Efficient Anonymous Authentication Scheme in Body Area Networks Via Signal Propagation Characterization

Mubarak Umar[1,2], Zhenqiang Wu[2], Xuening Liao[2], Jiawang Chen[2], and Bello Ahmad Muhammad[2]
[1]Department of Information Technology, Bayero University, Kano 700241, Nigeria
[2]School of Computer Science, Shaanxi Normal University, Xi'an 710062, China

Owing to its capability to measure the sensitive biological data of patients through embedded sensors and transmit them via open wireless channels to remote medical experts, wireless body area network (WBAN) has been playing an important role in pervasive healthcare systems. However, the open nature of the wireless channels renders the data susceptible to being eavesdropped by an adversary and linked to the identities of the transmitting devices, which can enable the adversary to gain sensitive information and launch targeted physical attacks. Therefore, anonymous authentication and confidentiality of the data in WBAN are vital. In the last few years, numerous anonymous authentication schemes based on cryptographic primitives and physiological features were designed to enhance security in WBAN. However, most of the existing schemes are not computationally efficient or require additional sensing hardware. To address these limitations, we propose an efficient anonymous authentication scheme for WBAN based on signal propagation characteristics. The key idea in the proposed scheme is to utilize the distinct received signal strength (RSS) variation profiles between on-body and off-body communication channels to conceal the identities of communicating devices, thereby ensuring their anonymity during authentication. We perform security and performance analyses of the proposed approach to prove its security strength and computational efficiency, respectively. Moreover, extensive experiments are conducted on human volunteers in indoor and outdoor environments to show the robustness of our approach. The results of the analyses and the experiments show that our scheme can successfully mitigate 88.8% of active attack attempts with less computation overhead.

Index Terms—**Wireless body area network (WBAN), authentication, anonymity, signal propagation characteristics.**

I. Introduction

With the advances in wearable devices and embedded technology, interests in wireless body area network (WBAN) have developed in recent years [1], [2]. A WBAN is a network of low power sensors positioned on patients' bodies to measure and send their sensitive physiological data such as body temperature to healthcare experts over unprotected wireless channels. These collected data are then used for real-time clinical diagnosis. WBAN has several applications, such as personal health care monitoring and emergency medical services [3], [4], and thus its use could revolutionize healthcare provision in modern medical systems. However, the open nature of the wireless channels causes the patients' sensitive data to be susceptible to security attacks and unauthorized access. Specifically, an adversary may monitor the sensitive data of the patients during transmission, perform traffic analysis, and link the data to the identities of the devices in transmission. Even without recognizing the context of the data, the adversary can gain useful information by just knowing which sensor is transmitting. For instance, an unusual traffic from a blood pressure sensor discloses to the adversary that this patient has a blood pressure related problem. With information like this, the adversary can launch effective attacks targeting specific devices [5], [6]. Therefore, reliable anonymous authentication while considering the inadequate resources of the devices in WBAN is essential to the WBAN's security and the well-being of the patients.

Related researches on anonymous authentication in body area network can be mainly categorized into cryptographic and non-cryptographic schemes. The existing cryptographic anonymous authentication techniques [5], [6], [7] are based on traditional encryption and decryption algorithms, which rely on pre-distributed secrets. The strength of these schemes is that they are computationally impossible to be broken by an adversary that does not possess the decryption keys. However, these schemes have heavy computations such as bilinear pairing, which cannot be executed by the resource-constrained WBAN devices. Non-cryptographic anonymous authentication schemes, on the other hand, are based on physiological features [8], [9] (e.g., electrocardiogram (ECG)), which are measured separately at a sender and a receiver and compared to establish trust. These schemes are more preferable due to their less computation. However, the schemes are susceptible to denial-of-service (DoS) attack considering that the measured biological features by different devices for the same person may be different. Besides, additional sensing hardware that is usually required makes them cost-prohibitive.

We can establish from the aforementioned discussion that, both the schemes based on cryptographic primitives and physiological features can ensure anonymous authentication in WBAN. However, the cryptographic based approaches are not computationally efficient, while the schemes based on the physiological features require additional sensing hardware. The devices in WBAN have limited resources (including hardware, energy, and user interfaces) and thus cannot perform

Corresponding author: Zhenqiang Wu (email: zqiangwu@snnu.edu.cn)
Email Addresses: Mubarak Umar (mubarakumar@snnu.edu.cn), Xuening Liao (liaoxuening@snnu.edu.cn), Jiawang Chen (jiawangc@snnu.edu.cn), Bello Ahmad Muhammad (bamuhammad@snnu.edu.cn)

This work is supported by the National Natural Science Foundation of China (62001273), the China Postdoctoral Science Foundation (2019M663618), the Natural Science Basic Research Plan in Shaanxi Province (2020JQ-424,2020JM288), the Fundamental Research Funds for the Central Universities (GK202103087), and the Xi'an Key Laboratory of Mobile Edge Computing and Security (201805052-ZD3CG36).

the expensive computations in the cryptographic based schemes. The requirement of additional sensing hardware in the available physiological feature based approaches, on the other hand, is not only cost-prohibitive but can lead to compatibility issues with legacy systems. To address these shortcomings, we propose in this paper, a computationally efficient anonymous authentication scheme for WBAN based on physical (PHY) layer signal propagation characteristics with no additional sensing hardware requirement. The main idea in the proposed scheme is to exploit the distinct received signal strength (RSS) variation signatures between on-body and off-body channels in WBAN to mask the identities of communicating devices during authentication. We summarize the contributions of this paper as follows.

1) We propose an efficient anonymous authentication scheme for WBAN, which exploits the inherent RSS variation profiles between on-body and off-body channels in WBAN to ensure the anonymity of the communicating on-body devices.
2) We perform security analysis to prove the resilience of our scheme to security attacks and performance analysis to demonstrate its computational efficiency.
3) Finally, we validate the robustness of our approach via comprehensive experiments on 6 human volunteers in real-world places. The experimental results demonstrate that our approach can successfully provide anonymous authentication in WBAN while remaining computationally attractive.

The remainder of this paper is organized as follows. Related works are reviewed in Section II. System models and preliminaries are presented in Section III. In Section IV, we present the proposed anonymous authentication approach. In Section V, we conduct the security and performance analyses of the proposed approach. In Section VI, we present the evaluation of our approach in real-world environments, followed by the conclusion of our work in Section VII.

II. Related Works

A. Cryptographic based Anonymous Authentication

Several anonymous authentication techniques based on bilinear pairing were proposed for WBAN [10], [11]. In [5], Liu *et al.* proposed a remote anonymous authentication technique based on bilinear pairing defined on an elliptic curve. However, their approach is prone to impersonation attack [6]. To fix the security limitation in [5], He *et al.* [6] designed another bilinear pairing based anonymous authentication approach, where security credentials are stored on a network manager. However, Wei *et al.* [7] proved that the scheme in [6] only achieves weak anonymity. To address this limitation, the authors in [7] proposed an anonymous authentication scheme using low entropy password. In [11], an authentication framework for WBAN with clients' anonymity and location privacy is designed based on bilinear pairing. However, their scheme is not computationally efficient. To overcome the computational cost of bilinear pairing, lightweight hash function and exclusive-OR (XOR) operations are used to design anonymous authentication techniques in WBAN [12], [13], [14]. In [12], Li *et al.* used XOR and hash function operations to design an authentication technique for a centralized two-hop WBAN. However, this scheme is insecure against node impersonation attack. An anonymous authentication scheme that adaptively selects relay nodes in normal situations and emergencies is proposed in [15]. A dynamic password is utilized in [16] to propose a robust authentication scheme for WBAN. A lightweight mutual authentication scheme based on hash function and XOR operation is proposed in [17], which ensures forward secrecy. However, the scheme provides weak anonymity. Compared to other cryptographic techniques, elliptic curve cryptography (ECC) offers equal security with a much lesser key size. Consequently, ECC-based anonymous authentication schemes are proposed in WBAN [18], [19], [20]. In [21], Shen *et al.* proposed a multilayer authentication scheme based on ECC. Unfortunately, their scheme requires a group key update every time a node is added or deleted. In [8], a unique pseudo identity and a polynomial share generated for each device by a trusted authority are used for authentication in WBAN.

The major drawback of cryptographic based anonymous authentication schemes is their high computational complexity. In contrast, our scheme is less complex as it uses lightweight cryptographic primitives and channel characteristics measurements for authentication, which can be easily executed by the resource-limited WBAN devices.

B. Physiological Feature based Anonymous Authentication

To address the high computational complexity of cryptographic based anonymous authentication schemes, physiological features are measured separately at a sender and a receiver and compared to establish trust in WBAN. A hybrid anonymous authentication technique using an ECG signal is proposed in [9] to solve the security shortcomings of [12]. However, the approach in [9] lacks forward secrecy and requires additional sensing hardware, which is cost-prohibitive. A time-invariant fingerprint identifier and a time-variant ECG feature are used in [22] for authentication in WBAN. A bloom filter is introduced in [23] to conceal generated ECG features used for authentication in WBAN. However, their scheme achieves weak anonymity. In [24], eight fiducial features are extracted from a single heartbeat and used for authentication in WBAN. Unfortunately, the scheme suffers from feature learning overhead. In [25], Peris–Lopez *et al.* proposed an ECG based continuous authentication mechanism with an attacker characterization. However, the additional ECG sensor required in their scheme incurs hardware cost.

The limitations of physiological feature based anonymous authentication schemes are their vulnerability to DoS attack and the requirement of additional sensing hardware. In contrast, our scheme is different in two ways. First, it does not require additional sensing hardware to measure the RSS values of exchanged messages between devices. Second, the measured RSS values are required to be within some acceptable threshold for authentication instead of being equal. Thus, the issue of the DoS attack is addressed in our scheme.

III. System models and preliminaries

In this section, we present the network and threat models used in the proposed approach as well as some preliminaries.

A. Network Model and Assumptions

As illustrated in Fig. 1, the network model in our scheme is composed of three entities, which are sensor nodes, a controller node, and an off-body attacker device.

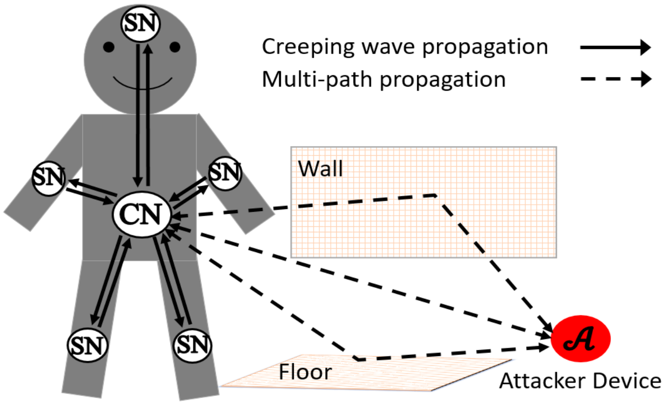


Fig. 1. Network model.

Sensor Nodes (SNs): There are n sensor nodes in our network, which are positioned on the patients' bodies to measure and transmit their biomedical data to medical experts for clinical diagnosis. The SNs have equal but limited resources, which make them unable to transmit the measured data directly to the medical professionals. Instead, the SNs transmit the data to a controller node, which is always within their transmission range as it is positioned at the center of the body of the patients.

Controller Node (CN): The controller node in our network is a smartphone that is positioned at the center of the body and has more resources than the SNs. The CN collects and relays the measured data from the SNs to medical servers [3], where medical experts can access them. Please note that the mode of communication between the SNs and the CN is half-duplex and they communicate directly via bluetooth over wireless channels. Moreover, to prevent interference between the signals of different communication links, we exclusively allocate all system resources to one communication link at a time. It should also be noted that creeping waves diffracted and trapped along the human body surface dominate the propagation of the on-body radio wave between the SNs and the CN, while the signal propagation between the CN and the attacker device is dominated by signal components arriving from several multipath radio channels caused by signal reflecting objects such as walls and floors [4]. In addition, anonymous authentication is needed before data is transmitted between any of the SNs and the CN.

Attacker Device ($\mathcal{A}$): The attacker device in our network is assumed to be an off-body device, which is not located on the same body as the legitimate SNs and the CN. It is, however, assumed to always be located within the proximity of few meters from the patient's body. More discussions on the capabilities of the attacker device are given in subsection III-B

B. Threat Model

We consider the following adversarial model in this paper.

- We use the Dolev-Yao (DY) attack model [26] where the attacker can capture transmitted messages, modify or delete some parts of the messages.
- The adversary can obtain the identities of devices from captured messages.
- The adversary can estimate the channel characteristics between the legitimate devices and itself.
- The adversary can initiate impersonation, man-in-the-middle, and replay attacks.

C. Theoretical Explanation of the Noticeable RSS Variation Signatures Between On-body and Off-body Channels

For succinctness, an on-body channel refers to a wireless link where both transceivers are situated on the same human body, whereas an off-body channel refers to a wireless channel where one of the transceivers is located on the body and the other is not. Previous empirical measurements [4], [27], [28] have demonstrated that there are significant RSS variation signatures between on-body and off-body channels because of the differences in the behavior of the signal waves as they travel on these channels. Although the propagation of the radio waves is reported to be influenced by multipath fading, direct path loss, and shadowing [28], the radio wave propagation on an on-body channel is mainly dominated by diffracted creeping waves that are trapped on the human body surface. This is due to the low-loss dielectric nature of the human body at microwave frequencies such as Wi-Fi and Bluetooth.

According to the theory of creeping wave [29], the electric field (E) released by the antenna of a transmitter over the human body on an elliptic path at a distance (d) between transmitter (T) and receiver (R) is expressed as

$$E = 2\sqrt{\frac{\varepsilon}{2\pi}}\frac{\sqrt{P_T G_T}}{d}e^{-j\omega d}F\left(\alpha, \beta, \theta, \vartheta\right), \tag{1}$$

where ε is the vacuum wave impedance, P_T is the transmission power in watts, G_T is the transmitter antenna gain, ω is the wave number in free space, $F(.)$ is the signal's fading factor, which is a function of α and β (with α and β respectively denoting the semi-major and semi-minor axes of the ellipse), θ is the signal's leaving point angle at T, and ϑ is the signal's receiving point angle at R. Moreover, the horizontal component of the electric field has a much higher attenuation than the vertical component [29] and thus, the antenna orientation on the body also impacts the path loss of the creeping waves greatly.

Eq. 1 hints that, rather than environmental dynamics, body surface as well as the orientations of the T and R antennas are the dominant components of the on-body radio wave propagations. Particularly, when two transceivers are positioned on the same body, motion of the body of any kind can adjust the body surface and the antenna locations, which can cause changes in the distance d between the T and R as well as the signal's fading factor $F(.)$. Consequently, on-body RSS would be steady when the body is static and fluctuates significantly when all or some parts of the body are in motion.

In contrast, the environmental dynamics and the distance between the two communicating antennas are the dominant components of the off-body radio wave propagations. This is largely attributed to the absence of the human body and the presence of free space between the T and R antennas. Thus, any changes in the environment or the distance between the two antennas will cause a significant RSS fluctuation at the R side. To this end, our proposed scheme utilizes these variations to hide the identities of the communicating devices and distinguish between their signals and those of the off-body attacker.

IV. The proposed anonymous authentication scheme

In this section, we proposed the anonymous authentication method for on-body devices in WBAN. As shown in Fig. 2, when SN and CN wish to authenticate each other anonymously, they start by exchanging messages that are empty and generating their RSS values. Next, the SN and the CN separately generate authentication parameters V_1 and V_2 using their identities and the generated RSS values. These authentication parameters are then exchanged by the SN and the CN and used to prove anonymously to each other that they are both on the same human body. Since the received RSS measurements depend on a receiver antenna, which is expected to be different for CN and the different kind of SNs in practice, our scheme does not require an exact match of the authentication parameters V_1 and V_1^* or V_2 and V_2^* at both ends for authentication. This is because it is impossible to guarantee that the received RSS of two different devices will be similar in practice. Thus, our scheme requires that the difference between the authentication parameters (i.e., $V_1 - V_1^*$ and $V_2 - V_2^*$) be within some acceptable threshold for authentication. This is made feasible in the proposed scheme due to the sufficiently distinct signal propagation profiles between on-body and off-body channels.

TABLE I. Notations and their descriptions.

Notation	Description
ID_{SN}	Real identity of SN
ID_{CN}	Real identity of CN
$Auth_{req.}$	Authentication request identifier
$Auth_{ack.}$	Authentication acknowledgment identifier
K_{SN}	Master key of SN
K_{CN}	Master key of CN
K_S	Session key
RSS_{SN}	Received signal strength value generated by SN
RSS_{CN}	Received signal strength value generated by CN
σ	A threshold value
$RNG(s)$	A random number generator that generates 128 bits K_S using a seed *"s"*
$\oplus$	Bitwise XOR operation
$E\,(K\,[a])$	A symmetric encryption function, which uses a key K to encrypt *"a"* using XOR operation
V_1, V_1^*, V_2, V_2^*	Authentication parameters

Our scheme is made up of two phases: a deployment phase and an authentication phase. In the deployment phase, the devices are placed on the body of the users together with their corresponding security parameters and identities. In the authentication phase, on the other hand, the devices engage each other for secure anonymous authentication. Please note that the deployment phase is carried out only once except when there is a new device to be deployed, while the authentication phase is executed whenever two devices wish to exchange data anonymously. The notations used in our approach are described in Table I.

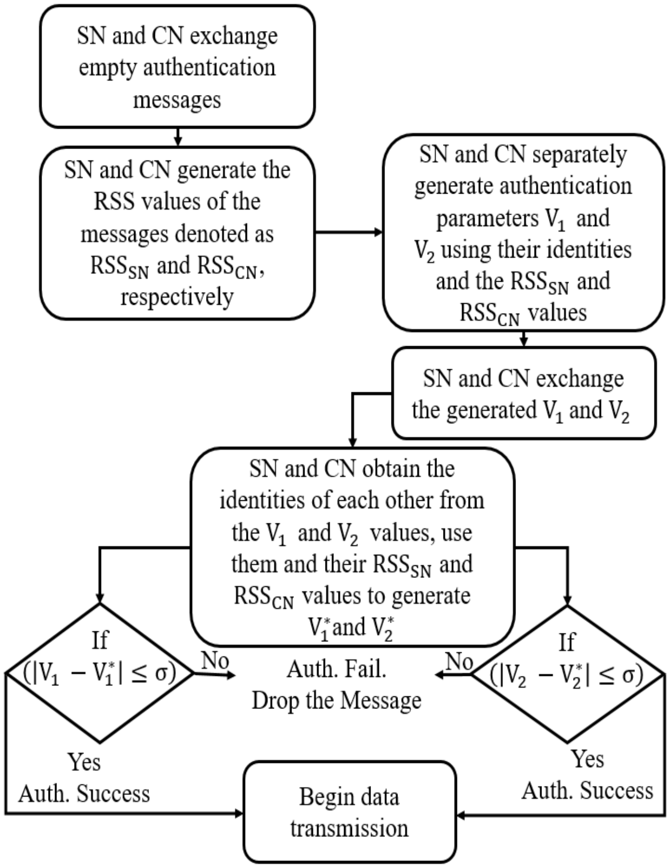

SN and CN exchange empty authentication messages
SN and CN generate the RSS values of the messages denoted as RSS$_{SN}$ and RSS$_{CN}$, respectively
SN and CN separately generate authentication parameters V$_1$ and V$_2$ using their identities and the RSS$_{SN}$ and RSS$_{CN}$ values
SN and CN exchange the generated V$_1$ and V$_2$
SN and CN obtain the identities of each other from the V$_1$ and V$_2$ values, use them and their RSS$_{SN}$ and RSS$_{CN}$ values to generate V$_1^*$and V$_2^*$
If (|V$_1$ − V$_1^*$| ≤ σ)
No
Auth. Fail. Drop the Message
No
If (|V$_2$ − V$_2^*$| ≤ σ)
Yes Auth. Success
Begin data transmission
Yes Auth. Success

Fig. 2. System flow diagram of the proposed scheme.

A. Deployment Phase

At this phase, a network administrator (NA) deploys the devices with the following steps.

Step 1: Positions the SNs and the CN on the body according to the network model.

Step 2: Picks the secret identities ID_{SN} for each SN and ID_{CN} for the CN.

Step 3: Picks a random K_{SN} and stores it on the memories of each SN and the CN. The NA also picks a random K_{CN} and stores it on the memories of CN and each of the SNs.

B. Authentication Phase

At this phase, we describe the 5 authentication steps as depicted in Fig. 3, which are followed in the proposed scheme whenever SN and CN wish to exchange data anonymously.

Step 1: $SN \rightarrow CN\,(Auth_{req.})$.
SN sends an $Auth_{req.}$ to CN indicating that it wishes to perform anonymous authentication with the CN.

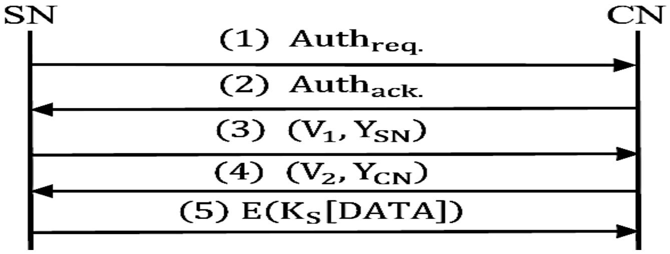


Fig. 3. The steps of the authentication in the proposed scheme.

Step 2: $CN \rightarrow SN\,(Auth_{ack.})$.
Upon reception of the message from SN, if CN wishes to perform anonymous authentication with the SN, it first obtains the RSS value of this message denoted as RSS_{CN}. CN then sends back a message containing $Auth_{ack.}$ to the SN.

Step 3: $SN \rightarrow CN\,(V_1, Y_{SN})$.
Upon reception of the message from the CN, the SN proceeds as follows.

- Obtains the RSS value of the message denoted as RSS_{SN}.
- Computes $X_{SN} = K_{SN} \oplus ID_{SN}$.
- Computes $Y_{SN} = X_{SN} \oplus K_{CN}$.
- Computes $V_1 = ID_{SN}^{RSS_{SN}}$.
- Sends the tuple (V_1, Y_{SN}) to CN.

Step 4: $CN \rightarrow SN\,(V_2, Y_{CN})$.
Upon reception of the tuple (V_1, Y_{SN}) from the SN, the CN proceeds as follows.

- Computes $X_{SN} = Y_{SN} \oplus K_{CN}$.
- Computes $ID_{SN} = K_{SN} \oplus X_{SN}$.
- Computes $V_1^{*} = ID_{SN}^{RSS_{CN}}$.
- Checks if $|V_1 - V_1^{*}| \leq \sigma$ (aborts the communication and ends the session if $|V_1 - V_1^{*}| > \sigma$).
- Computes $RSS_{SN} = log_{ID_{SN}}^{V_1}$ (this log operation is needed for the CN to obtain the RSS value of SN and use it to generate a session key K_S).
- Computes $K_S = RNG\left(RSS_{SN}^{RSS_{CN}}\right)$.
- Computes $X_{CN} = K_{CN} \oplus ID_{CN}$.
- Computes $Y_{CN} = X_{CN} \oplus K_{SN}$.
- Computes $V_2 = ID_{CN}^{RSS_{CN}}$.
- Sends the tuple (V_2, Y_{CN}) to SN.

Step 5: $SN \rightarrow CN\,(E\,(K_S\,[DATA]))$.
When the SN receives the tuple (V_2, Y_{CN}) from the CN, it proceeds as follows.

- Computes $X_{CN} = Y_{CN} \oplus K_{SN}$.
- Computes $ID_{CN} = K_{CN} \oplus X_{CN}$.
- Computes $V_2^{*} = ID_{CN}^{RSS_{SN}}$.
- Checks if $|V_2 - V_2^{*}| \leq \sigma$ (aborts the communication and ends the session if $|V_2 - V_2^{*}| > \sigma$).
- Computes $RSS_{CN} = log_{ID_{CN}}^{V_2}$ (this log operation is needed for the SN to obtain the RSS value of CN and use it to generate a session key K_S).
- Computes $K_S = RNG\left(RSS_{SN}^{RSS_{CN}}\right)$.
- Sends $DATA$ encrypted using the computed session key K_S (i.e., $E\,(K_S\,[DATA])$) to the CN.

Please note that we formulated the authentication problem in our proposed scheme as a binary hypothesis test to decide whether a message received by a destination device comes from a genuine device or an attacker. Therefore, when a destination gets a message at time t, it performs the hypothesis test below.

$$\begin{aligned} H_0 &: M(t) = M_{LD}(t) \\ H_1 &: M(t) = M_{\mathcal{A}}(t) \end{aligned} \tag{2}$$

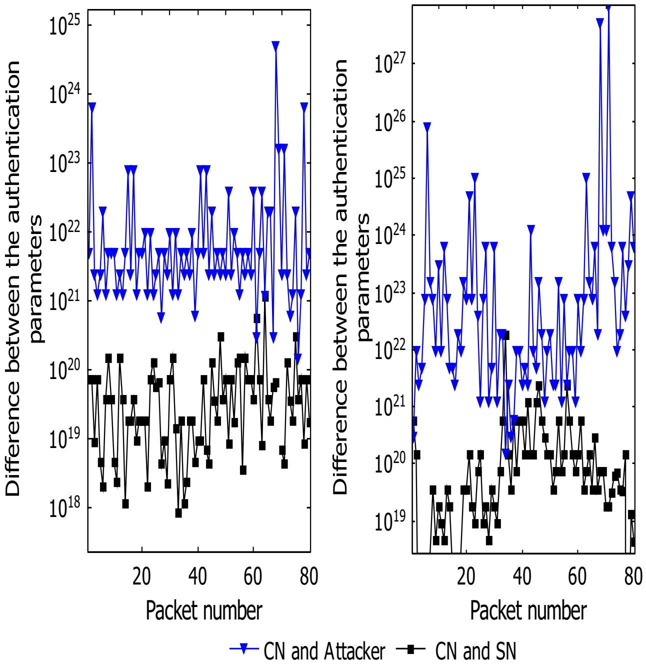
where the null hypothesis H_0 denotes that the origin of the received message $M(t)$ is a legitimate device (LD), and the alternative hypothesis H_1 implies that the origin of the received message $M(t)$ is the attacker $(\mathcal{A})$.

The authentication efficiency of our proposed scheme is based on a test threshold we estimated experimentally in a lab and a corridor located outside the lab. We used one Arduino device and one android smartphone in the experiments, which we positioned on a volunteer's body as SN and CN, respectively. Moreover, to simulate the off-body attacker, we asked another volunteer to hold another Arduino device and move within the proximity of the other volunteer during the experiments that lasted for 10 minutes in the lab and the corridor. During the experiments, each of the SN and the adversary exchange packets with the CN and vice versa in the following motions of the body of the volunteer: 1) sitting and standing in the lab, and 2) standing and walking in the corridor. The RSS values of the exchanged packets between the devices are generated and used to calculate the values of the authentication parameters V_1, V_1^{*}, V_2, and V_2^{*}. Next, we calculate and plot in Fig. 4, the results of the differences $(i.e., (|V_1 - V_1^{*}|), (|V_2 - V_2^{*}|))$ between the generated values of the CN and the attacker and the values of the CN and the SN.

We notice that the differences are small values between the CN and the SN, and large values between the CN and the adversary. We attribute these variations between the results to the following reason. As explained before, the propagation of the signal on the body is impacted by the surface of the body and the orientations of the devices' antennas. Thus, the effect of the body on the RSS values of the CN and the SN is almost the same since the devices are both located on the same body. This makes their RSS values to be close and hence the reason for the small differences between their calculated authentication parameters. In contrast, since the attacker in our scheme is not located on the same body as the CN, its RSS values are influenced by environmental dynamics and are not correlated with the RSS values of the CN. As a result, the calculated differences between their authentication parameters are large values. Based on these experimental observations, we conclude that if the generated results of $(|V_1 - V_1^{*}|)$ and $(|V_2 - V_2^{*}|)$ are less than or equals to a threshold value σ, the destination devices in our scheme accept H_0, otherwise they accept H_1. Therefore, the hypothesis test $(\mathcal{T})$ applied by the destination devices in our scheme is

$$\mathcal{T} = \mathcal{R} \underset{H_1}{\overset{H_0}{\lessgtr}} \sigma, \tag{3}$$

where $\mathcal{R}$ is the result of either $(|V_1 - V_1^{*}|)$ or $(|V_2 - V_2^{*}|)$.



(a) Sitting and standing in the lab.

(b) Standing and walking in the corridor.

Fig. 4. The results of $(|V_1 - V_1^*|)$ and $(|V_2 - V_2^*|)$ between the CN and the attacker, and between the CN and the SN under different body movements in different areas.

We define false alarm rate from the hypothesis test as the probability that a packet from a genuine device is considered as an attack attempt by a receiver, i.e.,

$$P_{FA} = P(H_1|H_0), \tag{4}$$

where P_{FA} denotes the probability of false alarm and $P(.|.)$ stands for conditional probability. False acceptance rate, on the other hand, is defined as the probability that an attack message is falsely accepted by a receiver, i.e.,

$$P_{FAc} = P(H_0|H_1), \tag{5}$$

where P_{FAc} denotes the probability of the false acceptance.

Through (4) and (5), we can define the probability of a receiver correctly accepting genuine messages as $P(H_0|H_0) = 1 - P_{FA}$, and the probability of a receiver accurately detecting and rejecting messages from the attacker as $P(H_1|H_1) = 1 - P_{FAc} = P_{AD}$, with P_{AD} denoting the probability of attack detection. Please note that we use the false alarm and the attack detection rates as the performance metrics to evaluate the effectiveness of our proposed approach. A good authentication scheme should be able to minimize the false alarm rate and maximize the rate of attack detection.

V. Security and Performance Analysis

In this section, we begin with a security analysis of our approach to prove its strength to security attacks. After that, we show the computational efficiency of the scheme through performance analysis.

A. *Security Analysis*

In this subsection, we demonstrate that our approach is secure against several security attacks. We define an intelligent off-body attacker $\mathcal{A}$ that can perform all the operations outlined in the threat model.

1) *Impersonation Attack*

We assume that $\mathcal{A}$ pretends to be SN to CN by sending $Auth_{req.}$ to CN. Upon reception of the message, the CN obtains the RSS value of the message represented as RSS_{CN} and sends $Auth_{ack.}$ to the $\mathcal{A}$. Next, $\mathcal{A}$ obtains the RSS value of the message represented as $RSS_{\mathcal{A}}$ and computes $X_{\mathcal{A}} = K_{SN_{\mathcal{A}}} \oplus ID_{\mathcal{A}}, Y_{\mathcal{A}} = X_{\mathcal{A}} \oplus K_{CN_{\mathcal{A}}}$, and $V_1 = ID_{\mathcal{A}}^{RSS_{\mathcal{A}}}$. $\mathcal{A}$ then sends $(V_1, Y_{\mathcal{A}})$ to the CN. Upon reception of the message from $\mathcal{A}$, the CN generates $X_{\mathcal{A}} = Y_{\mathcal{A}} \oplus K_{CN}$, $ID_{\mathcal{A}} = K_{SN} \oplus X_{\mathcal{A}}$, and $V_1^* = ID_{\mathcal{A}}^{RSS_{CN}}$. First of all, the generated $X_{\mathcal{A}}$ by the CN is not equal to the one generated by $\mathcal{A}$ because the $K_{CN_{\mathcal{A}}}$ used by $\mathcal{A}$ is different from the K_{CN} used by the CN (i.e., $K_{CN_{\mathcal{A}}} \neq K_{CN}$). Second, the generated $ID_{\mathcal{A}}$ by the CN is also different from that of the $\mathcal{A}$ because the K_{SN} and $X_{\mathcal{A}}$ used by the CN are different from those which the $\mathcal{A}$ used. Third, the generated V_1 and V_1^* by the $\mathcal{A}$ and the CN are not related because the $\mathcal{A}$ is not located on the same body as the CN and thus, its generated $RSS_{\mathcal{A}}$ used to compute V_1 is not related to the RSS_{CN} of the CN used to compute V_1^*. Thus, the difference between the V_1 and V_1^* will be greater than the threshold value with high probability (i.e., $|V_1 - V_1^*| > \sigma$). The same analysis applies to when $\mathcal{A}$ attempts to impersonate CN to SN. Thus, our scheme can resist the impersonation attack.

2) *Replay Attack*

The attacker $\mathcal{A}$ can intercept the tuple (V_1, Y_{SN}) from SN and replay it to CN to disguise as a legitimate SN. This attack will be detected by the CN since the RSS_{SN} used to generate V_1 is unique and randomly generated in each session. Thus, V_1 and Y_{SN} of one session cannot be considered legitimate in another session. The same analysis applies to when $\mathcal{A}$ attempts to replay the tuple (V_2, Y_{CN}) from CN to SN. Therefore, our proposed approach is resistant to the replay attack.

3) *Anonymity and Unlinkability of Sessions*

Let us assume that $\mathcal{A}$ intercepts communications from SN to CN and from CN to SN. The goal here is to ensure that from the intercepted messages, $\mathcal{A}$ cannot obtain the real identities of the communicating devices or link any two or more sessions to the same device. First of all, the real identities of the devices ID_{SN} and ID_{CN} are never placed on the channel in plain text in our scheme. Moreover, none of the $Auth_{req.}$ or $Auth_{ack.}$ identifiers contains the identities of the devices. Let us consider the tuple (V_1, Y_{SN}) from SN to CN. We have $V_1 = ID_{SN}^{RSS_{SN}}$, where RSS_{SN} is randomly generated by SN in each session. Thus, $\mathcal{A}$ cannot associate two separate authentication parameter V_1 with the same SN. The same analysis applies to the tuple (V_2, Y_{CN}). As these parameters are random, updated, and distinct in each session, $\mathcal{A}$ cannot associate two or more sessions with the same device. Thus, by utilizing channel characteristics, our scheme ensures the anonymity of the devices and the unlinkability of the sessions.

4) Man-in-the-Middle Attack

We assume that $\mathcal{A}$ intercepts messages (V_1, Y_{SN}) and (V_2, Y_{CN}) and attempts to modify these messages as a man-in-the-middle. The adversary $\mathcal{A}$ can generate $RSS_{\mathcal{A}}$ and try to compute V_1. However, without having ID_{SN} and the correct RSS value (since it not located on the body), $\mathcal{A}$ cannot generate the correct V_1. Likewise, to modify Y_{SN}, the adversary $\mathcal{A}$ has to get X_{SN}, K_{CN}, and K_{SN}, which are all secret and unknown to $\mathcal{A}$. Therefore, $\mathcal{A}$ cannot modify or generate the tuple (V_1, Y_{SN}). Similarly, $\mathcal{A}$ cannot modify or generate the tuple (V_2, Y_{CN}) because it cannot be able to generate the correct RSS value and does not know the secretly shared K_{SN}, K_{CN}, and ID_{CN}. Thus, our approach can prevent the man-in-the-middle attack.

5) Active and Passive Eavesdropping Attacks

The attacker $\mathcal{A}$ that can eavesdrop on all messages can obtain $Auth_{req.}$, $Auth_{ack.}$, V_1, Y_{SN}, $E\left(K_S\left[DATA\right]\right)$, V_2, and Y_{CN} from the common wireless channel. We need to protect K_S to prevent $\mathcal{A}$ from launching either active or passive eavesdropping attacks. It should be noted that the K_S in our approach is computed using a random number generator that takes the results of $RSS_{SN}^{RSS_{CN}}$ as a seed, where RSS_{SN} and RSS_{CN} are random and unknown to $\mathcal{A}$. First of all, since $\mathcal{A}$ does not know the identities ID_{SN} and ID_{CN} of SN and CN, respectively, $\mathcal{A}$ cannot get RSS_{SN} and RSS_{CN} from V_1 and V_2, respectively. Second, none of the Y_{SN}, Y_{CN}, $Auth_{req.}$, $Auth_{ack.}$ or $E\left(K_S\left[DATA\right]\right)$ contains any information about the RSS_{SN} or RSS_{CN}, which $\mathcal{A}$ can use to generate the K_S. Therefore, our scheme is resilient to the eavesdropping attacks, which can either be active or passive.

6) Channel Estimation Attack

We suppose that attacker $\mathcal{A}$ in our scheme uses the knowledge of its RSS value denoted as $RSS_{\mathcal{A}}$ and its distance to the CN and attempts to estimate the RSS_{CN} and RSS_{SN} of CN and SN, respectively. This type of attack is difficult to succeed in our scheme because of the following reasons. First, the pattern of the signal propagation on the body is directly affected by the surface of the body and has little to do with the distance between the transceivers. Thus, the continuous adjustment of the distance by $\mathcal{A}$ between itself and the CN will not give a similar effect to the signal as the surface and tissues of the body. Second, the multipath nature of the communication channel between the CN and the attacker means that the received signal at the CN is a combination of signals coming from several multipath channels. This environmental effect on the signal leads to the signal having a signature when the CN communicates with the attacker that is different from when the CN communicates with the SN. Due to the above reasons, the channel estimation attack in our scheme cannot succeed.

7) Mutual Authentication

From the above analysis of security thus far, we understand that only the legitimate SN and CN placed on the same body can generate V_1, V_1^*, V_2, and V_2^* values, where the results of $|V_1 - V_1^*|$ and $|V_2 - V_2^*|$ are less than or equals to the threshold value σ. Thus, SN and CN can confirm the legitimacy of each other by checking whether $|V_2 - V_2^*| \leq \sigma$ and $|V_1 - V_1^*| \leq \sigma$, respectively. As a result, mutual authentication is provided in our scheme.

B. Performance Analysis

In this subsection, we demonstrate the effectiveness of our approach regarding storage, communication, and computation costs. Moreover, we study the performance of the approach in comparison to the available anonymous authentication approaches of Liu *et al.* [5], He *et al.* [6], and Wei *et al.* [7].

1) Storage Cost

Each SN in our scheme is required to store its ID_{SN}, K_{SN}, and the CN's K_{CN}, which are respectively 16 bits, 128 bits, and 128 bits. The CN also is required to store its 16 bits ID_{CN}, 128 bits K_{CN}, and the 128 bits K_{SN} of all the registered SNs. Thus, the storage cost of each SN is 272 bits and that of the CN is 144 + 128n, where n stands for the number of the deployed SNs. Thus, the total storage overhead of our approach is 416 + 128n bits.

In Liu *et al.*'s scheme, each client is required to store $(N, ind_s, right)$, where N and ind_s are elements of an addition group G_1 with a prime order p, and $right$ is the client's right. Thus, a client's storage cost in their scheme is 1024 + 1024 + 64 = 2112 bits. In He *et al.*'s scheme, each client stores $(T_{id}, right)$, with T_{id} being an element of G_1. Thus, the client's storage cost in their scheme is 1024 + 64 = 1088 bits. In Wei *et al.*'s scheme, on the other hand, each client needs to store $credential = (id_C, \sigma.A_3(pw_C))$, which has a storage overhead of 544 bits.

In Table II, we summarize our scheme's storage cost compared to the other related schemes. From Table II, our approach has less storage cost than the other schemes except for Wei *et al.* [7] scheme.

2) Communication Cost

The SN and the CN in our approach exchange four messages between them for authentication. In step 1, the SN sends a 32 bits $Auth_{req.}$ to the CN. In step 2, the CN replies the SN with $Auth_{ack.}$, which is also 32 bits. In step 3, the SN sends the tuple (V_1, Y_{SN}) to the CN, which has 751 bits + 128 bits = 879 bits. In step 4, the CN replies the SN with the tuple (V_2, Y_{CN}), and the tuple has 751 bits + 128 bits = 879 bits. Thus, the entire communication overhead of the proposed method is 32 + 32 + 879 + 879 = 1822 bits.

In Liu *et al.*'s scheme, two messages $(d, L, t_C, R,' W')$ and $(MAC_{key}(d))$ are exchanged for authentication, where L, R', and W' are elements of G_1, d is a hash function generated digest, and t_C is a timestamp. Thus, the communication cost of their technique is 160 + 1024 + 32 + 1024 + 1024 = 3264 bits. In the scheme of He *et al.*, two messages (F, X, t_c) and $(J, Auth)$ are exchanged for authentication, where $F = E(key[id, right, U])$, $J = j.P$, $Auth = MAC(key[F, X, t_c, J])$, U and X are elements of G_1, t_c is a timestamp, $right$ and id are client's right and identity, respectively, P is a generator of a bilinear pairing group, and $j \in Z_q$. Thus, the communication overhead of He *et al.*'s approach is 1024 + 64 + 1024 + 32 + 160 + 1024 + 32 = 3360 bits. In Wei *et al.*'s scheme, three messages with a complete communication cost of 4224 bits are exchanged for authentication.

Table II gives a communication cost comparison of our technique among the existing techniques. From Table II, our technique has a lighter and efficient communication overhead compared to the related techniques.

TABLE II. Comparisons of our scheme and the existing schemes.

Schemes	Storage cost (bits)	Communication cost (bits)	Computation cost (s)
Liu *et al.* [5]	2112	3264	11.95
He *et al.* [6]	1088	3360	10.69
Wei *et al.* [7]	544	4224	8.92
Our scheme	416 + 128n	1822	0.006

3) Computation Cost

To determine the computation cost of the proposed scheme, we consider the following operations: T_{xor} is the time for one XOR operation, T_{log} is the time for one log operation, T_{mul} is the time for one big number multiplication operation, and T_{ks} is the time for one session key generation operation. The execution time for each of the operations is determined by repeated experiments using Arduino device. The average of all the experimental results for each operation is then taken as the final value. The execution times of T_{xor}, T_{log}, T_{mul}, and T_{ks} are calculated to be equal to 0.001 ms, 0.003 ms, 0.011 ms, and 2.75 ms, respectively.

In the proposed scheme, ten exclusive-OR operations, two log operations, four big number multiplication operations, and two session key computation operations are executed between SN and CN for authentication and data transmission. Thus, the computational overhead of our scheme is 10 T_{xor} + 2 T_{log} + 4 T_{mul} + 2 $T_{ks} \approx$ 0.006 s.

The execution times of all the operations performed in both the schemes of Liu *et al.*, He *et al.*, and Wei *et al.* are determined using a MICAz device, which has similar computation power to the Arduino device used in our experiments. The calculated running times of the bilinear pairing (T_e), scalar multiplication (T_{smul}), map-to-point hash function (T_H), point addition (T_{add}), modular exponentiation (T_{mexp}), and general hash function (T_h) operations used in the schemes are 5.32 s, 2.45 s, 0.89 s, 0.01 s, 1.25 s, and 0.01 s, respectively.

A client in Liu *et al.*'s technique executes four scalar multiplication operations, one map-to-point hash function operation, two point addition operations, one modular exponentiation operation, and three hash function operations during each authentication round. Thus, the computation overhead of their technique is 4 T_{smul} + 1 T_H + 2 T_{add} + 1 T_{mexp} + 3 $T_h \approx$ 11.95 s. In He *et al.*'s scheme, a client performs four scalar multiplication operations, one map-to-point hash function operation, one point addition operation, and four hash function operations during authentication. Thus, the computation overhead of their scheme is 4 T_{smul} + 1 T_H + 1 T_{add} + 4 $T_h \approx$ 10.69 s. In Wei *et al.*'s scheme, a client calculates five modular exponentiation operations and three map-to-point hash function operations during authentication. Thus, the computation overhead of their scheme is 5 T_{mexp} + 3 $T_H \approx$ 8.92 s.

In Table II, we summarize the computation cost of our approach and the related approaches. From Table II, our approach is computationally more effective than the approaches of Liu *et al.* [5], He *et al.* [6], and Wei *et al.* [7]. This is due to the complex bilinear pairing, modular exponentiation, and scalar multiplication operations used in the related schemes.

VI. Evaluation in real environments

In this section, we study the performance of our approach in indoor and outdoor places and discuss the experimental results.

A. Experimental Methodology

1) Implementation and Setup

As shown in Fig. 5, four devices (three Arduino UNO R3 devices and one Huawei Android Smartphone) are used in the experimental evaluation of the proposed scheme. The Arduino devices, which are used to emulate the on-body sensor devices have a portable battery and an optional sensor suite. They are fitted with a bluetooth 4.0 chipset to communicate at the 2.45 GHz band with the smartphone, which runs android 8.1 firmware. We implement the proposed scheme on the smartphone and the Arduino devices as an android background service and a sketch, respectively. As depicted in Fig. 5, two out of the three Arduino devices are used as legitimate on-body devices (i.e., the SNs), which are placed on the body of a volunteer using a strap for ease of movements. Specifically, one of them is located at the left shoulder and the other at the right thigh. The smartphone is positioned at the center of the volunteer's body and used as the controller node (CN). Moreover, we asked another volunteer to hold the third Arduino device to emulate the off-body attacker $\mathcal{A}$.

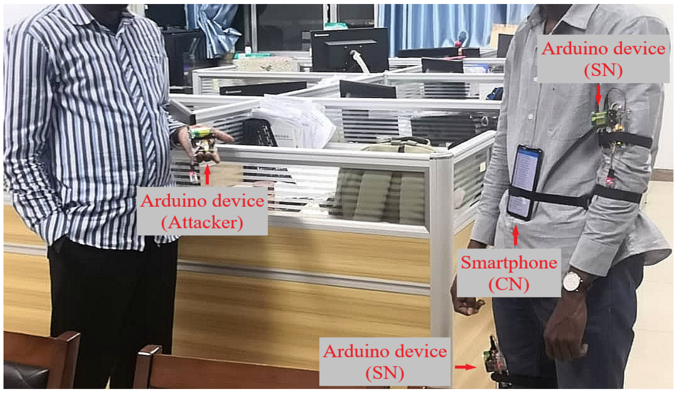


Fig. 5. Illustration of the positioning of the legitimate and attacker devices. The legitimate SNs initiate authentication by exchanging messages with the CN. The attacker device also sends messages to the CN in an attempt to disguise as a legitimate SN and authenticate with the CN.

To mimic real-life scenarios, we select two spots to perform the experiments: a 10 m × 8 m lab and a corridor outside the lab, which is an open place with people frequently passing by. Note that we do not enforce strict demands on the body movements of the volunteers. Moreover, the volunteer carrying the off-body attacker is not limited to any particular body movement and can walk freely within the proximity of the other volunteers wearing the legitimate on-body devices during the experiments. At the end of each experiment set, we collect RSS measurements of the messages exchanged between the devices and store them on the external storage of the smartphone for analysis.

2) Volunteers

Six volunteers labeled as $V1$, $V2$, $V3$, $V4$, $V5$, and $V6$ (age 28 ± 5 years, height 6 ± 1 ft, weight 150 ± 30 lbs) were involved in the experiments, which lasted for 20 minutes on each volunteer, with 10 minutes used in the lab and the other 10 minutes used in the corridor.

3) Evaluation Metrics

We use *attack detection rate* (ADR) and *false alarm rate* (FAR) as metrics to assess the performance of the proposed scheme.

ADR: This is defined as the rate at which attack messages are rejected.

FAR: This is defined as the rate at which legitimate messages are mistakenly rejected.

ADR and FAR computed as

$$ADR = \frac{\text{number of attack requests rejected}}{\text{total number of attack requests}} \times 100\%, \tag{6}$$

$$FAR = \frac{\text{number of legitimate requests rejected}}{\text{total number of legitimate requests}} \times 100\%. \tag{7}$$

As previously explained, the effectiveness of our scheme depends on the estimated value of the threshold σ. We notice that when the value of σ is very high, messages from the attacker are accepted as legitimate messages and thus the ADR of our scheme becomes low. If the value of the σ is very low, however, numerous legitimate messages are considered as attack messages and rejected, which leads to high FAR in the scheme. Thus, we carefully choose the value of the threshold σ that gives high ADR and low FAR in our scheme.

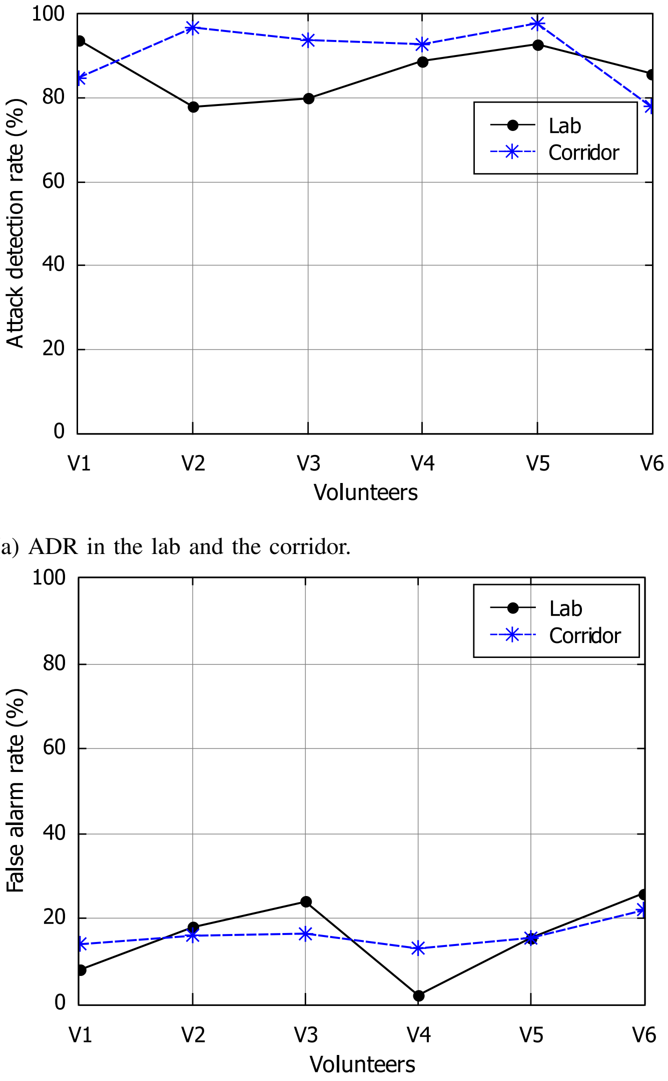
B. Performance Results and Discussions

In this subsection, we first investigate the performance of our approach in different places and body movements. After that, we examine the approach's overall performance on all the volunteers. In all the experiments conducted, a network setup of three on-body devices and one off-body attacker device is considered as illustrated in Fig. 5.

1) ADR and FAR of Our Scheme in Different Places and Body Movements

We validate the authentication efficiency of the presented approach in the lab and the corridor environments based on the following body movements of the volunteers: 1) *sitting and standing* in the lab, and 2) *standing and walking* in the corridor, both of which can be performed easily in real life. Essentially, the lab signal propagation differs noticeably from the corridor propagation with regard to multipath fading, shadowing, and direct path loss.

As shown in Fig. (6a), our scheme achieves an average ADR of 86.7% and 90.8% in the lab and the corridor, respectively. Interestingly, we observe from the results that the corridor has a higher ADR than the lab, which we believe is attributed to the less multipath variations in the corridor, which consequently leads to fewer messages from the attacker to be mistakenly characterized as legitimate ones. The lower ADR of the scheme in the lab, on the other hand, can be partly attributed to the fact that the lab tends to have a serious multipath impact on the signal because of the proximity between the volunteers and the signal reflecting objects (walls, computers, and desks) in the lab.



(a) ADR in the lab and the corridor.

(b) FAR in the lab and the corridor.

Fig. 6. Attack detection and false alarm rates of the proposed scheme in different environments and body movements.

Moreover, as illustrated in Fig. (6b), the proposed scheme has an average FAR of 15.6% and 16.2% in the lab and the corridor, respectively. According to Fig. (6b), the lab shows a lower FAR than the corridor. This is mainly because the disturbances on the signal caused by other people in the lab are less compared to those caused by the people frequently passing by in the corridor environment. In spite of the above differences, these results are consistent with those reported in the previous works [27], [28] and have shown the efficiency of our scheme in providing anonymous authentication in the presence of real-world environmental noise.

2) ADR and FAR of Our Scheme on Different Volunteers

We investigate the overall performance of the proposed scheme on each of the six volunteers. In these experiments, each of the volunteers is not restricted to any specific body movement or environment. The volunteers wander randomly and sometimes walk alongside each other in both the lab and the corridor for the duration of the experiments. In both the experiments, the wearers converse with one another while making casual gestures.

As shown in Fig. 7, our scheme achieves the average ADR and FAR of 88.8% and 15.9%, respectively. Specifically, it can correctly recognize 84.1% of on-body legitimate devices and successfully prevent 88.8% of active attack attempts from the off-body attacker. From the Fig. 7, we can see that due to the differences in the body features of the volunteers, our scheme's performance on each of the volunteers is different. Nonetheless, the results demonstrate the robustness of the proposed approach in providing anonymous authentication in WBAN with minimum overhead.

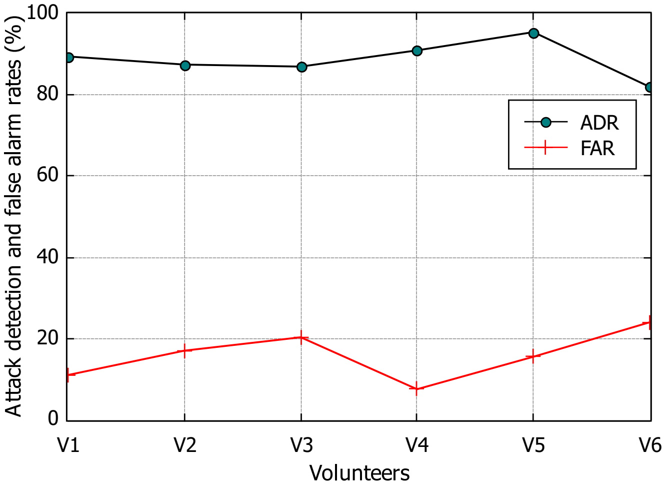


Fig. 7. Overall attack detection and false alarm rates of the proposed scheme for different volunteers.

VII. Conclusion

In this study, we presented a computationally efficient anonymous authentication approach for WBAN based on signal propagation characteristics. Our scheme utilizes the distinct RSS variation profiles between on-body and off-body channels to mask the identities of communicating devices, thereby ensuring their anonymity during authentication. Through rigorous analysis of security and computational complexity, we showed that our approach is secure against security attacks and ensures the anonymity of the communicating devices with a minimum computation cost. Moreover, the results of the real-world experiments we carried out on 6 human volunteers demonstrate that our scheme can successfully recognize 84.1% of legitimate on-body devices anonymously and detect 88.8% of active attack attempts. For the future, we plan to conduct additional security analysis of the proposed scheme using one of the formal methods and tools such as BAN logic and AVISPA. Moreover, the design simplicity of the proposed scheme gives it an edge over existing schemes as an appropriate choice for practical WBAN applications and other settings that require computationally inexpensive anonymous authentication schemes, such as wireless sensor networks and internet of vehicle computing.

References

[1] M. Kompara and M. Hölbl, "Survey on security in intra-body area network communication," *Ad Hoc Netw.*, vol. 70, pp. 23–43, 2018.

[2] M. Umar, Z. Wu, and X. Liao, "Mutual Authentication in Body Area Networks Using Signal Propagation Characteristics," *IEEE Access*, vol. 8, pp. 66411–66422, 2020.

[3] M. Umar, Z. Wu, and X. Liao, "Channel characteristics aware zero knowledge proof based authentication scheme in body area networks," *Ad Hoc Netw.*, vol. 112, pp. 102374, 2021.

[4] 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, 2013.

[5] J. Liu, Z. Zhang, X. Chen, and K. S. Kwak, "Certificateless Remote Anonymous Authentication Schemes for Wireless Body Area Networks," *IEEE Trans. Paral. Distr. Syst.*, vol. 25, no. 2, pp. 332–342, 2014.

[6] 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, 2017.

[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, 2018.

[8] 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. Heal. Informatics*, vol. 22, no. 4, pp. 1299–1300, 2018.

[9] A. M. Koya and P. P. Deepthi, "Anonymous hybrid mutual authentication and key agreement scheme for wireless body area network," *Comput. Networks*, vol. 140, pp. 138–151, 2018.

[10] 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, 2016.

[11] P. Vijayakumar, M. S. Obaidat, M. Azees, S. H. Islam, and N. Kumar, "Efficient and Secure Anonymous Authentication With Location Privacy for IoT-Based WBANs," *IEEE Trans. Ind. Informatics*, vol. 16, no. 4, pp. 2603–2611, 2020.

[12] X. Li, M. H. Ibrahim, S. Kumari, A. K. Sangaiah, V. Gupta, and K. K. R. Choo, "Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks," *Comput. Networks*, vol. 129, pp. 429–443, 2017.

[13] M. H. Ibrahim, S. Kumari, A. K. Das, M. Wazid, and V. Odelu, "Secure anonymous mutual authentication for star two-tier wireless body area networks," *Comput. Methods Programs Biomed.*, vol. 135, pp. 37–50, 2016.

[14] A. K. Das, M. Wazid, N. Kumar, M. K. Khan, K. K. R. Choo, and Y. H. Park, "Design of Secure and Lightweight Authentication Protocol for Wearable Devices Environment," *IEEE J. Biomed. Heal. Informatics*, vol. 22, no. 4, pp. 1310–1322, 2018.

[15] A. Arfaoui, A. Kribeche, and S. Senouci, "Context-aware anonymous authentication protocols in the internet of things dedicated to e-health applications," *Comput. Networks*, vol. 159, pp. 23–36, 2019.

[16] X. Liu, R. Zhang, and M. Zhao, "A robust authentication scheme with a dynamic password for wireless body area networks," *Comput. Networks*, vol. 161, pp. 220–234, 2019.

[17] Z. Xu et al., "A Lightweight Mutual Authentication and Key Agreement Scheme for Medical Internet of Things," *IEEE Access*, vol. 7, no. 3, pp. 53922–53931, 2019.

[18] X. Liu, C. Jin, and F. Li, "An Improved Two-Layer Authentication Scheme for Wireless Body Area Networks," *J. Med. Syst.*, vol. 42. no. 13, pp. 2–14, 2018.

[19] X. Li, J. Peng, S. Kumari, F. Wu, M. Karuppiah, and K. K. Raymond Choo, "An enhanced 1-round authentication protocol for wireless body area networks with user anonymity," *Comput. Electr. Eng.*, vol. 61, pp. 238–249, 2017.

[20] A. Andrew, O. Kittur, and P. K. Fagen, "An Efficient Remote Authentication Scheme for Wireless Body Area Network," *J. Med. Syst.*, vol. 41, pp. 1–9, 2017.

[21] J. Shen, S. Chang, J. Shen, Q. Liu, and X. Sun, "A lightweight multi-layer authentication protocol for wireless body area networks," *Futur. Gener. Comput. Syst.*, vol. 78, pp. 56–963, 2018.

[22] M. Al Reshan, H. Liu, C. Hu, and J. Yu, "MBPSKA: Multi-Biometric and Physiological Signal-Based Key Agreement for Body Area Networks," *IEEE Access*, vol. 7, pp. 78484–78502, 2019.

[23] X. Yao, W. Liao, X. Du, X. Cheng, and M. Guizani, "Using Bloom Filter to Generate a Physiological Signal-Based Key for Wireless Body Area Networks," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10396–10407, 2019.

[24] 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.

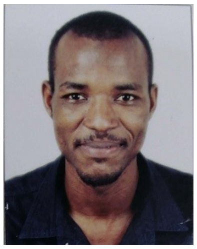
[25] P. Peris–Lopez, L. González–Manzano, C. Camara, and J. M. de Fuentes, "Effect of attacker characterization in ECG-based continuous authentication mechanisms for Internet of Things," *Futur. Gener. Comput. Syst.*, vol. 81, pp. 67–77, 2018.

[26] D. Dolev and A. C. Yao, "On the Security of Public Key Protocols," *IEEE Trans. Inf. Theory,* " vol. 29, no. 2, pp. 198–208, 1983.

[27] L. Shi, J. Yuan, S. Yu, and M. Li, "MASK-BAN: Movement-aided authenticated secret key extraction utilizing channel characteristics in body area networks," *IEEE Internet Things J.*, vol. 2, no. 1, pp. 52–62, 2015.

[28] Y. Huang, W. Wang, H. Wang, T. Jiang, and Q. Zhang, "Authenticating On-Body IoT Devices: An Adversarial Learning Approach," *IEEE Trans. Wirel. Commun.*, vol. 19, no. 8, pp. 5234–5245, 2020.

[29] T. Alves, B. Poussot, and J. Laheurte, "Analytical Propagation Modeling of BAN Channels Based on the Creeping-Wave Theory," *IEEE Trans. Antennas Propag.*, vol. 59 no. 4, pp. 1269–1274, 2011.



Mubarak Umar received his 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 Information Technology, 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 his B.S. degree in 1991 from Shaanxi Normal University, China, and received his M.S. and Ph.D. degrees in 2002, and 2007 respectively, all from Xidian University, China. He is currently a full professor at Shaanxi Normal University, China. Dr. Wu's research interests include computer communications networks, mainly wireless networks, network security, anonymous communication, and privacy protection, etc. He is a member of ACM and a senior of CCF.

Xuening Liao received her B.S. degree in 2012 from Shaanxi Normal University, China, and received her Ph.D. degree in 2018 at the School of Systems Information Science, Future University Hakodate, Hokkaido, Japan. She is now working as a post doctor in 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.

Jiawang Chen received his B.Sc degree in computer science from Xian Shiyou University, Xian, China, in 2016. He is currently pursuing the Ph.D degree in computer science with Shaanxi Normal University, China. His research interests include evolution of complex networks, graph generation with deep neural networks.

Bello Ahmad Muhammad received the B.Sc. and M.Sc. degrees in computer science from Bayero University, Kano, Nigeria, in 2010 and 2015, respectively. He is currently pursuing the Ph.D. degree in Computer Science with Shaanxi Normal University, China. He is also working with the University Library, Bayero University, Kano, Nigeria. His research interests include Learning style detection, recommender system, and graph representation learning.