and battery capacity. In general practical implementations, ECC public key is distributed through digital certificates with the help of public key infrastructure (PKI). The distribution and management of certificates increases communicational overload. Thus ECC based authentication schemes [18–22] are not suitable for their complex operations. Shamir [23] first proposed Identity based cryptography where the identity plays the role of the public key. Therefore, the ID-based cryptography mainly overcomes the certificates management problem of the trusted third party. Yang et al. [24] proposed an ID based mutual authentication scheme for mobile devices. Yoon et al. [25] shows the demerits of this scheme through cryptanalysis. He et al. [26] used ECC to design a new ID based authentication scheme which is provably secure. Later on Wang et al. [27] pointed that He et al.'s scheme suffers parallel session attack, reflection attack and also does not provide mutual authentication. Biswas et al. [28] proposed another ECC based authentication to remove security weakness in Yoon and Yoo's scheme. But Truong et al. [29] found that Yoon et al. scheme could not resist the denial of service attack. Some light weight authentication scheme have been found in wireless sensor networks [30–32] which fails to maintain perfect forward secrecy in communication.

Although the above ID-based authentication schemes is mainly suitable for client server environment with better performance than earlier schemes, but not suitable for BSN due to the algorithmic complexity. This paper proposes an improved authentication scheme based on public key cryptography for not only data security but also to maintain the privacy in BSN. The proposed scheme is based on Paillier cryptosystem which have homomorphic and self-binding property. This keeps the sensed data private while third party processes

the data without seeing it which is essential for body sensor network. Also this cryptosystem provides randomness in encrypted data, so that the same plain text after several encryptions produces different cipher texts. Hence the main contribution in this paper is as follows:

- The proposed scheme is efficiently authenticates user device using biometric features while data transmission from body sensors to health server in WBAN.
- This scheme used Pallier cryptosystem which is mainly used for privacy preservation of sensor data.
- Proposed Authentication approach enforces very light computational load due to simple operations like exclusive-OR operations.
- Mutual authentication as well as secret session key generation is essentially improves security.
- Proposed scheme also has low communicational load and messages are encrypted using symmetric encryption for this critically constrained devices.

The rest of the paper is organized as follows:
Section 2 presents Background, Sect. 3 provides Proposed Mutual Authentication Protocol; Sect. 4 discusses Security Analysis; Sect. 5 presents Performance Analysis; Finally, concluded in Sect. 6.

2 Background

In this section security threats and security requirements in WBAN are discussed.

2.1 Security Requirements, Threats and Solutions in WBAN

There are many sensor nodes in WBSN which are involve in data sensing. After that the gateway node will collect the sensed data and transmitted it to a health server via internet [33]. In such scenario, following security requirements are found in WBSN:

- Data Confidentiality is essential to protect the data from a disclosure, the system require data confidentiality.
- Data integrity is necessary as an adversary can alter the data that is transmitted over an insecure channel.
- Data authentication is essential to ensure that the data is coming from trusted node.
- Data availability is to ensure that the patient's information is accessible to the doctor.
- Efficient key management is essential to securely transmission of data
- Efficient encrypting techniques are essential as the computation power is limited.
- Anonymity and Non traceability is required to maintain the privacy of the patient data.
- Perfect Forward Secrecy must be maintained even if the secret keys of the client and application provider is compromised.
- Mutual Authentication is essential to ensure user and server.

WBANs are vulnerable to many threats such are listed below:

- Message Modification- This type of threat is applicable to the message after intercepting it from the network. Sometimes the adversary can delete or delay the data to harm the person. Strong encryption algorithm and hash function can be used for prevention of this attack.
- Message Disclosure- This threat is activated when an application fails to properly protect sensitive information from others. Due to this privacy threat, some sensitive private data may be disclosed to those who are not supposed to get the information.
- Unauthorized access- When some unauthorized user gets some access grant, the data and the resources can be misused. Unauthorized access can be prevented by strong access control policy.
- Denial of Service- Due to this attack, the user cannot get the desired service. The attacker might use different strategies to achieve this such as by inserting bogus request to a server or drop request packets of the client. It can be resisted by implementing suitable Intrusion Detection System.
- Node tampering- An adversary can gain full control over a sensor node by this attack.

Also he can perform malicious activity by capturing that node. It can be resisted by any inconsistency detection algorithm.

- Routing attacks- Fake routing messages can be inserted in communication channels by this attack to divert the routes of the messages. Hence it is preferable to use secure routing protocols.
- Jamming Attacks- Due to this attack, the adversary can perform radio frequency interference to block the entire network. One simple solution is to apply high transmission power on jammed channels to avoid this attack.

2.2 Paillier Cryptosystem

The Paillier Cryptosystem is a modular, public key encryption scheme created by Pascal Paillier, with several interesting properties [34]. This public key encryption is based on composite residuosity classes. It has homomorphic property through which a person can delegate to process his own data without giving access on it. Also, it has self-blinding property through which a plaintext can be mapped into many different ciphertexts. Like all cryptosystems, it has three processes: Key generation, encryption and decryption.

In the key generation process, to construct the public key, one must choose two large primes, p and q, then calculate their product, n = p.q. Then a semi-random, nonzero integer, g, in Z_n^2, must be selected, such that the order of g is a multiple of n in Z_n^{*2} [Z_n^{*2} being the units, or invertible elements, of Z_n^2].

The modular paillier cryptosystem uses the concept of public key encryption technique. To encrypt the message, the sender first generates a public key by choosing two large primes number p and q. Now, calculates n = p*q. For example [34], consider p = 7 and q = 11. The calculated value of n is 77. After that, a semi-random, non-zero integer g is chosen such that the order of g is a multiple of n in Z_n^{*2}. The choose value of g is 5652, which fulfill the addressed properties. Thus, the generated public key is represented by (n,g) = (77, 5652).

Steps for Encryption:

1. Generate the public key.

In this example, the generated public key is (77, 5652).

2. Create a message m such that $m \in Z_n$.
   Let m = 42.
3. Choose a random nonzero integer $r \in Z_n$.
   Let r = 23.
4. Compute the ciphertext $c \equiv g^m r^n \bmod n^2$.
   The value of $c \equiv (5652)^{42} * (23)^{77} \bmod 5929 \equiv 4624 \bmod 5929 = 4624$

Steps for Decryption:

1. Compute $\lambda(n) = \text{lcm}[(p-1)(q-1)]$ by Carmichael's function.
   $\lambda(77) = \text{lcm}[(6),(10)] = 30$
2. Calculation of $u = g^{\lambda(n)} \bmod n^2$ is necessary for the decryption of the message.
   $U = (5652)^{30} \bmod 5929 = 3928$
3. $L(u) = (u-1)/n$
   $L(3928) = 3927/77 = 51$
4. $\mu = L(u)^{-1} \bmod n$
   $\mu = 51^{-1} \bmod 77 = 74$
5. Compute the plain text message $m \equiv L(c^{\lambda(n)} \bmod n^2) * \mu \bmod n$
   $M \equiv L(4624^{30} \bmod 5929) * 74 \bmod 77 \equiv 42 \bmod 77 \equiv 42$ (plain text message)

The paillier cryptosystem have following properties:

1. The result of multiplication of two encrypted is equivalent to the addition of original of plaintext mod n.
2. The result of full encryption of the second message (r^n is left out) is multiply with the first encrypted message is equivalent to the addition of original of plaintext mod n.
3. A constant power on the ciphertext gives the result in the term of constant multiple of the original plaintext.

To solve Privacy issues, Paillier cryptosystem's are used to ensure homomorphic encryption in databases [35]. Pallier cryptosystems are mainly depending upon modular arithmetic operations and integer arithmetic operations such as multiplication and exponentiation modulo n^2 for the encryption and decryption. Details of module sizes of Pallier Cryptosystem are as follows (Table 1):

Table 1 Fundamental sizes of Pallier cryptosystem

Pallier operations	Modulo size n	Modulo size n^2	# of ModMult with n^2	# of words [d] for n^2
Encryption/Decryption	512	1024	516/514	32
Encryption/Decryption	1024	2048	1028/1026	64
Encryption/Decryption	2048	4096	2052/2050	128

3 Proposed Authentication Protocol

In this section an authentication protocol based on Paillier Cryptosystem has been proposed.

3.1 System Network Model

This is a system network model of an electronic health care system which is mainly monitoring vital parameters of critically ill patient. The doctors are monitoring this parameter remotely with the help of their smart phones. Considering this scenario, many body sensor nodes has been installed in the patient body for measuring different vital parameters like heart rate, pulse, pressure, temperature and oxygen saturation etc. All sensor nodes are sending captured data to the gateway node. The gateway node will send data to local processing centre (Base Station) through the network coordinator which is called User Device. The user device is issued by the health care system while initial phase. All the captured data is gathered in the health cloud through this device and the doctors, nurses are observing data from the cloud server. The main focus is only on the secure transmission of data from the body sensor to the health cloud server. Figure 1 shows the architecture of the network.

3.2 Notations Used in this Protocol

Consider two large prime p and q over ($\mathbb{F}_p$).

N	The product of two prime p and q
G	The semi-random, nonzero integer in $\boldsymbol{Z}_{\mathbf{n}}^2$
H(.)	Hash function which is a one way function
$E_k(.)$	Asymmetric encryption function which uses key K
$D_k(.)$	Asymmetric decryption function which uses key K
T_1, T_2	Present Timestamp of node

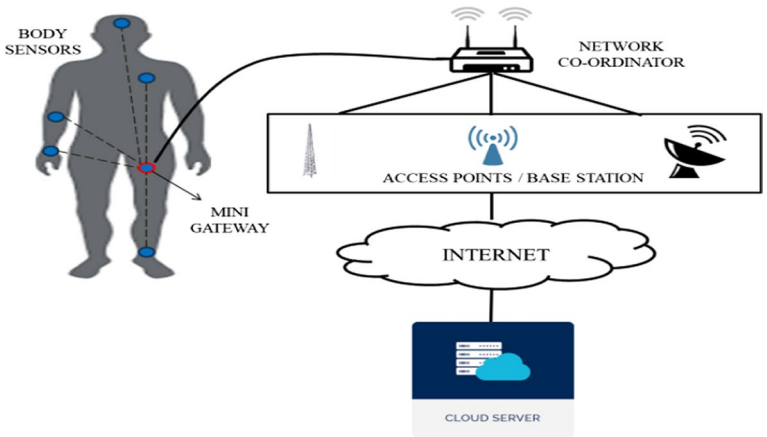

Fig. 1 System model of BSN

ΔT	Expected transmission delay
T_s	Session Duration Time
$\oplus$	Logic exclusive OR (XOR) operation
$\|$	A bitwise concatenation operation
UID	Identity of User Device
SID	Health Server ID
PID	Patient ID
P	Secret No
n_u, P_u	Private and Public key of User Device respectively
n_s, P_s	Private and Public key of Health Server respectively

Assumptions

Consider many body sensor node has been installed in a human body for measuring different body parameters. All nodes are sending captured data to the gateway node. The gateway node will send data to local processing center (Base Station) through the network coordinator which is called User Device. After deployment of the sensor nodes, following assumptions are made

- After valid registration of the user device, it will forward capture data of sensor node.
- User Device is considered as trusted one.
- Clock of the nodes in human body are synchronized with the user device.
- Each sensor data is accumulated to a main gateway which is also a sensor.
- After Registration BS will send user details to Health Server.
- Health Server will create each patients table for storing his/her data.
- BS is playing the role of trusted third party.
- Signal intensity is within a given fixed range with high transmission power.

3.3 Phases of Authentication Protocol

The proposed scheme shown in Fig. 2 is divided into three phases as described below:

A. User Registration phase:

First the patients biometric input B will capture and pass through a fuzzy extractor which could produce a random string σ. The Fuzzy extractor will operate two functions (*Gen & Rep*) which will produce random string for identification. The random string will be same for close change of input. Actually the *Gen()* will output a random string σ and a random auxiliary string ν in enrolment phase. *Rep()* is computed while identification process after receiving biometric input B^* and the corresponding auxiliary string ν to recover σ.

(i) During registration phase, a temporal key is generated from the hash of biometric profile. The device first capture patients biometric impression B_i and computes $(\sigma_i,\nu_i) = Gen(B_i)$. The temporal key is $h(PW \| \sigma_i)$ where PW is the user password.

Now user device will send a request which contain user identity (UID) and the temporal key (η) to base station (Local Processing Centre).

The request message $R_u = UID \| h(PW \| \sigma_i)$

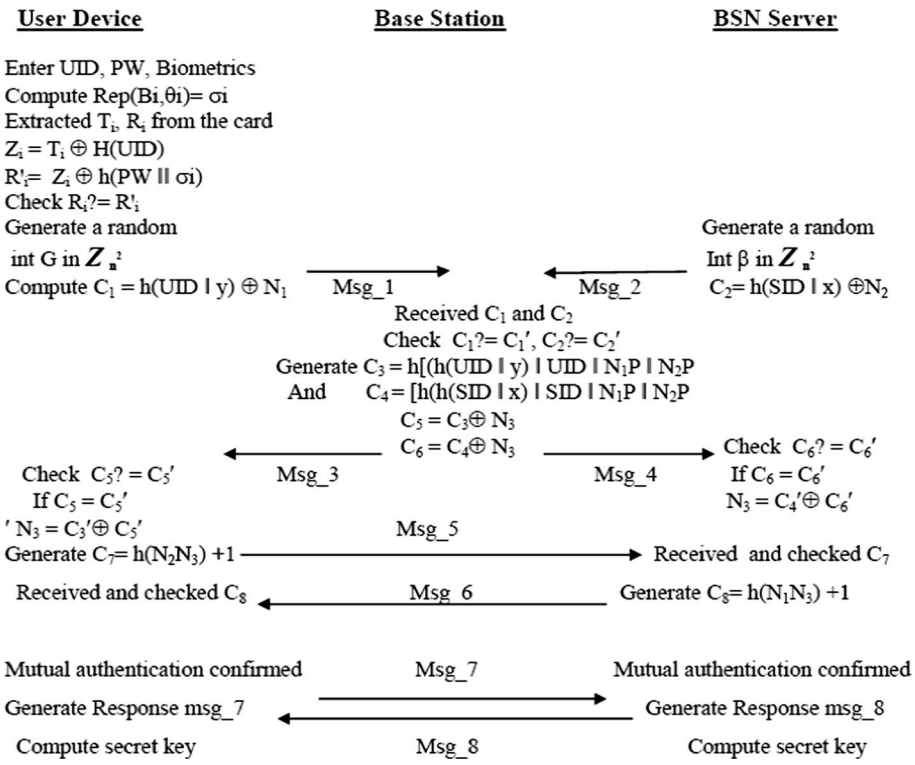

Fig. 2 Proposed authentication scheme

At the same time BSN cloud server send a registration request $R_s \| SID$ where $R_s = h(SID \| x)$. Here x is the server secret.

(ii) After R_u and R_s local processing center will compute the following parameters

$$R_i = h(UID \| y)$$

$$Z_i = R_i \oplus h(PW_i \| \sigma_i)$$

$$T_i = Z_i \oplus h(UID)$$

T_i and R_i is stored in the Smart card and the card is issued for that user device which will collect patient data to the local processing center.

(iii) Now the base station also sends a list of registered users to cloud health server which is responsible to collect and store data of the patients. In this way the base station completes the registration phase for secure data collection. The message flow is shown in Table 2. BS will send an updated list of records to cloud server including UID and PID (Patient ID) with regular interval.

B. Login phase:

During this phase, user will perform following steps as shown in Table 3:

Table 2 Flow of registration phase

Steps	Flow	Message	Description
1.	UN → BS	Sub_id()	UID ‖ h(PW ‖ σ_i)
2.	HS → BS	Reg_no()	h(SID‖ x)
3.	BS → HS	Nod_list()	UID ‖ PID ‖P
4.	BS → UN	Con_no()	UID ‖ P ‖ R_s

Table 3 Flow of Login phase

Steps	Flow	Message	Description
1.	UN → BS	Msg_1	UID‖ C_1‖ PU_A‖ N_1P
2.	HS → BS	Msg_2	SID ‖ C_2 ‖ PU_S‖ N_2P
3.	BS → UN	Msg_3	Enc(C_3 ‖ C_5 ‖ N_2P)
4.	BS → HS	Msg_4	Enc(C_4 ‖ C_6 ‖ N_1P)

Step 1 The user device first submits its biometric impression B_i^* and UID with password (PW). The device will compute $Gen\,(B_i^*, \nu_i) = \sigma_i$ and extracted the value T_i from the card to compute $Z_i' = T_i \oplus h(UID)$.

Now the device computes $R_i' = Z_i' \oplus h\,(PW_i||\sigma_i)$ and matches with extracted value of R_i.

Step 2 The user device will generate the public key $PU_A = (N,G)$ using Pailliar cryptosystem. Now it sends a message to local processing center (BS) which contains a token $C_1 = h(UID||x) \oplus N_1$ and the public key with user ID for authentication.

Hence $Msg\_1 = UID\|C_1\|PU_A\|N_1P$

Similarly Health server will send a message $Msg\_2 = SID\|C_2\|PU_S\|N_2P$

Step 3 BS will verify $C_1? = C_1', C_2? = C_2'$. After verification BS will generate

Two tokens for user device and health server. The tokens are

$$C_3 = h\left[h(UID||y)\right]||UID||N_1P||N_2P \text{ and } C_5 = C_3 \oplus N_3$$

$$C_4 = h[h(SID||x)]||SID||N_1P||N_2P \text{ and } C_6 = C_4 \oplus N_3$$

BS will generate two encrypted Msg using Pailliar cryptosystem for user device and server.

$$Msg\_3 = Enc\,(C_3||C_5||N_2P)$$

$$Msg\_4 = Enc\,(C_4||C_6||N_1P)$$

Step 4 User Device first checks $C_5? = C_5'$. If it is equal than extract N_3 by $C_3 \oplus C_5$.

Now generate another token $C_7 = h(N_2N_3) + 1$ for acknowledgement.

Similarly Server first checks $C_6? = C_6'$. If it is equal than extract N_3 by $C_4 \oplus C_6$.

Now generate another token $C_8 = h(N_1N_3) + 1$ for acknowledgement.

C. Mutual authentication phase:

In this phase the user device and BSN server will perform mutual authentication by using following steps:

Step 4 In this step User Device generate a message Msg_5 = Enc [UID || C_7|| T_1] and send to BSN server.

After receiving of Msg_5, server decrypts it and get the session time. If $T - T_1 \leq \Delta T$ where T is the present timestamp of server, then it accepts the message otherwise rejects. Now BSN servers get the UID value and compute

$$C_7' = h(N_2N_3) + 1 \text{ . If } C_7' = C_7, \text{ then it computes Msg\_6} = \text{Enc}[\text{SID}||C_8||T_2]$$

Step 2 In this step, User received Msg_6 from BSN server. After decryption it first checks the timestamp with present timestamp. If it is valid, then it computes $C_8' = h(N_1N_3) + 1$.

If $C_8' = C_8$, then it generates the response message Msg_7 as a proof of mutual authentication and shared secret key generation.

$$\text{Msg\_7} = h(C_7)||\text{UID and the shared secret key } K = h(\text{UID}||y) \oplus h(\text{SID}||x) \oplus h(N_3).$$

Step 3 After receiving Msg_7, server confirmed that the user is valid user and generate the shared secret key K = h(UID|| y) ⊕ h(SID|| x) ⊕ h(N_3). Server sends the confirmation message Msg_8 = h(C_8)|| SID. The message flow is shown in Table 4. After that all messages will be sending using symmetric encryption.

4 Detail Security Analysis

In this section analysis of the proposed authentication scheme on the basis of different attacks and also formal proof using BAN logic is performed.

4.1 Probable Attack Analysis

This sub section includes detail discussion of following attacks:

4.1.1 Password Guessing Attack

Considering a case, an attacker gets the smart card and he has tried to login the system. First he need to give the biometric impression of the patient as the device is registered for that patient. The smart card also carries the specific biometric parameter of that patient. If he is able to do that, then also he has to submit the password for authentication. Moreover

Table 4 Flow of mutual authentication phase

Steps	Flow	Message	Description
1.	UN → CS	Msg_5	Enc [UID || C_7|| T_1]
2.	CS → UN	Msg_6	Enc [SID || C_8|| T_2]
3.	UN → CS	Msg_7	h(C_7)|| UID
4.	CS → UN	Msg_8	h(C_8)|| SID

it is not possible to guess biometrics and password correctly at the same time. Hence online password guessing attack could not be successful.

The off-line password guessing attack also will not work as h(PW || σ_i) is used to calculate R_u and the two parameters

$$Z_i = R_i \oplus h(PW_i||\sigma_i) \text{ where } R_i = h(UID||y),\ T_i = Z_i \oplus h(UID)$$

At a time both are required and limited attempts will be given. Hence this protocol will resist dictionary attack.

4.1.2 Replay Attack

To prevent replay attack, nonce value is inserted in each message. Also the freshness of the message is always be calculated after receiving each message. For example Msg_1 = UID|| C_1|| PU_A|| N_1P contains random nonce for preventing replay attack.

Similarly Health server message Msg_2 = SID || C_2 || PU_S|| N_2P also carrying random nonce for preventing replay attack.

In mutual authentication phase, User Device generate a message Msg_5 = Enc [UID || C_7|| T_1] and send to BSN server. After receiving of Msg_5, server decrypts it and get the session time. If $T–T_1 \leq \Delta T$ where T is the present timestamp of server, then it accepts the message. This is also for prevention of replay attack.

4.1.3 Impersonation Attack

Impersonation attack happened when an attacker pretend as a valid user. The probability of this attack is very less as biometric impression is captured and inserted in the smart card. To prevent impersonation, mutual authentication phase is also there. In this phase the BSN server authenticates itself to the user so that any fake server cannot able to establish a connection.

4.1.4 Insertion/Message Modification Attack

In this authentication protocol after login message all messages are in encrypted form. After mutual authentication, a shared session key is generated to encrypt the data which the sensors are sending to BSN server. For example,

$$Msg\_3 = Enc\ (C_3||C_5||N_2P)$$

$$Msg\_4 = Enc\ (C_4||C_6||N_1P)$$

$$Msg\_5 = Enc\ [UID||C_7||T_1]$$

$$Msg\_6 = Enc\ [UID||C_8||T_2]$$

Now after mutual authentication the shared secret key is used for data transmission. For insertion attack, an attacker must have to decrypt the messages and for decryption he needs the shared key. If any insider knows the UID and SID, then also he has to know N_3. No single message carrying N_3 which can be tracked by an attacker. Hence this attack cannot be possible.

4.1.5 Man-in-Middle Attack

In this attack, the attacker manages to set a key between the user and the server so that he will be able to hear all the transmitted messages. For that intension, he wants to set a common key between user device and BSN server. Now to replace the value of attacker replace the value of C_7, C_8 by C_7', C_8', the attacker first have to decrypt the Msg_5 and Msg_6. It is impossible. If he replaces these messages with another encrypted messages, then also a successful session key will not established.

Thus this attack is not possible with this scheme.

4.1.6 Server Spoofing Attack

There is no verification table stored in the server so that it can authenticate any user device. All user devices are authenticated by the Base Station and after authentication this device will communicate with the server. Suppose the intended server block the BSN server and capture the message $Msg\_4 = Enc(C_4 \parallel C_6 \parallel N_1P)$ which is coming from the user device. The attacker must decrypt the message to get C_4 and C_6 which carries N_3. Again to authenticate itself, the fake server also needs to know the value of x as the authentication needs h(SID||x). Therefore, Server Spoofing attack cannot be successful.

4.1.7 Perfect Forward Secrecy

This property shows that even if the secrets x, y of the past session is disclosed, then also the attacker cannot able to calculate the past session key. The shared secret key $K = h(UID \parallel y) \oplus h(SID \parallel x) \oplus h(N_3)$. To calculate the past session key, the attacker must know the past nonce value of N_3. Hence the scheme is preserving perfect forward secrecy.

4.1.8 Message Disclosure

This threat is triggered when some sensitive private data may be disclosed to those who are not supposed to get the information. During communication, one of the sensitive information is login details. In this scheme, password $h(PW \parallel \sigma_i)$ is used to calculate R_u and the two parameters $Z_i = R_i \oplus h(PWi \parallel \sigma_i)$where $R_i = h(UID\|y)$, $T_i = Z_i \oplus h(UID)$. From this message it is very difficult to gain the knowledge of password which is sensitive information.

Other sensitive information such as patient vital parameters data is always sent and restored in an encrypted form so that unauthorized person cannot get the data. Only those who have the shared secret key and access right, can access the original data. Paillier cryptosystem is used to maintain the privacy of the data. Hence message disclosure threat cannot be successful in the proposed scheme.

4.1.9 Node Tempering Attack

In this proposed scheme, the sensor nodes are implanted inside the body. Suppose the user device which is transferring the data to the base station is compromised and the attacker gets all stored information such as UID, PW. From that, T_i, R_i is generated and stored in the Smart card and the card is issued for that user device.

During login, the user device first submits user's biometric impression B_i^* and UID with password (PW). The device will compute $Gen\ (B_i^*, \nu_i) = \sigma_i$ and extracted the value T_i from the card to compute $Z_i' = T_i \oplus h(UID)$. Now the device computes $R_i' = Z_i' \oplus h(PW_i || \sigma_i)$ and matches with extracted value of R_i.

If the device is tampered, then also with valid smart card any adversary cannot able to send data using that device.

4.1.10 Jamming Attack

It is one of the possible attacks in sensor network. To avoid this attack, high transmission power on jammed channels has been considered as mentioned in protocol assumptions.

4.2 Authentication Proof Based on BAN Logic

The authentication protocol can be proved by using BAN logic [14] which is defined as a set of logical rules to analyze any protocol. Here goal has been set and on the basis of six defined rule. For verification, this work first starts with its normal definition:

Let us consider R and S are principals, I and J are statements, K is the encryption key.

Now the standard relationships and its uses are shown in Table 5 below

Table 5 Symbol representation

$R\| \equiv I$	R believes I
$\#(I)$	I is fresh as no one has sent it before
$R \rightarrow I$	R controls I
$R\Delta I$	R receives message with I which he can read
$R\| \sim I$	R sent a message containing I sometime
(I, J)	I or J is one part of the formula (I, J).
$\langle I \rangle J$	The formula I combines with a secret parameter J
$\{I\}_K$	The formula I is encrypted with the key Key
$(I)_h$	The formula I is hashed
RKS	R and S use the shared key Key to communicate
SK	The session key used in the current session
$\frac{R\|\equiv RKS, R\triangleleft\{I\}_k}{R\|\equiv SI}$	Message meaning rule(if R believes that Key is shared with S, if R receives a message encrypted with key, then R trust on S)
$\frac{R\|\equiv\#(I)}{R\|\equiv\#(I,J)}$	Freshness conjugation rule (if I is fresh then message (I, J) is also a fresh)
$\frac{R\|\equiv S\|\equiv(I,J)}{R\|\equiv S\|\equiv(I)}$	The belief rule (If the principal R believes I and J, then the principal S believes (I, J)
$\frac{R\|\equiv\#(I), R\|\equiv S\|\sim I}{R\|\equiv S\|\equiv I}$	The nonce-verification rule (If the principal R believes that I is fresh and the principal S sent I once then the principal R believes that S believes I)
$\frac{R\|\equiv S\|\rightarrow I, R\|\equiv S\|\equiv I}{R\|\equiv I}$	The jurisdiction rule (If the principal R believes that S has jurisdiction right to I and S believes I, then R believes that I is true)

For correctness measurement, the key agreement protocol must achieve the following goals:

Goal 1: $U_n| \equiv U_n \overset{SK}{\leftrightarrow} S_n$

Goal 2: $U_n| \equiv S_n| \equiv U_n \overset{SK}{\leftrightarrow} S_n$

Goal 3: $S_n| \equiv U_n \overset{SK}{\leftrightarrow} S_n$

Goal 4: $S_n| \equiv U_n| \equiv U_n \overset{SK}{\leftrightarrow} S_n$

Now transforming the proposed scheme to the idealized form is as follows:

1. Message 1: $U_n \rightarrow$ BS: $(UID, I)_{\text{h(UID}\|\text{k)}}$
2. Message 2: $S_n \rightarrow$ BS: $(UID, I, SID, J)_{\text{h(SID}\|\text{k)}}$
3. Message 3: BS $\rightarrow U_n$: $(UID, SID, I, J, U_n \overset{J}{\leftrightarrow} S_n)_{\text{h(UID}\|\text{ k)}}$
4. Message 4: BS $\rightarrow S_n$: $(UID, SID, I, J, U_n \overset{I}{\leftrightarrow} S_n)_{\text{h(SID}\|\text{ k)}}$
5. Message 5: $S_n \rightarrow U_n$: $(UID, SID, I, J, U_n \overset{SK}{\leftrightarrow} S_n)_{SK}$
6. Message 6: $U_n \rightarrow S_n$: $(UID, SID, I, J, U_n \overset{SK}{\leftrightarrow} S_n)_{SK}$

Verifying this protocol using BAN logic requires some assumption. They are as follows

- A_1: $U_n| \equiv \#(I)$
- A_2: $S_n| \equiv \#(J)$
- A_3: $U_n| \equiv U_n \overset{\text{h(UID}\|\text{k)}}{\leftrightarrow} BS$
- A_4: $BS| \equiv U_n \overset{\text{h(UID}\|\text{k)}}{\leftrightarrow} BS$
- A_5: $S_n| \equiv S_n \overset{\text{h(SID}\|\text{k)}}{\leftrightarrow} BS$
- A_6: $BS| \equiv S_n \overset{\text{h(SID}\|\text{k)}}{\leftrightarrow} BS$
- A_7: $U_n| \equiv \text{BS} \Rightarrow U_n \overset{J}{\leftrightarrow} S_n$
- A_8: $S_n| \equiv \text{BS} \Rightarrow U_n \overset{I}{\leftrightarrow} S_n$
- A_9: $S_n| \equiv U_n \Rightarrow U_n \overset{SK}{\leftrightarrow} S_n$
- A_{10}: $U_n| \equiv S_n \Rightarrow U_n \overset{SK}{\leftrightarrow} S_n$

Now with the help of BAN logic rules and assumptions, the proof of the proposed scheme will be performed.

From Msg 1, it will get that

S_1: $BS \triangleleft (UID, I)_{\text{h(UID} \| \text{ K)}}$

Using assumption A_4 and message meaning rule, it will get that

S_2: $BS| \equiv U_n(UID, I)$

From Msg 2, it will get that

S_3: $BS \triangleleft (UID, SID, I, J)_{\text{h(SID} \| \text{ K)}}$

Using assumption A_6 and message meaning rule, it will get that

S_4: $BS| \equiv S_n(UID, I, SID, J)$

From Msg 3, it will get that

S_5: $U_n \triangleleft (UID, SID, I, J, U_n \overset{J}{\leftrightarrow} S_n)_{\text{h(UID}\|\text{ k)}}$

Using assumption A_4 and message meaning rule, it will get that

S_6: $U_n| \equiv BS(UID, SID, I, J, U_n \overset{J}{\leftrightarrow} S_n)$

Using assumption A_3 and freshness conjugation rule, it will get that

S_7: $U_n| \equiv BS \equiv (UID, SID, I, J, U_n \overset{J}{\leftrightarrow} S_n)$

Now break the conjunctions to produce

S_8: $U_n| \equiv BS \equiv (U_n \overset{J}{\leftrightarrow} S_n)$

According to assumption A_7, apply the jurisdiction rule to obtain

S_9: $U_n| \equiv U_n \overset{J}{\leftrightarrow} S_n$

Now session key *SK* is a secret parameter could obtain

S_{10}: $U_n| \equiv U_n \overset{sk}{\leftrightarrow} S_n$ (**Goal 1 is achieved)**

According to Msg 5, it will get that

S_{17}: $U_n \lhd (UID,\ SID,\ I,\ J,\ U_n \overset{SK}{\leftrightarrow} S_n)_{\ SK}$

Using assumption S_{10} and message meaning rule

S_{18}: $U_n| \equiv S_n(UID, SID, I, J, U_n \overset{sk}{\leftrightarrow} S_n)$

According to assumption A_1, apply the freshness conjunction rule to obtain

S_{19}: $U_n| \equiv S_n \equiv (UID, SID, I, J, U_n \overset{sk}{\leftrightarrow} S_n)$

According to S_{19} and BAN logic rule to break conjunction to produce

S_{20}: $U_n| \equiv S_n \equiv (U_n \overset{sk}{\leftrightarrow} S_n)$ (**Goal 2 is achieved)**

From Msg 4, it will get that

S_{11}: $S_n \lhd (UID,\ SID,\ I,\ J,\ U_n \overset{I}{\leftrightarrow} S_n)_{\ h(SID\|\ k)}$

Using assumption A_6 and message meaning rule

S_{12}: $S_n| \equiv BS \sim (UID, SID, I, J, U_n \overset{I}{\leftrightarrow} S_n)$

According to assumption A_2, apply the freshness conjunction rule to obtain

S_{13}: $S_n| \equiv BS \sim (UID, SID, I, J, U_n \overset{I}{\leftrightarrow} S_n)$

Now applying BAN logic rule to break conjunction rule, it will get that

S_{14}: $U_n| \equiv BS \equiv (U_n \overset{I}{\leftrightarrow} S_n)$

Using assumption A_6 and jurisdiction rule, it will get that

S_{15}: $S_n| \equiv (U_n \overset{I}{\leftrightarrow} S_n)$

Now session key *SK* is a secret parameter could obtain

S_{16}: $S_n| \equiv (U_n \overset{sk}{\leftrightarrow} S_n)$ (**Goal 3 is achieved)**

According to Msg 6, it will get that

Table 6 Throughput measurement during encryption and decryption

Operations using Paillier system	Throughput (k bits/s)		
	n = 512	n = 1024	n = 2048
Encryption	98	28	8.2
Decryption	198	58	14.8

Table 7 Performance comparison of different algorithms

Authentication Scheme	Registration phase	Login phase	Authentication phase	Total
This Scheme	4 T_H	4T_H	4T_H	12 T_H
Dhillon and Kalra [30]	8 T_H	6 T_H	8 T_H	22 T_H
Xue et al. [31]	7 T_H	6 T_H	13 T_H	26 T_H
Turkanovi et al. [32]	7 T_H	5 T_H	7 T_H	19 T_H

Table 8 Functionality comparison of the scheme with existing protocols

Functionalities	Dhillon and Kalra [30]	Xue et al. [31]	Turkanovi et al. [32]	This scheme
Man-in-the-middle attack	Yes	No	Yes	Yes
Impersonation attack	Yes	No	No	Yes
Mutual authentication	Yes	Yes	Yes	Yes
Replay attack	Yes	Yes	Yes	Yes
Perfect forward secrecy	No	No	No	Yes
Insertion attack	No	No	No	Yes
Server spoofing attack	No	No	Yes	Yes
Password guessing attack	No	No	Yes	Yes

S_{21}: $S_n \lhd (UID, SID, I, J, U_n \overset{sk}{\leftrightarrow} S_n)$ SK

Using S_{19} and applying message meaning rule to produce

S_{22}: $S_n| \equiv U_n(UID, SID, I, J, U_n \overset{sk}{\leftrightarrow} S_n)$

According to assumption A_2 and freshness conjunction rule

S_{23}: $S_n| \equiv U_n \equiv (UID, SID, I, J, U_n \overset{sk}{\leftrightarrow} S_n)$

According to S_{23} to break conjunctions to produce

S_{24}: $S_n| \equiv U_n \equiv (U_n \overset{sk}{\leftrightarrow} S_n)$ **(Goal 4 is achieved)**

From Goal 1, Goal 2, Goal 3, and Goal 4 it shows that the session key shared by the user and BSN server is only known to them only.

5 Performance Analysis

Performance analysis of the proposed scheme has been done in following two parts:

A. The performance of the proposed protocol is measured in terms of computation cost (total time required for performing complex operation such as hashing) and communication cost (total no of bits transmitted). Also the throughput is measured for different modulus size shown below in Table 6.

The communication cost is mainly calculated for considering message transmission. Assuming that the identity (UID, SID) are 10 bytes long and the random nonce (N_1, N_2), secure one-way hash function are 160 bit long, the total no. of bits exchanged between user

Table 9 Remote data transfer delay for equal sample size

Data sample	Parameter range	Data arrival time (s)	Sample size (byte)	Data rate (kbs)	Delay (s)
ECG	2.5–3.0 mV.	0.003	2	0.50	1.031
Blood pressure	20–300 mm HG	0.02	2	1.2	1.135
Blood flow	1–300 ml/s	0.002	2	0.52	1.028

and base station is 940 bits (for transmitting msg 1, msg 3). Total no. of bits exchanged between base station and BSN server is 940 bits (for transmitting msg 2, msg 4). For mutual authentication total no. of bits exchanged is 976 bits (for transmitting msg 5, msg 6, msg 7, msg 8). Performance comparison is shown in Table 7 where T_H is the time required to perform one hashing.

Now the proposed scheme is compared with other existing algorithms in Table 8. Functionality Comparison shows that the scheme is favorably comparable with existing protocols.

B. To evaluate the performance of overall proposed system model, a database is considered from the hospital server which is mainly used for remote patient monitoring. The data samples are collected from different body sensors and aggregated in the hospital server into large packets to improve the transmission efficiency. The simulation scenario is considered that patient data (suppose ECG Signal, blood pressure and blood flow) is transmitted through the network coordinator to the remote computer (Doctor's laptop). OPNET simulator is used for this purpose. The total end to end delay is summarized in Table 9 given bellow:

The Table 9 shows that it is possible to transfer patient data within a reasonable delay for remote monitoring purpose or any emergency cases.

6 Conclusion

In this paper, a strong efficient authentication protocol for Wireless Body Sensor Networks is being proposed which can be applied in healthcare applications. It resist all possible attacks in distributed networks. The scheme provides mutual authentication between target server and user and also generate different session key for different server. The proposed scheme is based on Paillier cryptosystem which have homomorphic and self-binding property. For privacy preservation this type of system is very useful. The experiment results show that this scheme has low computational load and communicational load.

References

1. Samaneh, M., Mehran, A., Justin, L., David, S., & Abbas, J. (2014). Wireless body area networks: a survey. *IEEE Communications Surveys & Tutorials, 16*(3), 1658–1686.

2. Zimmerman, T. G. (1996). Personal area networks: Near-field intra body communication. *IBM Systems Journal, 35*(3/4), 609–617.
3. Shi, L., Li, M., Yu, S., & Yuan, J. (2012). "BANA: Body area network authentication exploiting channel characteristics. In *Proceedings of 5th ACM Conference Security. Privacy Wireless Mobile Network*, Tucson, AZ, USA: ACM, pp. 1–12.
4. Cai, L., Zeng, K., Chen, H., & Mohapatra, P. (2011). "Good neighbor: Ad hoc pairing of nearby wireless devices by multiple antennas. In *Proceedings of Network Distributed System Security Symposium*, pp. 1–15.
5. Shi, L., Yuan, J., Yu, S., & Li, M. (2013). "ASK-BAN: Authenticated secret key extraction utilizing channel characteristics for body area networks. In *Proceedings* of the *6th ACM Conference* on *Security* and *Privacy* in *Wireless* and *Mobile Networks*, pp. 155–166.
6. Shi, L., Li, M., Yu, S., & Yuan, J. (2013). BANA: Body area network authentication exploiting channel characteristics. *IEEE Journal on Selected Areas in Communications, 31*(9), 1803–1816.
7. Varshavsky, A., Scannell, A., LaMarca, A., & DeLara, E. (2007). "Amigo: Proximity-based authentication of mobile devices. In *Proceedings of 9th International Conference* on *Ubiq computing* (pp. 253–270). Berlin, Germany: Springer.
8. Kalamandeen, A., Scannell, A., DeLara, E., Sheth, A., & LaMarca, A. (2010). Ensemble: Cooperative proximity-based authentication. In *Proceedings of the 8th International Conference on Mobile Systems, Applications, and Services* (pp. 331–344). New York, NY, USA: ACM.
9. Mathur, S., Miller, R., Varshavsky, A., Trappe, W., & Mandayam, N. (2011). Proximate: Proximity-based secure pairing using ambient wireless signals. In *Proceedings of the 9th International Conference on Mobile Systems, Applications, and Services* (pp. 211–224).
10. Poon, C., Zhang, Y., & Bao, S. (2006). A novel biometrics method to secure wireless body area sensor networks for telemedicine and mhealth. *IEEE Communications Magazine, 44*(4), 73–81.
11. Singh, K., Muthukkumarasamy, V. (2007). "Authenticated key establishment protocols for a home health care system. In *Proceedings of 3rd International Conference on Intelligent Sensors, Sensor Networks and Information (ISSNIP'07)* (pp. 353–358).
12. Venkatasubramanian, K., & Gupta, S. (2010). Physiological value based efficient usable security solutions for body sensor networks. *ACM Transactions on Sensor Network, 6,* 31:1–31:36.
13. ElGamal, T. (1985). A public key cryptosystem and a signature protocol based on discrete logarithms. *IEEE Transactions on Information Theory, 31*(4), 469–472.
14. Rivest, R., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public key cryptosystems. *Communications of the ACM, 21*(2), 120–126.
15. Li, M., Yu, S., Lou, W., & Ren, K. (2010). Group device pairing based secure sensor association and key management for body area networks. In *Proceedings of IEEE INFOCOM* (pp. 1–9).
16. He, Debiao, Zeadally, Sherali, Kumar, Neeraj, & Lee, Jong-Hyouk. (2017). Anonymous authentication for wireless body area networks with provable security. *IEEE Systems Journal, 11*(4), 2590–2601.
17. Venkatasubramanian, K., Banerjee, A., & Gupta, S. (2010). Pska: Usable and secure key agreement scheme for body area networks. *IEEE Transactions on Information Technology in Biomedicine, 14*(1), 60–68.
18. Abi-char, P. E., Mhamed, A., & El Hassan, B "A secure authenticated key agreement protocol based on elliptic curve cryptography. In *International Symposium on Information Assurance and Security, IEEE* (vol. 57, pp. 89–94).
19. Bringer, J., Hervé, C., & Thomas I (2010) "Password based key exchange protocols on elliptic curves which conceal the public parameters. In *ACNS 2010, Lecture Notes in Computer Science* (vol. 6123/2010, pp. 291–308).
20. Chatterjee, K., De, A., & Gupta, D. (2015). A secure and efficient authentication protocol in wireless sensor network. *Wireless Personal Communications, 81*(1), 17–37.
21. Chatterjee, K., De, A., & Gupta, D. (2011). "Timestamp based authentication protocol for smart card using ECC. In *Proceedings of International Conference on Web Information System and Mining (WISM 2011),LNCS 2008* (vol. 6987, pp. 368–375).
22. Lim, M.-H., Yeoh, C.-M., Lee, S., Lim, H. & Lee, H. (2008). A secure and efficient three-pass authenticated key agreement protocol based on elliptic curves. In *Networking, LNCS 2008* (vol. 4982/2008, pp. 170–182).
23. Shamir, A. (1984). "Identity based cryptosystems and signature schemes. In *Proceedings of Advanced cryptology (CRYPTO'84)* (pp. 47–53). Berlin, Germany: Springer.
24. Yang, J., & Chang, C. (2009). An ID-based remote mutual authentication with keyagreement scheme for mobile devices on elliptic curve cryptosystem. *Computer Secuity, 28*(3–4), 138–143.

25. Yoon, E., & Yoo, K. (2009). "Robust ID-based remote mutual authentication with key agreement protocol for mobile devices on ECC. In *Proceedings of International Conference* on *Computer Science and Engineering*, Vancouver, Canada (pp. 633–640).
26. He, D., Chen, J., & Hu, J. (2012). An ID-based client authentication with key agreement protocol for mobile client-server environment on ECC with provable security. *Information Fusion, 13*(3), 223–230.
27. Wang, D., & Ma, C. (2013). Cryptanalysis of a remote user authentication scheme for mobile client-server environment with provable security based on ECC. *Information Fusion, 41*(4), 498–503.
28. Islam, S., & Biswas, G. (2011). A more efficient and secure ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem. *Journal of Systems and Software, 84*(11), 1892–1898.
29. Truong, T., Tran, M., & Duong, A. (2012). "Improvement of the more efficient and secure ID-based remote mutual authentication with key agreement scheme for mobile devices on ECC. In *Proceedings of the 26th International Conference Advanced Information Networking Application Workshops* (pp. 698–703).
30. Dhillon, P. K., & Kalra, S. (2017). A lightweight biometrics based remote user authentication scheme for IoT services. *Journal of Information Security and Applications, 34,* 255–270.
31. Xue, K., et al. (2013). A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks. *Journal of Network and Computer Applications, 36*(1), 316–323.
32. Turkanović, Muhamed, Brumen, Boštjan, & Hölbl, Marko. (2014). A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion. *Ad Hoc Networks, 20,* 96–112.
33. Al-Janabi, S., et al. (2017). Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. *Egyptian Informatics Journal, 18*(2), 113–122.
34. O'Keeffe, M. (2008). The paillier cryptosystem. *Mathematics Department April, 18,* 1–16.
35. San, I., et al. (2016). Efficient paillier cryptoprocessor for privacy- preserving data mining. *Security and Communication Networks, 9*(11), 1535–1546.

Kakali Chatterjee is working as Assistant Professor in Computer Science and Engineering Department of National Institute of Technology Patna, India. She has completed her Ph.D. from Delhi University (formerly Delhi College of Engineering). She has involved in information security project of Govt. of India. She has many published research papers in LNCS (*Springer*) and reputed International Journals of eminent publishers like Springer and Elsevier. She is working in the field of Information Security and Cryptography for last 12 years.