IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 1, 2020, accepted March 25, 2020, date of publication April 2, 2020, date of current version April 20, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2985261

Mutual Authentication in Body Area Networks Using Signal Propagation Characteristics

MUBARAK UMAR[1,2,3], ZHENQIANG WU[1,2], AND XUENING LIAO[1,2]

[1]School of Computer Science, Shaanxi Normal University, Xi'an 710062, China
[2]Key Laboratory of Modern Teaching Technology, Ministry of Education, Xi'an 710062, China
[3]Department of Computer Science, Bayero University, Kano, Kano 3011, Nigeria

Corresponding author: Xuening Liao (liaoxuening@sina.cn)

This work was supported in part by the China Fundamental Research Funds for the Central Universities under Grant GK201903087, and in part by the China Postdoctoral Science Foundation under Grant 2019M663618.

ABSTRACT Developments in wireless communications and wearable devices have facilitated the emergence of a network of tiny sensors embedded in, on or around human body called Wireless Body Area Network (WBAN). Over the last decade, WBAN has increasingly been playing a vital role in modern medical systems because of its potential to revolutionize healthcare delivery. The data collected by the sensors contain sensitive information and are transmitted via wireless channels. However, the openness of these channels makes WBAN vulnerable to attacks by unauthorized users. Therefore, secure authentication and data encryption schemes in WBAN are essential. The resource constraint nature of the sensors makes traditional cryptographic schemes unsuitable. Consequently, authentication schemes based on channel characteristics are proposed, which are more suitable with fewer requirements. However, existing approaches do not consider mutual authentication as well as passive/active attacks. Motivated by these limitations, we propose in this paper, a mutual authentication and data encryption scheme based on signal propagation characteristics and enhanced butterfly algorithm. To validate the effectiveness of our scheme, we conducted an extensive real-world experiment involving 5 volunteers in indoor and outdoor areas, under distinct scenarios. We further conducted security and performance analyses to validate the effectiveness of our scheme in terms of resources and its resilience to various attacks. The results of the experiments and the analyses show that our scheme could mutually identify legitimate users and protect user data against active/passive eavesdropping attacks with minimal overhead.

INDEX TERMS Authentication, active attack, passive attack, signal propagation characteristic, wireless body area network (WBAN).

I. INTRODUCTION

Wireless body area network (WBAN) consists of small sensors embedded within, on or around a human body, tasked with the remote monitoring of the wearer's physiological data such as an electrocardiogram (ECG), and blood pressure (BP) [1], [2]. WBAN has recently been evolving as an essential framework for the realization of advanced medical care. However, due to the open nature of wireless channels, the data transmitted in WBAN are vulnerable to be accessed and falsified by unauthorized users. As these data are the basis of clinical diagnoses, any leakage of the data may put the lives of patients at risk [3]. Therefore, it is essential to provide secure and reliable authentication schemes in WBAN to guarantee that only legitimate users have access to the patients' confidential information.

Research works on authentication in WBAN can be categorized into cryptographic and non-cryptographic techniques. Cryptographic based schemes rely on pre-shared keys, encryption, and decryption algorithms to provide authentication in WBAN [1], [2], [4]. The main strength of these mechanisms is that attackers have limited computational capabilities; thus, it is computationally challenging for them to decrypt the encryption algorithms without the secret keys. However, the devices in WBAN do not have enough resources to afford the high computations in these schemes. Moreover, if a node is compromised, the pre-shared keys can be stolen by the attackers. Non-cryptographic methods, which use either physiological feature [15]–[19], or channel characteristics [23]–[28], have recently attracted much attention because

The associate editor coordinating the review of this manuscript and approving it for publication was Amjad Mehmood.

of their simple requirements, less computation, and absence of pre-shared secrets. These schemes have been recognized as a complementary approach for authentication in WBAN. However, it is hard for two sensors to generate exact features with the same accuracy in physiological feature based schemes, while some channel based schemes require advanced hardware [26] or extreme learning phase [23], [25].

In the existing cryptographic authentication techniques in WBAN, the commonly used methods are symmetric and asymmetric encryption, both of which rely on a secret key. In [5]–[7], bilinear pairing based authentication schemes are proposed to guarantee secure communication in WBAN. In [3], He *et al.* proposed a bilinear and hash function based authentication scheme. However, the security analysis of their scheme shows that it suffers from weak anonymity. Moreover, the devices in WBAN cannot afford the complex bilinear operations in these schemes. To avoid bilinear pairing operations, several authentication schemes [8]–[11] based on elliptic curve cryptography (ECC) have been proposed. In [12], Wazid *et al.* proposed an ECC based authentication scheme, where a trusted third party generates identities for network devices that are used in key generation. In [13], Khernane *et al.* proposed an authentication scheme based on a zero knowledge proof technique. With the zero knowledge proof, sensors prove to each other having a secret without revealing it in the process. Unfortunately, Bu and Potop-Butucaru [14] pointed out that [13] could not resist data replay, redundancy information, and denial-of-service (DoS) attacks. To fix the weaknesses in [13], the authors in [14] proposed random key for each session and hop-by-hop authentication.

Non-cryptographic methods of authentication in WBAN are either based on physiological features [15]–[19] or channel characteristics [23]. On physiological feature based schemes, an ECG feature and a three-party password were used in [20] for intra-WBAN and inter-WBAN authentication, respectively. 128 bits were generated from the interpulse interval (IPI) of an ECG in [21] to encrypt and decrypt a fuzzy vault containing a session key. Biokeys were generated by two on-body sensors from IPI of an ECG feature in [22] to establish trust. An off-body controller authenticates the sensors if the generated keys are similar. Unfortunately, the scheme is susceptible to impersonation attack. Although these methods do not rely on pre-shared secrets, the requirement that each sensor measures a specific physiological value brings additional cost to WBAN. Moreover, the schemes are susceptible to DoS attack as it is hard for two sensors to generate exact features with the same accuracy. Channel characteristic based schemes have been proven to be very promising to provide lightweight authentication for WBAN. In [23], the biometric behaviors of patients in four scenarios, which are used for authentication in WBAN, were generated by using the propagation characteristics of the wireless channel. In [24], Shi *et al.* proposed a one-way authentication scheme for WBAN by adopting K-means clustering to distinguish between a received signal strength (RSS) traces of legitimate devices and attackers. In [25], Mohamed and Cheffena used RSS values as a source of gait recognition to obtain time series, auto-correlation, and crossing rate level features, which are applied to distinguish one person from another. In [26], an accelerometer data is used to provide one-way authentication for WBAN. However, continuous sampling of the accelerometer data consumes battery power of the devices in WBAN. In [27], Wang *et al.* developed an on-body detection framework named SecureTag by exploiting creeping wave propagation to secure on-body devices. However, their scheme is concerned with user identification, and does not provide mutual authentication.

We can demonstrate from above that, although both cryptographic-based and non-cryptographic-based schemes can achieve authentication in WBAN, non-cryptographic techniques, especially channel characteristic based methods, are more suitable due to their simple requirements and less computation overhead. However, there are still some limitations. Most available works on the channel characteristic based authentication schemes only considered one-way authentication and impersonation attack. In other words, mutual authentication and possible passive and active eavesdropping attacks have not been explored yet. As mutual authentication in WBAN ensures that two communicating devices are legitimate before data transmission, its absence may lead to an impersonation attack. In addition, passive and active eavesdropping attacks, when not prevented, may lead to unauthorized access and tempering of the patient's information. Motivated by these shortcomings, we consider in this paper, a WBAN with an attacker capable of launching both passive and active attacks, and investigate a hybrid mutual authentication scheme based on channel characteristics and lightweight symmetric encryption. The contributions of the paper are summarized as follows.

1) We first propose a mutual authentication scheme by exploiting signal propagation variations between on-body and off-body channels to distinguish between legitimate and attacker devices. Different from other schemes, we use RSS traces to provide mutual trust instead of constructing a propagation pattern that consumes memory and requires learning training.
2) To prevent the network from passive and active eavesdropping attacks, a butterfly update algorithm is then proposed to generate random numbers representing the signal propagation variations, which are then encrypted symmetrically and exchanged between the devices.
3) Finally, we conducted extensive experiments to validate the effectiveness of our scheme by inviting 5 volunteers under different scenarios in indoor and outdoor environments. The results indicated that our proposed scheme can provide robust mutual authentication and resource-efficient data encryption.

The rest of the paper is organized as follows. Section II describes the system models and preliminaries. Section III presents the proposed mutual authentication scheme. Security and performance analyses of our scheme are provided in

Section IV. Section V contains the evaluation of the scheme in real environments and discussion of the results. Section VI concludes our work.

II. SYSTEM MODELS AND PRELIMINARIES

A. NETWORK MODEL AND ASSUMPTIONS

As shown in Fig. 1, we consider a network that is made up of n strategically positioned sensor nodes (SNs), and a central controller node called sink. Moreover, we consider the presence of an off-body attacker in the network that sends authentication requests to the sink in order to gain access to the network. As a common assumption in WBAN [2], all the SNs have equal but limited resources such as memory, energy, and computational abilities. Due to the limited resources of the SNs and thus their limited transmission range, they are not within the transmission range of an off-body device responsible for relaying the sensed data to a medical server as commonly depicted in the WBAN's architecture [1]. Therefore, the sink, which is a smartphone in our network and assumed to have more resources than the SNs, is placed at the center of the body to collate the sensed data and relay them to the off-body device. Moreover, since these devices are located on the same body, they are assumed to be within each other's transmission range, and therefore can communicate directly in a single hop manner through bluetooth over wireless channels. The devices in our network transmit data in a half-duplex mode and are positioned on the body at a distance of some centimeters away from each other to ensure non-interfering wireless channels. Due to the human body presence, the propagation of the signal between the SNs and the sink is dominated by a direct path component of the signal [24], whereas the propagation of the signal between the sink and the attacker is influenced by the multipath components of the signal caused by signal reflecting objects and the free environment between them.

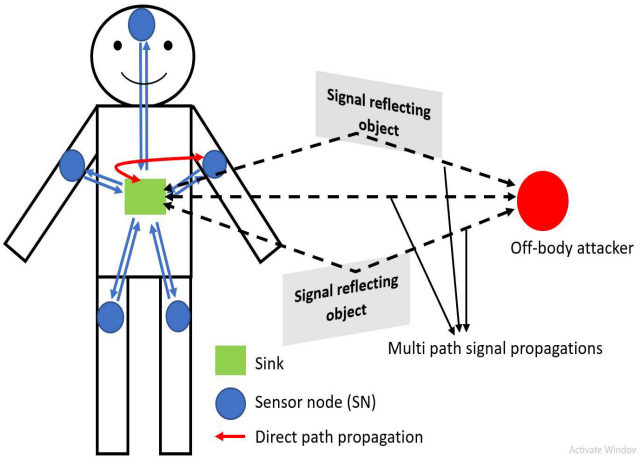


FIGURE 1. Network model.

B. ATTACK MODEL

For the attack model, we consider in this paper, an **impersonation** and **eavesdropping (both passive and active)** attacks. An impersonation attack is when the attacker device attempts to pretend to be a legitimate device to join the network, thereby enabling it to launch further attacks. The attacker is able to fabricate physical addresses and forge authentication credentials of legitimate devices in order to launch the impersonation attack. When the attacker successfully launched the impersonation attack, we assumed that it can be able to further initiate **data replay**, and **man-in-the-middle** attacks. A data replay attack is when the attacker device attempts to maliciously repeats or delays a valid data transmission, while in the man-in-the-middle attack, the attacker device attempts to secretly relays and possibly alters the communication between two legitimate devices who believe they are communicating with each other. On the eavesdropping attacks, the attacker may intercepts exchanged encrypted messages from the communication channel, and attempts to launch passive attack by decrypting the messages to view their contents, or active attack by injecting false data or replacing some of the previously sent messages. Note that we assumed the attacker to be an off-body device, therefore, attacks from malicious devices placed on the patient's body are not considered. Moreover, we do not consider jamming and DoS attacks.

C. SIGNAL PROPAGATION OF ON-BODY AND OFF-BODY CHANNELS

There are significant variations in the characteristics of on-body and off-body channels [24], [27], [28], which are due to the differences in the way signal propagates on these channels. The propagation of the signal in an on-body channel mainly consists of creeping waves diffracted from the human tissues and trapped on the surface of the human skin [27]. Thus, at a very close range, a direct path is the dominant path among all the multipath components of the signal at the receiver. For an off-body channel, the relative motion between an off-body and on-body device leads to a Doppler shift [24]. Consequently, any change in the environment will result in a remarkable signal variation at the receiver side.

Therefore, it is concluded in [24] that, the variations of on-body channels come from the creeping waves and direct path components because their characteristics are highly susceptible to body motion and device antenna location, but less sensitive to environmental dynamics and the distance between sender and receiver antennas. However, these variations disappear in off-body channels, as their characteristics depend mainly on the multipath nature of the signal's propagation caused by the environment.

In our scheme, we use path loss as a signal propagation parameter to distinguish between on-body and off-body channel propagations. The path loss of a signal for WBAN, which is defined as the reduction in the signal's power density as it propagates through a medium [29], [30] is modeled in [31]–[34] as shown in (1).

$$PL_{dB}(d) = PL_{0_dB}(d_0) + 10\log_{10}\frac{d}{d_0} + S \qquad (1)$$

where $PL_{dB}(d)$ is the average path loss in decibel at a distance d, $PL_{0_{dB}}$ is the path loss at a reference distance d_0, n is the path loss exponent, d is the transmitter and receiver antennas distance, and S is the loss due to shadowing effect.

D. BINARY HYPOTHESIS TESTING

In this paper, the problem of authentication is formulated as a binary hypothesis testing to determine whether a received message by a destination is from a legitimate source or the off-body attacker. Thus, at time t, when the destination receives the message, the authentication based on the hypothesis test is given by (2) below.

$$H_0 : M(t) = M_L(t)$$
$$H_1 : M(t) = M_A(t) \quad (2)$$

where the null hypothesis H_0 represents that the source of the message (M) at time t is a legitimate device whose message is denoted by M_L, while the alternative hypothesis H_1 indicates that the source of the message at time t is the attacker, whose message is denoted by M_A.

III. THE PROPOSED AUTHENTICATION SCHEME

In this section, we introduce the proposed mutual authentication scheme for WBANs. As illustrated in Fig. 2, the Sink and SN begin by exchanging authentication messages. Each of the devices then generates the pathloss values of the messages, which are then exchanged between the devices as random numbers and used for the establishment of mutual authentication. Table 1 describes the notations used in this work.

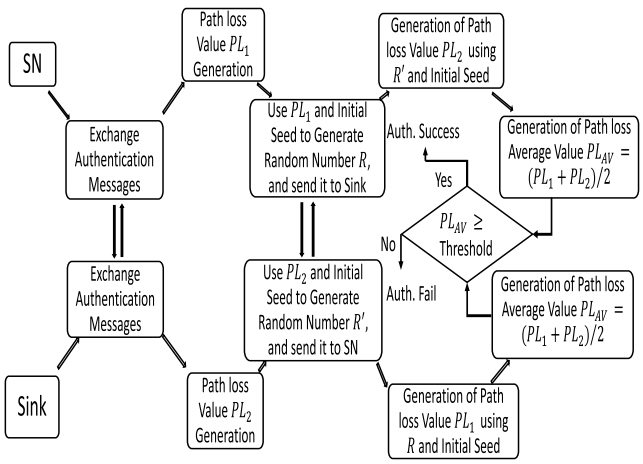


FIGURE 2. Block diagram of the authentication scheme.

Note that in our scheme, two devices mutually authenticate each other in each session before data are exchanged between them. Thus, our scheme is different from certificate based authentication schemes where authentication certificates are generated by a trusted central authority.

A. RANDOM NUMBER GENERATION USING ENHANCED BUTTERFLY SEED UPDATE PROCEDURE

The path loss values of the exchanged packets are estimated by the devices in our scheme by using (3) at both ends of the channel.

$$PL_{dBmW} = \left| P_{recv_{(dBmW)}} - P_{trans_{(dBmW)}} \right| \quad (3)$$

where P_{dBmW} is the path loss in decibel milliwatts at a destination after a packet has arrived, $P_{recv_{(dBmW)}}$ is the received power at the destination in decibel milliwatts, and $P_{trans_{(dBmW)}}$ is the transmitted power in decibel milliwatts at the source.

To ensure mutual authentication, these values are passed from one end of the channel to the other and vice versa. However, they can not be sent out in a plain text as there is a passive or active attacker monitoring the channel. Therefore, we send out a random number that represents the values instead. Thus, even if the attacker intercepts this arbitrary number, it cannot gain any useful information from it. To achieve that, we adopted a butterfly update algorithm proposed in [35] with a slight modification to suit our proposal. In their scheme, an initial random number called seed is agreed upon by the two devices. A randomly generated number in each session is then used to update the seed by inverting the bit that is in a position of the random number value.

The strength of the scheme in [35] lies in its lightness and the fact that, inverting a single bit in a number results in another different number. To explain how this is used in our scheme, the initial seed denoted by $S_{initial}$ of the seed update procedure is agreed upon at the initialization stage of our scheme; then, at each session, a path loss value is used as a random number to update the initial seed through the enhanced butterfly seed update procedure. Note that, we assume at the initialization stage, the knowledge of the initial seed is only known to the legitimate devices. To introduce much randomness, we invert the bits in the initial seed beginning from the least significant bit (LSB) down to the bit represented by the path loss value of that particular session. The inversion procedure in our scheme is summarized

TABLE 1. Symbols used and their descriptions.

Symbols	Descriptions
ID_{SN}	Identity of a sensor node
$nonce_{SN}$	A randomly generated nonce by a sensor node
ARq	Authentication request
PL	Path loss value
$S_{initial}$	Initial seed of a seed update procedure
$\delta(a, b)$	A seed update function which takes an initial seed a, and a pointer b to the end of the bits inversion
R	A random number generated as an output to the seed update procedure
Key	Session key
L	A generated random number representing a session key Key
ARp	Authentication reply
Ack	Acknowledgment
K_1	Initial key
$E(K[a])$	A symmetric encryption function that encrypts a with a key K using exclusive-OR operation
PL_{AV}	Average of path loss values
ID_S	Identity of a sink
$nonce_S$	A randomly generated nonce by a sink
σ	A threshold for a hypothesis test

in Algorithm 1. The output of this procedure is always a random number R that is related to a specific session.

Algorithm 1 Enhanced Butterfly Seed Update Procedure

Input: Initial seed ($S_{initial}$), path loss (PL), start point of inversion (s_p)
Output: A random Number R
Initialization: I, $LIMIT$, $LEN = 0$, Integer Array $[0 \ldots 255]VAL$, r, q, $s_p = 0$

```
while S_initial > 0 do
    Convert S_initial to a binary number
    while S_initial > 0 do
        r ← (S_initial) mod 2
        q ← ((S_initial) − r) / 2
        VAL[LEN] ← r
        Update S_initial
        S_initial ← q
        Increment the value of LEN by 1
        LEN ← LEN + 1
    end while
    if LEN < 255 then
        for LEN ← LEN + 1 to 255 do
            Pad 0's until the array length reaches 256
            VAL[LEN] ← 0
        end for
    end if
    Set the stopping point of the inversion
    LIMIT ← s_p + PL
    if LIMIT ≤ LEN then
        for I ← s_p to LIMIT do
            if VAL[I] = 0 then
                Assign 1 to VAL[I]
                VAL[I] ← 1
            else
                Assign 0 to VAL[I]
                VAL[I] ← 0
            end if
        end for
    end if
    R ← 0
    for I ← LEN to 0 do
        Convert from binary to decimal
        R ← R + VAL[I] × (2^I)
    end for
    return R
end while
```

B. AUTHENTICATION PROTOCOL

For two devices, SN and the Sink that wish to exchange data in our scheme, they execute the five steps as shown in Fig. 3. The authentication session is initiated by SN as follows.

1) A sensor node SN sends an authentication request message $M = E(K_1[(ID_{SN}, nonce_{SN}, ARq)])$ to the sink encrypted with K_1 which is made up of its ID_{SN}, $nonce_{SN}$ to ensure message freshness and authentication request identifier ARq.

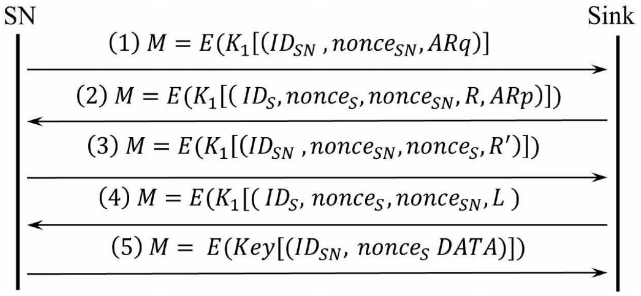


FIGURE 3. Authentication steps of our proposed scheme.

2) When the sink receives the message, it decrypts it using K_1 and stores $nonce_{SN}$. It then generates a path loss value $PL_1 = |P_{recv} - P_{trans}|$ and uses the result to computes $R = \delta(S_{initial}, PL_1)$ through our enhanced seed update procedure. The sink then sends back a message $M = E(K_1[(ID_S, nonce_S, nonce_{SN}, R, ARp)])$ to SN encrypted with K_1. The message contains the sink's ID_S and its $nonce_S$, $nonce_{SN}$, authentication reply ARp and the generated R.
3) When the SN receives the reply from the sink, it decrypts the message, obtains $nonce_{SN}$ and compares it with the one it sent at step 1. If the two nonces are the same, it stores $nonce_S$. It then generates $PL_1 = \delta(S_{initial}, R)$ and $PL_2 = |P_{recv} - P_{trans}|$. It computes the average of the two values, $PL_{AV} = (PL_1 + PL_2)/2$ and checks whether $PL_{AV} \geq \sigma$. If true, the SN generates $R' = \delta(S_{initial}, PL_2)$ and sends back a message $M = E(K_1[(ID_{SN}, nonce_{SN}, nonce_S, R')])$ encrypted with K_1 to the sink. The message is made up of ID_{SN}, $nonce_{SN}$, $nonce_S$, and R'. Otherwise, it drops the authentication request.
4) Upon receiving the reply, the sink decrypts the message, gets $nonce_S$ and compares it with the nonce it sent at step 2. If the two nonces are similar, the sink stores $nonce_{SN}$ and uses R' to generates $PL_2 = \delta(S_{initial}, R')$. It then computes the average of the two values, $PL_{AV} = (PL_1 + PL_2)/2$ and checks whether $PL_{AV} \geq \sigma$. If true, the sink generates 128 bits key to be used for this session's data encryption. It then uses the PL_{AV} and the generated key Key to compute a random number $L = Key^{PL_{AV}}$ that will be sent instead of the plain text session key. A message $M = E(K_1[(ID_S, nonce_S, nonce_{SN}, L)])$ encrypted with K_1 which contains ID_S, $nonce_S$, $nonce_{SN}$ and L is then sent back to the sensor. Otherwise, the authentication request is dropped and the session closed.
5) Upon receiving a reply from the sink, the SN decrypts it, gets $nonce_{SN}$ and compares it with the nonce it sent at step 3. If the two nonces are the same, the sensor stores $nonce_S$ and extracts the key from L using $Key = \sqrt[PL_{AV}]{L}$. It then uses the key, encrypt the whole message $E(Key[(ID_{SN}, nonce_S, Data)])$ and sends it to the sink.

Otherwise, it drops the authentication message and closes the session.

In our proposed scheme, a destination generates a path loss whenever it receives message from another device. It should be noted that, the messages exchanged between the source and the destination devices at steps 2 and 3 of our scheme have locally estimated path loss values in them, which are hidden within a random number generated through the enhanced seed update procedure. Therefore, it is expected at any of the steps 2 or 3 that the destination has two path loss values denoted by PL_1 and PL_2. The destination then generates the average of these two values as shown in (4).

$$PL_{AV} = (PL_1 + PL_2)/2 \tag{4}$$

where PL_{AV} stands for the average of the two path loss values.

The detection accuracy of our scheme depends on the test threshold denoted by σ, which was determined through preliminary experiments we conducted. We noticed that the average of the path loss values is always higher when both of the devices are on the body, and lower when one or both of the devices are not on the body. Thus, we define in (5), the threshold for the hypothesis test.

$$\sigma = (\alpha + \beta)/2 \tag{5}$$

where α represents the lower bound of the sink's path loss values, and β represents the upper bound of the SN's path loss values. If the generated average of the path loss values by the receiver is greater than or equals to the σ, it accepts the null hypothesis H_0. Otherwise, the receiver accepts H_1. Thus, the hypothesis test applied by the destination is given by (6).

$$T = PL_{AV} \underset{H_1}{\overset{H_0}{\gtrless}} \sigma \tag{6}$$

The false rejection rate, which is denoted by P_{fr} is defined in (7) as the probability that a message from a legitimate device is viewed as a message from the attacker, i.e.,

$$P_{fr} = P_r(H_1|H_0) \tag{7}$$

where $P_r(.|.)$ is the conditional probability. Similarly, false acceptance rate denoted by P_{fa} is the probability that a packet from the attacker passes the authentication, which is given by (8).

$$P_{fa} = P_r(H_0|H_1) \tag{8}$$

By using (7) and (8), the probability for the receiver to accept legitimate packet is given by $P_r(H_0|H_0) = 1 - P_{fr}$, and the probability to reject a fake message by the receiver is $P_r(H_1|H_1) = 1 - P_{fa}$.

IV. SECURITY AND PERFORMANCE ANALYSIS

In this section, we present the security and performance analyses of our proposed scheme.

A. SECURITY ANALYSIS

In what follows, we perform a formal security analysis of our scheme using the formalization in [14]. Let us define a sensor node (SN) which holds a known information Y as

$$I_{SN} = \{Y\}$$

Let the operation of sending a message containing X from SN to sink S at i^{th} authentication step be.

$$SN : (SN, X, S)_i, \quad i \in \{1, 2, 3, 4, 5\}$$

Let the checking operation by a legitimate device S to verify if a received message from SN is valid or not, be donated by

$$Validating_S((SN, X, S)_i)$$

If the message $(SN, X, S)_i$ fail to be correctly decrypted or X is not a correct reply to the previously sent challenge, the validation operation fails, then the received message is dropped, and the authentication is rejected. Otherwise, the validation succeeds, and the next authentication step is executed.

An attacker node Z is assumed to be a smart device that is located some meters away from the legitimate devices and can perform the following operations:

1) It can intercept a message from SN to S and vice versa.
2) It can initiate authentication by sending $Z : (Z, X, S)$ where X can be anything belonging to its known information I_Z.
3) It may not perform Validating$_Z((SN, X, S)_i)$ for any S and SN.
4) It can update I_Z using guessed data and previous communication history.
5) It can attempt to decrypt encrypted messages by using information from I_Z at any time.

1) IMPERSONATION ATTACK

Proposition 1: Our scheme is resistant to Impersonation Attack.

Proof: An adversary Z can attempt to impersonate SN to authenticate with S. The initial information of Z and S respectively are.

$$I_Z = \{ID_Z, nonce_Z, K_{1_Z}, Arq\}$$
$$I_S = \{ID_S, S_{initial}, K_1, Arp\}$$

The following operations shown below demonstrate how our scheme can detect impersonation attack.

1) $Z : (Z, X, S)_1$
2) Validating$_S((Z, X, S)_1)$
3) Validation Failed: $K_1 \neq K_{1_Z}$, with high probability.

Since Z has no access to K_1, the attempt to decrypt the message by S will fail because $K_{1_Z} \neq K_1$. Additionally, the use of K_1 to encrypt the messages in all the steps prevents the attacker from getting access to the generated random numbers R and R'.

2) DATA REPLAY ATTACK

Proposition 2: Our scheme is resistant to Data Replay Attack.

Proof: Assume Z intercepts a message exchanged between SN and S at say time $t1$, delay and re-transmit it in the hope that it can get the session key or the data. Assuming the attacker somehow got the identities of the SN and S, its initial information after intercepting the message at step 4 is.

$$I_Z = \{ID_Z, ID_S, ID_{SN}, L_{(t1)} = K_{S_{(t1)}}{}^{PL_{AV_{(t1)}}}\}$$

The following operations below proves how our scheme is resistant to data replay attack.

1) S : $(S, E(K_1[(ID_S, nonce_{S_{(t1)}}, nonce_{SN_{(t1)}}, L_{(t1)})]), SN)_4$
2) Z intercepts $(S, E(K_1[(ID_S, nonce_{S_{(t1)}} nonce_{SN_{(t1)}}, L_{(t1)})]), SN)_4$
3) Z replays $(S, E(K_1[(ID_S, nonce_{S_{(t1)}}, nonce_{SN_{(t1)}}, L_{(t1)})]), SN)_4$
4) Validating $_{SN}((S, E(K_1[(ID_S, nonce_{S_{(t1)}}, nonce_{SN_{(t1)}}, L_{(t1)})]), SN)_4)$
5) Validation Failed: $nonce_{SN_{(t1)}}$ is not fresh with high probability

At this stage, the $nonce_{SN_{(t1)}}$ will be different from the current nonce generated by SN at time $t2$. Remember that nonces are generated to ensure the freshness of the data and prevent its replay. Hence our scheme is resilient against data replay attack.

3) MAN-IN-THE-MIDDLE ATTACK

Proposition 3: Our scheme is resistant to Man-in-the -Middle Attack.

Proof: The attacker Z can intercept messages exchanged between SN and S and try to guess the secret $S_{initial}$ that the SN and S hold or have access to the exchanged session key Key. The initial information of Z is.

$$I_Z = (ID_Z, ID_{SN_Z}, ID_{S_Z}, R_Z, K_{1_Z}, Arp', nonce_{S_Z}, nonce_{SN_Z})$$

From the following operations shown below, Z cannot get the $S_{initial}$ or the session key Key.

1) Z intercepts $(S, E(K_1[(ID_S, nonce_S, nonce_{SN}, R, Arp)]), SN)_2$
2) Z replaces ID_S, $nonce_S$, $nonce_{SN}$, R, and Arp with ID_{S_Z}, $nonce_{S_Z}$, $nonce_{SN_Z}$, R_Z, and Arp', respectively. Z then forwards $(S, E(K_{1_Z}[(ID_{S_Z}, nonce_{S_Z}, nonce_{SN_Z}, R_Z, Arp')]), SN)_2$
3) Validating$_{SN}((S, (ID_{S_Z}, nonce_{S_Z}, nonce_{SN_Z}, R_Z, Arp'), SN)_2)$
4) Validation Failed: $K_1 \neq K_{1_Z}$, with high probability.

Since Z did not use the correct original key K_1, an attempt to decrypt the message by SN will fail, because $K_1 \neq K_{1_Z}$. Moreover, Z can not generate the session key Key because none of R_Z or R'_Z can be used to generate the PL_1 and PL_2 values without the knowledge of the initial seed $S_{initial}$ and the initial key K_1. Therefore, our scheme is resistant to man-in-the-middle attack.

4) PASSIVE AND ACTIVE EAVESDROPPING ATTACKS

Proposition 4: Our scheme is resistant to Passive and Active eavesdropping Attacks.

Proof: An attacker Z can obtain all the encrypted transmitted information from the common channel. However, without the knowledge of the initial key K_1, the attacker will not get any useful information from the encrypted messages. Hence, the attacker cannot lunch active and passive attacks on the data.

5) STOLEN VERIFIER ATTACK

Proposition 5: Our scheme is secure against Stolen Verifier Attack.

Proof: In the proposed scheme, no verifier table is maintained by either the sink or the SN. They each make use of their locally stored K_1, $S_{initial}$, and their separately generated session specific path loss values for authentication. Therefore, our scheme is secure against stolen verifier attack.

6) MUTUAL AUTHENTICATION

Proposition 6: Our scheme provides Mutual Authentication.

Proof: According to the principle of channel reciprocity [36], [37], we know that only legitimate SN and the sink can be able to generate correlated channel parameters. Then, the SN and the sink can confirm the validity of each other because the average of the path loss values generated independently from their end of the channel is always greater than or equals to the threshold. i.e., $PL_{AV} \geq \sigma$. Therefore, our scheme provides mutual authentication.

B. PERFORMANCE ANALYSIS

In this subsection, we first give a detailed analysis of our scheme's performance in terms of resources, and then compare its performance with some related works.

1) STORAGE COST

Due to the stringent nature of the sensors' resources, storage cost is a vital parameter for evaluating the performance of an authentication scheme in WBAN [3]. In our scheme, each node stores an initial key K_1, and an initial seed $S_{initial}$. Therefore, a device's storage overhead is $128 + 256 = 384$ bits. The storage cost comparisons of our scheme with other related schemes are listed in Table 3. According to the Table 3, our scheme has less storage overhead than the other related works.

2) COMMUNICATION COST

A total of 5 messages are exchanged in our scheme for authentication and data transmission. In step 1, the SN sends a tuple $(ID_{SN}, nonce_{SN}, ARq)$ to the sink, and the tuple has $48 + 64 + 24 = 136$ bits. In step 2, the sink sends back $(ID_S, nonce_S, nonce_{SN}, R, ARp)$ to the SN, and it has 456 bits. In step 3, the SN sends tuple $(ID_{SN}, nonce_{SN}, nonce_S, R')$ to the sink which has $48 + 64 + 64 + 256 = 432$ bits. In step 4, the sink sends back the tuple $(ID_S, nonce_S, nonce_{SN}, L)$ to the

SN and it has 432 bits. In step 5, the SN sends (ID_{SN}, $nonce_S$) to the sink which is made up of 112 bits. In total, the communication cost in our scheme is 136 + 456 + 432 + 432 + 112 = 1568 bits. The communication cost in our scheme and other related schemes are compared in Table 3. From the Table 3, our scheme has lighter communication cost than both of He *et al.* [3] and Wei *et al.* [7] schemes. However, our scheme has a slightly heavier communication cost than the scheme of Chaudhry *et al.* [10].

3) COMPUTATION COST

Here, we present the analysis of the computation cost of our proposed scheme. The running time in milliseconds (ms) of the operations used in the scheme are listed in Table 2. For convenience, some notations used here are explained below.

1) T_{xor}: The running time of exclusive-OR operation
2) T_{su}: The running time of seed update operation
3) T_{keyGen}: The running time of key generation operation
4) T_{PLGen}: The running time of path loss value generation
5) T_{PLAV}: The running time of generating a path loss average value
6) T_{exp}: The running time of exponential operation

TABLE 2. Running time of the operations in our scheme.

T_{xor}	T_{su}	T_{keyGen}	T_{PLGen}	T_{PLAV}	T_{exp}
2 ms	4 ms	2 ms	0.011 ms	0.045 ms	1000 ms

In the authentication scheme, between the sink and *SN*, a total of 35 *XOR* operations, 4 seed update operations, 1 key generation operation, 2 path loss generation operations, 2 operations of path loss average generation and 2 exponential operations were performed. Therefore, the total computation cost in our scheme is 2×35 ms $+ 4 \times 4$ ms $+ 2 \times 1$ ms $+ 0.011 \times 2$ ms $+ 0.045 \times 2$ ms $+ 1000 \times 2$ ms $= 2088.112$ ms ≈ 2.09 s. Table 3 shows the computation cost comparison of our scheme among other related schemes. According to the Table 3, our proposed scheme has lower computation cost than both of the other schemes. The lesser computation cost in our scheme is attributed to the use of operations that are less complex than the bilinear operations in He *et al.*'s [3] scheme or the ECC operations in Wei *et al.* [7] and Chaudhry *et al.* [10] schemes.

TABLE 3. Storage cost, computation cost, and communication cost comparisons with other related schemes.

Schemes	Storage costs (bits)	Computation cost (s)	Communication cost (bits)
Proposed scheme	384	2.09	1568
He *et al.* [3]	1088	10.69	3360
Wei *et al.* [7]	544	8.92	4224
Chaudhry *et al.* [10]	480	13.42	1184

4) AUTHENTICATION TIME

In our scheme, the first three rounds of messages are required to be exchanged before mutual authentication is reached or denied. We observed during the experiments that it takes 8 ms, 13 ms, and 10 ms for the first, second, and third messages to reach their destinations, respectively. A total of 24 *XOR* operations, 2 path loss generation operations, 2 path loss average generation operations, and 4 seed update operations are executed before mutual authentication is reached or denied. Thus, the overall authentication time of our scheme is 0.095 s. Our scheme has a faster authentication time than the 15 s, 10 s, 12 s, and 20 s reported in [18], [20], [24], and [27], respectively.

V. EVALUATION IN REAL ENVIRONMENT

In this section, we evaluate the proposed scheme in real environments. The scheme is tested relative to these factors: environmental type, body motion states of the volunteers, and their differences in terms of age and body shape.

A. EXPERIMENTAL SETUP

1) IMPLEMENTATION AND SETUP

We conducted the experiments with 4 devices in total, 3 of which are arduino UNO R3 to emulate the on-body sensors and 1 is a TECNO android smartphone version 7. We equipped the arduinos with HM-10 Bluetooth Low Energy (BLE) chipset operating at 2.45 GHz. For simplicity, two out of the three arduino devices named $D1$ and $D2$, are placed on the body of the volunteers at different locations. $D3$ in the experiment is the smartphone that represents the sink, while $D4$ is chosen to represent the attacker. We set the transmission power of the devices to 6 *dBm*, and the receiver sensitivity of the arduino and android devices are -94 *dBm* and -86 *dBm*, respectively. Two channels from the left arm to the waist and from right thigh to the waist are considered. Fig. 4 shows the placement of the devices at different locations on the body.

We implemented the scheme as an android background service and a sketch on the smartphone and the arduino devices, respectively. The implementation of our scheme runs a background service on the smartphone and does not require any changes to the commercially off-the-shelf (COTS) devices. Our android application relies only on Bluetooth API in the COTS devices; thus, it can readily be implemented on other platforms. Fig. 5(a) and Fig. 5(b) show the developed android application and one of the arduino devices used in the experiments, respectively.

For convenience of movements, a strap is used in the experiments to fasten the smartphone at the center of the wearer's body, while $D1$ and $D2$ are strapped on the right thigh and left shoulder of the subjects, respectively

2) VOLUNTEERS

We used five people as volunteers named $VL1$, $VL2$, $VL3$, $VL4$, and $VL5$ in the experiments. $VL1$ to $VL4$ are males while $VL5$ is a female. The aim of using different volunteers is to evaluate the performance of the scheme across distinct body shapes and ages.

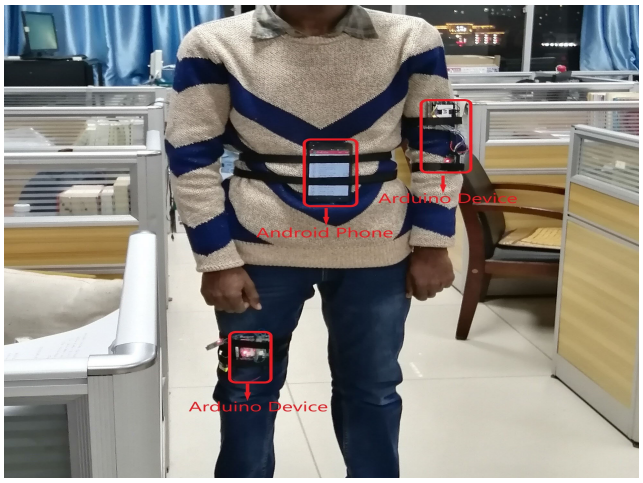
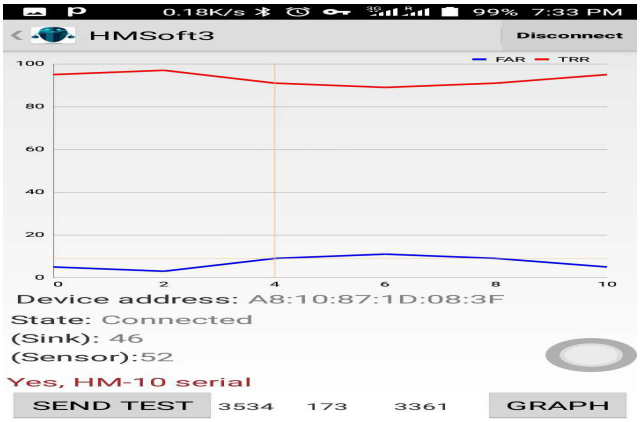
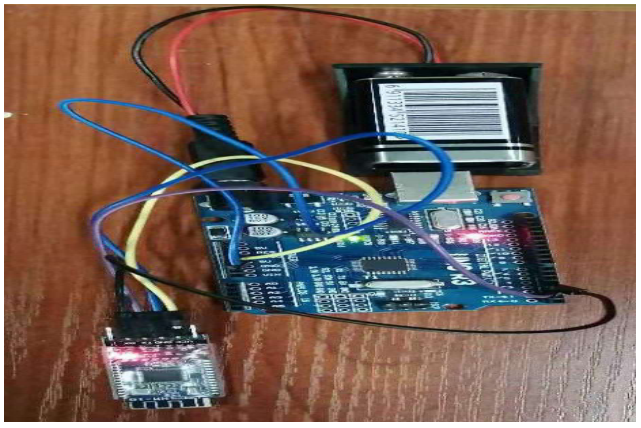


FIGURE 4. Devices placement on the body.



(a) The developed android application.



(b) One of the arduino UNO R3 devices used in our scheme.

FIGURE 5. Illustrations of the developed android application, and one of the arduino devices used to emulate the sensors.

3) PROCEDURE

The experiments conducted in a lab of 10 m × 8 m, and a corridor outside the lab lasted for 24 minutes on each volunteer. In the lab, we used 12 minutes for communication between the sink and the SNs, with the other 12 minutes used for communication between the sink and the attacker. Note that, during the experiments, the volunteers switch between sitting and standing scenarios. Similarly, we used 12 minutes in the corridor of the lab for communication between the sink and the SNs, while the other 12 minutes between the sink and the attacker, this time however, the volunteers switch between standing and walking situations. As the smartphone has more resources than the arduino devices, we used the android background services of the developed application to store the traces of RSS measurements of the exchanged packets for analysis and validation of the proposed scheme.

4) PERFORMANCE METRICS

We use true rejection rate (TRR) and false rejection rate (FRR) to evaluate the performance of our scheme. The true rejection rate is defined as the ratio of the number of attack attempts that are successfully rejected to the total number of the attack attempts. False rejection rate refers to the ratio of the number of requests from legitimate devices that are falsely rejected to the total number of sent requests by the legitimate devices. TRR and FRR are defined in (9) and (10), respectively.

$$TRR = \frac{\sum_{i \in EXP} (\text{number of attack request rejected})_i}{\sum_{i \in EXP} (\text{total number of attack request})_i} \quad (9)$$

$$FRR = \frac{\sum_{i \in EXP} (\text{number of true request rejected})_i}{\sum_{i \in EXP} (\text{total number of true request})_i} \quad (10)$$

where $i \in \{2, 4, 6, 8, 10, 12\}$ represents an interval of 2 minutes in the experiment (EXP).

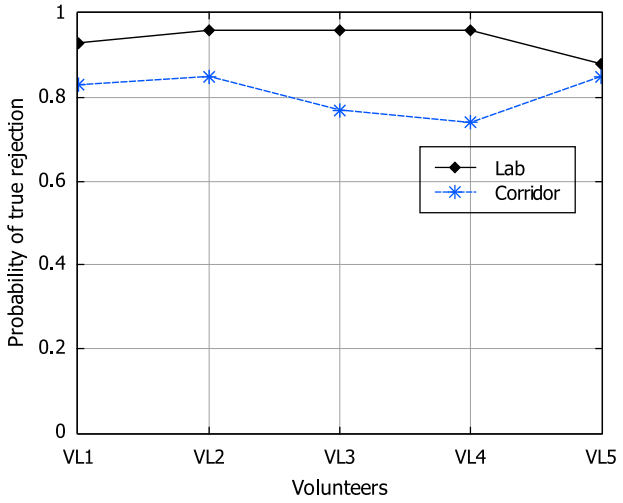
B. MODEL VALIDATION

Here, we first evaluate the effectiveness of our scheme in different environments under distinct scenarios. Next, we conduct overall performance evaluation of the scheme on different volunteers.

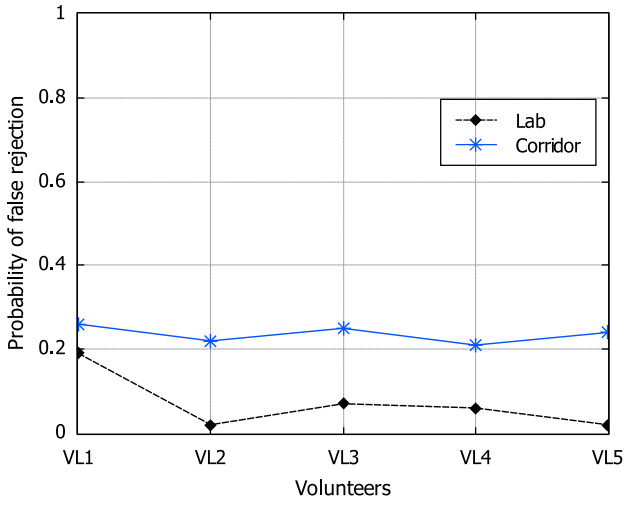
1) EVALUATION OF OUR SCHEME IN DIFFERENT ENVIRONMENTS AND SCENARIOS

In this subsection, we investigate the true and false rejection rates of our scheme in different environments. We used the lab as the indoor environment where the volunteers conducted their experiments. The indoor place is used to evaluate the performance of the scheme in the presence of signal reflecting objects, such as computers and tables. Corridor outside the lab is then used as the outdoor environment to examine the effect of an open place and passers-by on the performance of the scheme. The experiments in both of the places lasted for 4 days. We consider a network scenario of 3 devices attached on the body of the volunteers and an off-body attacker held and moved randomly within the vicinity of the volunteer's body. We ensure that the off-body attacker keeps sending authentication request messages to the sink in order to gain access to the network. To evaluate the scheme's performance relative to different actions of the volunteers, we consider

sitting and standing actions in the indoor places, and standing and walking actions in the corridors.



(a) True rejection rate.



(b) False rejection rate.

FIGURE 6. True and false rejection rates of our scheme in the lab, and the corridor under different scenarios.

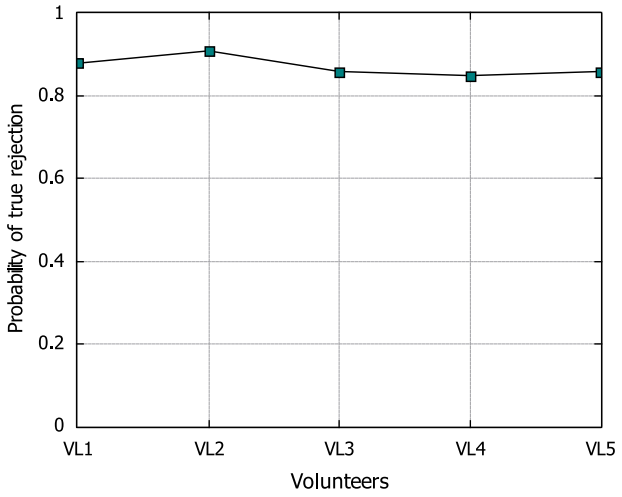
Results and Discussions: The experimental results are shown in Fig. 6. For the 4 days of the experiments, we can observe from the Fig. 6 that, the average true and false rejection rates of our scheme in the lab are 93.7% and 7.4%, respectively. In the corridor of the lab on the other hand, our scheme achieves an average true and false rejection rates of 87.7% and 23.5%, respectively. We notice that the worst performance of the scheme comes in the corridor at a 23.5% false rejection rate. This is due to the effect of the open nature of the corridor and the passers-by on the signal propagation, as well as the challenging walking scenario in the corridor. In this scenario, the relative speed of the volunteers was higher, which decreased the chances of the legitimate devices observing similar channel variations [36]. Thus, the variations of the legitimate devices were easily recognized as off-body propagation. In real cases, the chance is rare for the expected patients to walk at a speed of the healthy volunteers used in our experiments, and thus, our scheme can still achieve a low false rejection rate. The impressive performance of the scheme in the lab was due to the relative stability enjoyed by the signal as it propagates in the closed environment, under sitting and standing motion states. The results are consistent with the literature, and have further validated the effectiveness of our scheme across different environments, under distinct scenarios. Therefore, based on these experimental results, our scheme is secure against impersonation attack, thereby preventing the attacker from launching data replay and man-in-the-middle attacks. Moreover, the encryption of the data using a randomly generated session key prevents the attacker from initiating both passive and active eavesdropping attacks.

2) PERFORMANCE EVALUATION OF OUR SCHEME ON DIFFERENT VOLUNTEERS

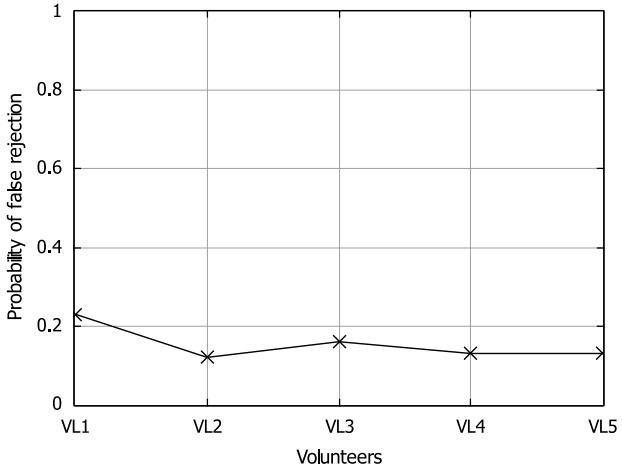
Here, we study the effectiveness of our scheme on different volunteers. We evaluate the proposed scheme in the lab, and the corridor for 4 days, with 4-hour traces in total from the 5 volunteers used. In each experiment set, we consider a network scenario of 3 devices and an off-body attacker. Each of the volunteers wears the smartphone at the center of their body, while the other two devices are attached on their left arm and right thigh. The attacker device is held by one of the subjects and moved around the body of the volunteer wearing the other three devices at any moment. The wearers perform the motions as stated in Section V, subsection V-B1.

Results and Discussions: Fig. 7 shows the experimental results of our scheme for all the volunteers. The scheme achieves the average true and false rejection rates of 87.2% and 15.5%, respectively. From the results, we can observe that, $VL4$ and $VL1$ have the lowest true rejection rate of 84.9% and the highest false rejection rate of 22.5%, respectively. This is due to the severe fading the signal suffers from the shadowing of the relatively short and thick bodies of $VL4$ and $VL1$. The results have again validate the effectiveness of the scheme across different volunteers, and indicate that our scheme is resistant to impersonation attack, and ensures the privacy of the patients' data.

Regarding the improvements observed in the scheme compared to previous methods, please note that, this the first work that proposes a hybrid mutual authentication based on signal propagation characteristics and symmetric cryptography. Thus, the goal of this paper is to investigate the performance of hybrid mutual authentication methods rather than compare our scheme with others or improve the performances of existing methods. Although there exist previous schemes on channel characteristics and symmetric cryptography separately, none of the schemes combine both the two methods of authentication to create a hybrid scheme like our work. Moreover, the existing channel characteristic based methods provide one-way authentication. Thus, comparing



(a) True rejection rate.



(b) False rejection rate.

FIGURE 7. True and false rejection rates of our scheme for different volunteers.

the existing schemes with our scheme may tell us little about which outperforms the others.

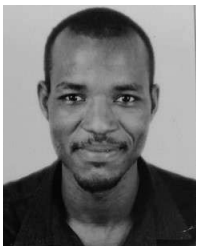
VI. CONCLUSION

In this paper, we presented a hybrid mutual authentication and data encryption scheme for body area networks based on a signal propagation characteristic and enhanced seed update algorithm. First, our technique exploits path loss variations between on-body and off-body channels to establish mutual trust before data transmission. We observed that this variations at the two ends of an on-body channel are higher than when one of the devices is not on the body. Then, we proposed an enhanced seed update algorithm to protect the exchanged data against active and passive attacks. We implemented our scheme on android phone and arduino devices, and the results of the experiments conducted on 5 volunteers have validated our observation, and shown that our scheme can effectively provide mutual authentication between on-body devices. Moreover, the security and performance analyses we conducted have indicated that our scheme is resilient to various security attacks and effective in terms of computation overhead. The simplicity in the design of our scheme makes it a suitable candidate for deployment in resource-constrained networks such as WBAN, where lightweight security solutions are required. As we considered an off-body attacker in our work, in the future, we plan to investigate authentication schemes that consider attacks from malicious devices that are placed on the user's body (on-body attackers), as well as the effect of privileged insider, and random number leakage attacks on the performance of such schemes.

REFERENCES

[1] M. Kompara and M. Hölbl, "Survey on security in intra-body area network communication," *Ad Hoc Netw.*, vol. 70, pp. 23–43, Mar. 2018.
[2] S. Zou, Y. Xu, H. Wang, Z. Li, S. Chen, and B. Hu, "A survey on secure wireless body area networks," *Secur. Commun. Netw.*, vol. 2017, pp. 1–9, May 2017.
[3] D. He, S. Zeadally, N. Kumar, and J.-H. Lee, "Anonymous authentication for wireless body area networks with provable security," *IEEE Syst. J.*, vol. 11, no. 4, pp. 2590–2601, Dec. 2017.
[4] M. Masdari and S. Ahmadzadeh, "A survey and taxonomy of the authentication schemes in Telecare medicine information systems," *J. Netw. Comput. Appl.*, vol. 87, pp. 1–19, Jun. 2017.
[5] Q. Jiang, X. Lian, C. Yang, J. Ma, Y. Tian, and Y. Yang, "A bilinear pairing based anonymous authentication scheme in wireless body area networks for mHealth," *J. Med. Syst.*, vol. 40, no. 11, pp. 1–10, Nov. 2016.
[6] L. Wu, Y. Zhang, L. Li, and J. Shen, "Efficient and anonymous authentication scheme for wireless body area networks," *J. Med. Syst.*, vol. 40, no. 6, pp. 1–12, Jun. 2016.
[7] F. Wei, P. Vijayakumar, J. Shen, R. Zhang, and L. Li, "A provably secure password-based anonymous authentication scheme for wireless body area networks," *Comput. Electr. Eng.*, vol. 65, pp. 322–331, Jan. 2018.
[8] X. Li, J. Peng, S. Kumari, F. Wu, M. Karuppiah, and K.-K. R. Choo, "An enhanced 1-round authentication protocol for wireless body area networks with user anonymity," *Comput. Electr. Eng.*, vol. 61, pp. 238–249, Jul. 2017.
[9] X. Liu, C. Jin, and F. Li, "An improved two-layer authentication scheme for wireless body area networks," *J. Med. Syst.*, vol. 42, no. 8, pp. 2–14, Aug. 2018.
[10] S. A. Chaudhry, H. Naqvi, M. Sher, M. S. Farash, and M. U. Hassan, "An improved and provably secure privacy preserving authentication protocol for SIP," *Peer-to-Peer Netw. Appl.*, vol. 10, no. 1, pp. 1–15, Jan. 2017.
[11] S. Challa, A. K. Das, V. Odelu, N. Kumar, S. Kumari, M. K. Khan, and A. V. Vasilakos, "An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks," *Comput. Electr. Eng.*, vol. 69, pp. 534–554, Jul. 2018.
[12] M. Wazid, A. K. Das, N. Kumar, M. Conti, and A. V. Vasilakos, "A novel authentication and key agreement scheme for implantable medical devices deployment," *IEEE J. Biomed. Health Informat.*, vol. 22, no. 4, pp. 1299–1309, Jul. 2018.
[13] N. Khernane, M. Potop-Butucaru, and C. Chaudet, "BANZKP: A secure authentication scheme using zero knowledge proof for WBANs," in *Proc. IEEE 13th Int. Conf. Mobile Ad Hoc Sensor Syst. (MASS)*, Oct. 2016, pp. 307–315.
[14] G. Bu and M. Potop-Butucaru, "BAN-GZKP: Optimal zero knowledge proof based scheme for wireless body area networks," *Ad Hoc Netw.*, vol. 77, pp. 28–41, Aug. 2018.
[15] D. K. Altop, B. Seymen, and A. Levi, "SKA-PS: Secure key agreement protocol using physiological signals," *Ad Hoc Netw.*, vol. 83, pp. 111–124, Feb. 2019.
[16] P. Peris-Lopez, L. González-Manzano, C. Camara, and J. M. de Fuentes, "Effect of attacker characterization in ECG-based continuous authentication mechanisms for Internet of Things," *Future Gener. Comput. Syst.*, vol. 81, pp. 67–77, Apr. 2018.

[17] W. Liang, M. Tang, L. Jing, A. K. Sangaiah, and Y. Huang, "SIRSE: A secure identity recognition scheme based on electroencephalogram data with multi-factor feature," *Comput. Electr. Eng.*, vol. 65, pp. 310–321, Jan. 2018.
[18] H.-S. Choi, B. Lee, and S. Yoon, "Biometric authentication using noisy electrocardiograms acquired by mobile sensors," *IEEE Access*, vol. 4, pp. 1266–1273, 2016.
[19] S. Zebboudj, F. Cherifi, M. Mohammedi, and M. Omar, "Secure and efficient ECG-based authentication scheme for medical body area sensor networks," *Smart Health*, vols. 3–4, pp. 75–84, Sep. 2017.
[20] P. Dodangeh and A. H. Jahangir, "A biometric security scheme for wireless body area networks," *J. Inf. Secur. Appl.*, vol. 41, pp. 62–74, Aug. 2018.
[21] S. Pirbhulal, P. Shang, W. Wu, A. K. Sangaiah, O. W. Samuel, and G. Li, "Fuzzy vault-based biometric security method for tele-health monitoring systems," *Comput. Electr. Eng.*, vol. 71, pp. 546–557, Oct. 2018.
[22] A. M. Koya and P. P. Deepthi, "Anonymous hybrid mutual authentication and key agreement scheme for wireless body area network," *Comput. Netw.*, vol. 140, pp. 138–151, Jul. 2018.
[23] N. Zhao, A. Ren, M. U. Rehman, Z. Zhang, X. Yang, and F. Hu, "Biometric behavior authentication exploiting propagation characteristics of wireless channel," *IEEE Access*, vol. 4, pp. 4789–4796, 2016.
[24] L. Shi, M. Li, S. Yu, and J. Yuan, "BANA: Body area network authentication exploiting channel characteristics," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1803–1816, Sep. 2013.
[25] M. Mohamed and M. Cheffena, "Received signal strength based gait authentication," *IEEE Sensors J.*, vol. 18, no. 16, pp. 6727–6734, Aug. 2018.
[26] B. Liu, H. Luo, and C. W. Chen, "A novel authentication scheme based on acceleration data in WBAN," in *Proc. IEEE/ACM Int. Conf. Connected Health, Appl., Syst. Eng. Technol. (CHASE)*, Jul. 2017, pp. 120–126.
[27] W. Wang, L. Yang, Q. Zhang, and T. Jiang, "Securing on-body IoT devices by exploiting creeping wave propagation," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 696–703, Apr. 2018.
[28] N. Zhao, Z. Zhang, M. U. Rehman, A. Ren, X. Yang, J. Zhao, W. Zhao, and B. Dong, "Authentication in millimeter-wave body-centric networks through wireless channel characterization," *IEEE Trans. Antennas Propag.*, vol. 65, no. 12, pp. 6616–6623, Dec. 2017.
[29] R. Chavez-Santiago, C. Garcia-Pardo, A. Fornes-Leal, A. Valles-Lluch, G. Vermeeren, W. Joseph, I. Balasingham, and N. Cardona, "Experimental path loss models for in-body communications within 2.36-2.5 GHz," *IEEE J. Biomed. Health Informat.*, vol. 19, no. 3, pp. 930–937, Apr. 2015.
[30] D. Goswami, K. C. Sarma, and A. Mahanta, "Path loss variation of on-body UWB channel in the frequency bands of IEEE 802.15.6 standard," *Healthcare Technol. Lett.*, vol. 3, no. 2, pp. 129–135, Jun. 2016.
[31] R. Bharadwaj and S. K. Koul, "Experimental analysis of ultra-wideband body-to-body communication channel characterization in an indoor environment," *IEEE Trans. Antennas Propag.*, vol. 67, no. 3, pp. 1779–1789, Mar. 2019.
[32] A. Thielens, R. Benarrouch, S. Wielandt, M. Anderson, A. Moin, A. Cathelin, and J. Rabaey, "A comparative study of on-body radio-frequency links in the 420 MHz–2.4 GHz range," *Sensors*, vol. 18, no. 12, p. 4165, 2018.
[33] K. Ali, A. Brizzi, S.-L. Lee, G.-Z. Yang, A. Alomainy, and Y. Hao, "Quantitative analysis of the subject-specific on-body propagation channel based on statistically created models," *IEEE Antennas Wireless Propag. Lett.*, vol. 14, pp. 398–401, 2015.
[34] S. J. Ambroziak, L. M. Correia, R. J. Katulski, M. Mackowiak, C. Oliveira, J. Sadowski, and K. Turbic, "An off-body channel model for body area networks in indoor environments," *IEEE Trans. Antennas Propag.*, vol. 64, no. 9, pp. 4022–4035, Sep. 2016.
[35] R. Sampangi and S. Sampalli, "Butterfly encryption scheme for resource-constrained wireless networks," *Sensors*, vol. 15, no. 9, pp. 23145–23167, 2015.
[36] Q. Wang, "A novel physical layer assisted authentication scheme for mobile wireless sensor networks," *Sensors*, vol. 17, no. 2, p. 289, 2017.
[37] Z. Li, H. Wang, and H. Fang, "Group-based cooperation on symmetric key generation for wireless body area networks," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1955–1963, Dec. 2017.



MUBARAK UMAR received the B.Sc. and M.Sc. degrees in computer science from Bayero University, Kano, Nigeria, in 2011 and 2015, respectively. He is currently pursuing the Ph.D. degree in computer science with Shaanxi Normal University, China. He is also a Lecturer with the Department of Computer Science, Bayero University, Kano, Nigeria. His research interests include authentication in body area networks, sensor networks security, information security of wireless communication, and cryptography.

ZHENQIANG WU received the B.S. degree from Shaanxi Normal University, China, in 1991, and the M.S. and Ph.D. degrees from Xidian University, China, in 2002 and 2007, respectively. He is currently a Full Professor with Shaanxi Normal University, China. His research interests include computer communications networks, mainly wireless networks, network security, anonymous communication, and privacy protection. He is a member of ACM and a Senior Member of CCF.

XUENING LIAO received the B.S. degree from Shaanxi Normal University, China, in 2012, and the Ph.D. degree from the School of Systems Information Science, Future University Hakodate, Hokkaido, Japan, in 2018. She currently holds a postdoctoral position with the School of Computer Science, Shaanxi Normal University, China. Her research interests include network coding, physical layer security of wireless communication, and performance modeling of buffer-aided relay wireless networks.