Securing Health Monitoring via Body-centric Time-frequency Signature Authorization

Nan Zhao, Zhiya Zhang, Xiaodong Yang, Senior Member, IEEE, Aifeng Ren, Jianxun Zhao, Masood Ur Rehman, Senior Member, IEEE

Abstract—**Identity-based attacks serve as the basis of an intruder's attempt to launch security infringements in mobile health monitoring scenarios. Wireless channel perturbations due to the presence of human body are a relative phenomenon depending heavily on the subject's dielectric properties. A new Body-Centric Signature Authorization (B-CSAI) approach based on time-frequency domain characteristics was proposed. This method utilizes multiple millimeter wave bands of 27-28 GHz, 29-30 GHz, and 31-32 GHz, thereby enhancing the security in body-centric communications exploiting benefits of subject specific channel signature. The proposed bornprint method is based on the intrinsic identity related time-frequency domain information, which generated by the user's natural hand motion signature and resulting creeping waves and space waves. It can meet the unconditional keyless authorization requirements. A detailed measurement campaign considering radiation efficiency ($\bar{\eta}(dB) = -25.8, -24.7, -26.4$), pathloss exponent, and shadowing factor in three millimeter wave bands, using six human subjects confirm the usability and efficiency of the proposed approach. This also shows that there is a wide space for realizing security from physical mechanisms.**

Index Terms—**Mobile health, body-centric communications, signature authorization, subject specific, bornprint.**

I. Introduction

NOWADAYS health service architecture based on the core of medical institutions faces enormous challenges from new social changes [1]. Ubiquitous mobile health, the intention to join mobile communication technology into the health service architecture [2], and patient-centric based precision medicine [3], has become the main focus of research community. Implantable and wearable body centric medical devices are expected to improve the quality of medical diagnostics, but provide convenience while increasing security risks [4] [5]. Pioneer work in [6], proposed a security, lightweight, anti-denial-of-service upper security architecture. But also pointed out, for wireless body area networks deployment, or body-centric devices distribution, many protocols have emerged, but they all focus on protocol reliability and ignore security vulnerabilities. Traditional security solutions are impractical for a variety of emerging networks, especially the exponentially growing handheld applications, where most of their lightweight computing power comes from wireless devices [4] [7].

Traditionally, the security of wireless networks has been considered as a problem independent of the transmission of physical radio waves. However, some new network structures do not follow the traditional definition, such as streamlined protocol stacks to reduce energy consumption, and data encryption adopted by secure communications. It has raised the interest to exploit potential physical characteristics of radio waves for communication security attributes.

An overview of the low-complexity physical layer security protocols for Internet-of-Things (IoT) devices is presented in [8]. In [9], traditional security and authentication approaches are reviewed. In these traditional authentication methods, the core purpose is to determine whether the data are being generated and sent by a legitimate user. One of the key methods employed to solve such problems is digital signature technology. Signature authorization serves as a cornerstone in business transactions including the issuance of contracts and cheques, without it, business activities will not function properly. A forward-looking study in [10], raised the issue as one-way authentication and has given directional guidance. Certain digital phenomena have similar attributes as handwritten signatures [11] and can be used easily to identify and determine user authenticity as it cannot be randomly generated. This large class of technologies is collectively referred as one-way authentication.

A formulation that extracts useful information from certain distortion data set ensuring authentication is a more specific solution [9]. Due to the conversion of analog signals to digital format, the vast majority of processed information is to some extent distortion. The authorization has therefore a very wide range of applications in modern electronic systems.

In this paper, for wireless health monitoring scenarios, a new body-centric signature authorization (B-CSAI) scheme that meets unconditional and keyless authentication is implemented through the time-frequency domain characteristics of the user's body center channel. This solution combines the human tissue time-frequency domain characteristics with legitimate users. A prototype system was also constructed to confirm the availability and efficiency of the proposed signature authorization scheme. The main advantages of the scheme are:

Nan Zhao, Zhiya Zhang, Xiaodong Yang, Aifeng Ren, Jianxun Zhao are with the School of Electronic Engineering, Xidian University, Xi'an, Shaanxi, China, 710071.

Masood Ur Rehman is with the School of Engineering, University of Glasgow, Glasgow G12 8QQ, UK.

the test frequency bands meet the mainstream 5G definition and can be easily applied to 5G terminals; electromagnetic wireless devices are equipped with antennas, and the proposed scheme has no additional hardware requirements; the natural binding of signature authorization data to users has good security performance. The main contributions of this paper are as follows:

1) Based on the channel characterization at 27-28 GHz, 29-30 GHz, and 29-30 GHz, it is verified that the user's body-centric channel is subject-specific.

2) It is confirmed through experiments that the body-centric channel characteristics could not be simulated by the attacker, which satisfies the optimal conclusion of unconditional keyless authorization, and can be used for secure signature authorization.

3) The proposed signature authorization scheme confirms the security from the perspective of physical mechanism, which can resist active and passive attacks well and has good scalability.

Following the introduction, the paper is divided into five parts. Section II reviews related research. Section III describes the physical basis of B-CSAI, using radio wave propagation and gives details of security scenarios considered. Section IV discusses the basic principles of the proposed B-CSAI security technique. Section V presents the experimental design, results, and analysis. Finally, conclusions are drawn and recommendations are given in Section VI.

II. Related Work

In this section, it is divided into three parts to introduce the conventional security authorization, the millimeter wave related physical layer security, and the main concerns of this manuscript.

A. Conventional Security Method

In previous studies [12], security has traditionally relied on encryption in a defined network structure through an isolation principle. This kind of mature and large-scale application of cryptographic system operation is easy to understand, and if deployed correctly, these systems can provide reliable security guarantees. But there are always some recognized limitations. First of these is the security strength. Such systems usually assume that the adversary has only limited computing resources, which were true at the information age beginning, however, with the advancement of microelectronics, this assumption is becoming increasingly unrealistic. Second, the overhead generated by the key distribution involved in security. As the system becomes larger, improper key management may be exposed to social engineering attacks. Although many smart physical layer communication process encryption schemes are designed, attempt to meet those requirements by the channel [11]. However, reliable access to the channel state information of both communication parties is always a recognized obstacle.

In [13], key-based authentication is solved from the perspective of privacy-limited registration data. It is assumed that the user's measurement during the authentication phase is controlled through a cost-limited "action" sequence. The issue of identification and certification from the perspective of information theory is discussed considering user-generated source data, such as biometric data sources. In [14], an adaptive positioning fitting model is proposed to effectively deal with overlapping fingerprint separations. Retinal image registration is crucial for the diagnosis and treatment of various eye diseases. Many methods have been developed to solve this problem. In [15], a new retinal image registration method has been suggested to utilize significant feature areas. However, the rapid and accurate recording retinal images is still a challenging issue due to low content contrast, large intensity differences, and deterioration of unhealthy retinas. In fact, traditional biometrics represented by the above fingerprints and irises can be well implemented in resource insensitive applications. However, there is still an urgent need to explore new biometrics in lightweight network architecture.

B. Physical Layer Security with Radio Wave Propagation

In [16], the potential application of physical layer security in millimeter-wave (mm-wave) ad hoc networks is explored. It is being observed that the low transmit power state using a low mm-wave frequency can achieve better security performance. A transition from low mm-wave frequency to a high mm-wave frequency is required to obtain a higher confidentiality rate when the transmit power is increased. Because in the case of high transmit power, the sensitive high frequency can be more effective to facilitate communication establishment in an increased path loss state and provide security bits. However, the main drawback of security solutions in existing wireless communication scenarios, is that they do not take advantage of the wireless media characteristics [17]. For example, the broadcasting and fading characteristics of a wireless medium that brings variation in channel parameters over time, frequency, and space.

In our view, combining wireless authentication with confidential communication can partially replace or facilitate password peers for more secure communications, at least for initial trust. Although physical layer security has attracted many research work, health-IoT related authentication signatures are still relatively unexplored [17]. As physical layer security relies on the radio wave propagation and channel characteristics, advances in this area are also vital importance. With the continuous advancement in miniaturization of electronic devices, wearable computing has been a reality with a variety of commercially body-worn devices. Radio wave propagation is relatively stationary between basestation with mobile terminals [18], but it is highly unstable in on-body or body-to-body communication scenarios.

Studies of channel characteristics and antenna propagation performance in the on-body S-band (around 2.45 GHz) link has shown that the path loss can vary up to 50 dB due to different antenna arrangements and changing body postures [18] [19]. It infers that the characterization of radio wave propagation should necessarily take into account the changes caused by the geometry of local environment. That can also impact the antenna input matching and radiation patterns. Wireless propagation in body-worn sensors up to X-band frequencies is a

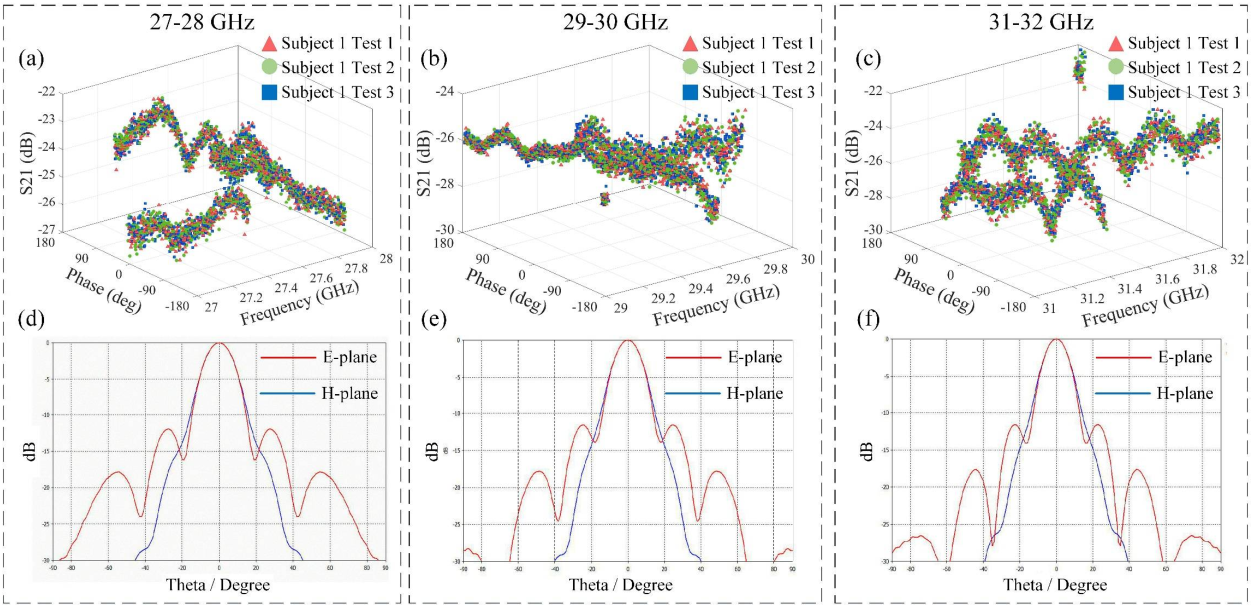


Fig. 1. Time frequency characteristics of the millimeter wave wireless link and along with antenna radiation patterns at the three studied frequency bands, (a) time-frequency data for subject 1's attempts to sign and authorize in 27-28 GHz band based on three measurements, (b) time-frequency data for subject 1's attempt to sign and authorize in 29-30 GHz band, (c) time-frequency data for subject 1's attempt to sign and authorize in the 31-32 GHz band, (d-f) radiation patterns of the B-CSAI antenna operating in the corresponding frequency band.

well-studied paradigm [20] [21]. However, higher frequencies of millimeter wave and sub-millimeter wave, which are fast strengthening their claim as one of the key enabling 5G technologies, are needed further ascertaining [22].

C. *Threats and Concerns*

Researchers have considered the security challenges faced by the four different protocols included in IEEE 802.15.6 [23]. That work has clearly shown that the IEEE 802.15.6 standard lacks security and suffers from serious signature authentication problems. Millimeter waves also exhibit higher free space attenuation relative to microwaves [24]. This is an important feature as far as security is concerned as it contains the wave propagation within the vicinity of the human body and minimizes interference with other systems. It makes the body-centric loss difficult to be obtained at a distance inherently enhancing security attributes. The underlying physical layer features have been valued by many researchers and are considered as a potential addition/replacement to security services in wireless networks. Identity-based attacks are thought to be the first step in an intruder's attempt to launch various attacks [25]. Signature authorization is an essential part of the basic security process and is exactly what the body-centric communication needs [26].

Authorization, authentication, and trust, the process of entity identification are prerequisites for authorization. In most scenarios, the authorization will not be possible without proper authentication, and authentication is essentially based on trust [27]. The authors proposed and discussed the authentication in body-centric networks in [28]. For a large scale deployment of the physical layer security technologies in wearable applications, it is necessary to expand our understanding from authentication towards authorization. The next section will introduce the security significance of radio propagation.

III. Physical Basis of B-CSAI

A. *Security Potential of Microwave*

The classical monograph urges us to employ more open-minded visions to examine the network's security issues [29]. Interdisciplinary thinking is not only helpful, it is rather indispensable in today's increasingly vulnerable information sharing world. Over the past decade, physical layer security research has seen unprecedented growth with many promising design insights. Most of these solutions are based on wireless communication because a large amount of data is transmitted over wireless links, which are more exposed to security threats as compared to their wired counterparts. In [30], hardware resources are considered as a potential information theoretic security device, having excellent reliability against strong adversary models.

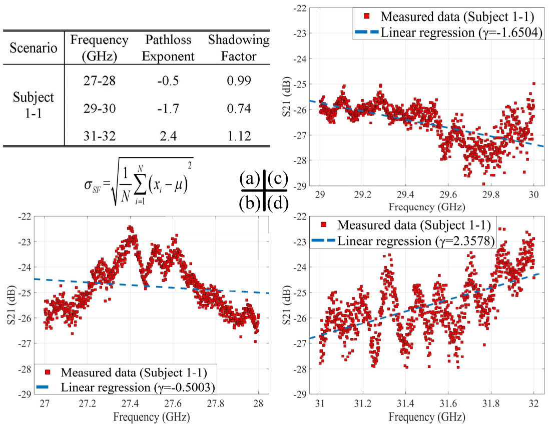
In [31], an excellent template for body-centric correlation channel model study is given, studying numerical characterization and link budget assessment of wireless implants for different digital human models using multiple non-uniform phantoms. It is observed experimentally that the antenna pattern strongly depends on the location of wireless implants and the body composition of subjects, which makes the body-centric communication highly user-specific. The understanding is further cemented through the work presented in [32] where the authors have characterized the ultra-wideband (UWB) wireless channel for medical applications. The numerical analysis has revealed the dependence of antenna performance and wireless channel characteristics on the gender, height, and body mass index of the user. Variation in the path loss between different users is reported to be one-fifth of the free-space value, which embodies rich features of the body-centric communications time-frequency parameters. And these characteristics can be utilized effectively as a potentially good candidate for biometrics. More extensive, in [33] [34] shows the potential security meaning of human electrical properties.

B. Basic of B-CSAI Physical Channel Model

In our considered application scenario of signature authorization (where a human hand and its impact on the wireless channel is used as signing and authorization tool), this time-frequency characteristic of the human hand is of special interest. We have used three mm-wave frequency bands of 27-28 GHz, 29-30 GHz, and 31-32 GHz in this investigation due to growing commercial interest on them. These frequencies offer a very high data rate for real-time audio and video streaming in 5G and beyond communication paradigms. Moreover, shorter wavelengths allow device miniaturization, which is vital for body-centric portable/wearable/implantable applications. Furthermore, mm-waves interaction with biological tissues is also controllable as they reduce both the possible health concerns associated with human exposure to electromagnetic radiation and can couple enough subject feature information.

Figure 1 presents the time-frequency domain information (using S_{21} (path loss/transmission coefficient)) of one human subject's hand in three mm-wave frequency bands. For the sake of experimental rigor, radiation patterns of the antenna used in the corresponding frequency band are also depicted, in Fig. 1(d-f). Results for three tests are given to stipulate the idea. The results show that good communication links are built on creeping waves (which propagate beneath the body surface and are very sensitive to surface and near-surface defects) and surface waves (which propagates over the human body surface). Which are major reasons for B-C communication link changes.

Figure. 1(a) shows the time-frequency domain characteristics in the 27-28 GHz frequency band. The phase of the millimeter wave signal varies between -180° to 180° and the signal frequency gradually increases from 27 GHz to 28 GHz (in 1 MHz step). The quantified data shows very good autocorrelation characteristics. A high level of repeatability in multiple experimental trials is evident showing satisfactory stability of the measurements. The radiation patterns show that with increase in the frequency, antenna main beam gradually narrows, but there is no obvious distortion. This not only helps in the multi-band feature extraction, but also shows that the high repeatability observed in Figs. 1(a-c) is indeed caused by the subject, not only by the antenna.



Scenario	Frequency (GHz)	Pathloss Exponent	Shadowing Factor
Subject 1-1	27-28	-0.5	0.99
	29-30	-1.7	0.74
	31-32	2.4	1.12

$$\sigma_{SF}=\sqrt{\frac{1}{N}\sum_{i=1}^{N}\left(x_i-\mu\right)^2}$$

Fig. 2. Dependence of path loss on the frequency band, for the considered body-centric link (a) mathematical expression and calculated values (shadowing factor is represented using standard deviation), (b-d) path loss data and linear fit for the three considered frequency bands, respectively.

To gain further insight into the relationship between path loss (S_{21}) and change in the frequency bands, mathematical modeling is needed. Path loss is the gradual loss in the energy of the wireless signals as they propagate. We considered body-centric hand channel can be modeled in terms of path loss exponent and shadowing factor through the following expression:

$$PL(d)=PL(d_0)+10\gamma\log_{10}\left(\frac{d}{d_0}\right)+N(0,\sigma) \tag{1}$$

where $PL(d_0)$ is the estimated or simulated path loss in the distance d_0 between the sending and receiving parties, γ is defined as path loss exponent, $N(0,\sigma)$ is a simplified definition of standard deviation (to avoid increased complexity of the time-frequency model of B-CSAI and stipulate the workability of the proposed technique) where σ represents shadowing factor. The definition of σ_{SF} is further detailed in Fig. 2(a). Equation (1) shows that the channel variation depends on γ, $N(0,\sigma)$, and the distance d for sending and receiving signals. The distance of the application scenario is kept

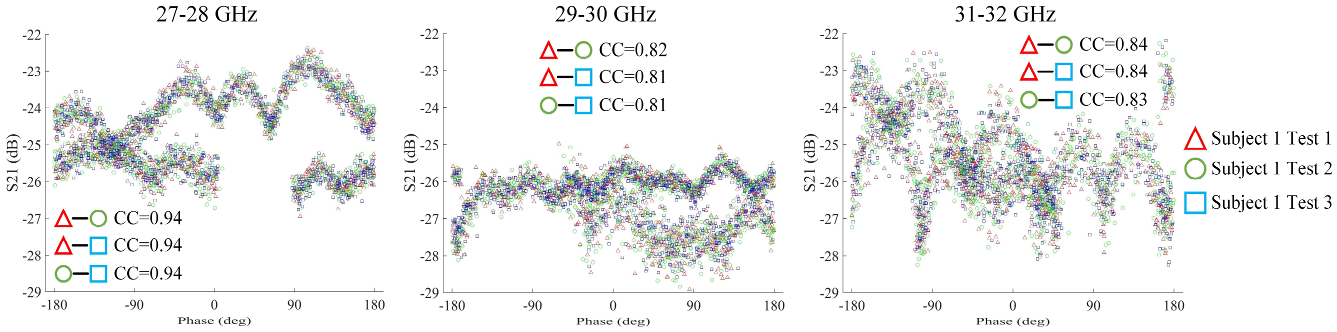


Fig. 3. Path loss of a given test showing the time-frequency relationship between the three frequency bands and the specific correlation coefficient.

constant in this work for the sake of simplicity, so the main influencing factor is the user's body itself. For example, at 29-30 GHz, the pathloss exponent is equal to -1.7, and the shadowing factor is 0.74 (with 95% confidence bounds).

The 3-D data of Fig. 1 is shown 2-D space in Fig. 3 (x-axis is phase, y-axis is S_{21}). It is clear that in different frequency bands, repeated tests by the same subject are highly reproducible. The correlation coefficient (CC) shows that the body-centric channel induces a hand effect, and repeated experiments certainly have distortion, which means biometrics and the correlation between distortions are extremely stable. For example, in 27-28 GHz band, CC = 0.94 which indicates it is nearly consistent. In the other bands, CC changes are minimal having fluctuations of the order 0.01. It should also be noted that Fig. 3 maps spatial time-frequency features to 2-D planes, and the local data point clouds are occluded. This reduces the high repeatability of CC, but also shows the richness of raw B-CSAI features.

To further understand the effect of the human hand on the path loss at different operating frequencies, let us consider the Debye model for dispersion [35]:

$$\varepsilon(\omega) = \varepsilon_\infty + \sum_{p=1}^{P} \frac{\Delta\varepsilon_p}{1 + j\omega\tau_p} \tag{2}$$

where ε_∞ is relative permittivity at infinite frequency, $\Delta\varepsilon_p$ is due to the relative permittivity change caused by Debye pole, τ_p is the pole relaxation time. Eq. 2 shows that the dielectric constant of the human body is dependent on the frequency of the electromagnetic wave. In other words, with the change in the electromagnetic wave frequency, the human organs composed of similar tissues will exhibit different electric properties. Human organs composed of different tissues will have different responses even at the same frequency. This theoretical derivation is corroborating with the results in Fig. 3 where the pathloss exponent and shadowing factor of the same subject have changed significantly in the three bands while the CC is still very high in the same frequency band. This infers that raw B-CSAI is a stable approach for the participants themselves. Fig. 4 illustrates the experimental data distribution from a statistical point of view. It shows that due to the increase in frequency, the characteristics of the channel have greatly changed, and the received signal is no longer a perfectly normal distribution signal. In the lower frequency band (27-28 GHz), the probability density function (PDF) curve presents a saddle-shaped double peak, mapping to the cumulative distribution function (CDF) curve is a more obvious two-phase acceleration. In 29-30 GHz, the S_{21} data is enriched at -26 dB, which corresponds to its average value of -26.6 dB, and there is also a steeply accelerated section in the CDF curve. At 31-32 GHz, the data distribution is more uniform and the PDF peak appears around -26 dB, which is also consistent with its mean value of -25.5 dB.

Combining communication channel modeling and bornprint we know:

$$P_{\widehat{sign}} = P_{sign}\left(1-\left|S_{11}\right|^2\right)G_t\left(\frac{\lambda}{4\pi d}\right)^2 G_r\left(1-\left|S_{22}\right|^2\right) \tag{3}$$

where $P_{\widehat{sign}}$ is B-CSAI that passes through the body-centric channel, P_{sign} is the signature authorized original signal, G_t and G_r is the gain on the transmit and receive sides, The S_{11} and S_{22} are the reflection coefficients. Combining Eq. 1 and 3, we can deduce that:

$$P[dB] = P_0 + 10\gamma\log_{10}\left(\frac{d}{d_0}\right) + \underset{\text{Creeping waves}}{\Psi[dB]} + \underset{\text{Surface waves}}{\Pi[dB]} \tag{4}$$

where $\Psi[dB]$ represents the creeping wave component and $\Pi[dB]$ represents the surface wave component. This further explains the combined effect of creeping wave and surface wave component in the B-CSAI that is statistically reflected in Fig. 2(a). Due to microwave modeling of body area network, at the microscopic level, the creeping wave propagating is mainly in the shallow surface of the body. The surface waves collectively carries and couples the user's time-frequency characteristics into themselves and become a good source of signature authority. Our time-frequency domain body-centric signature authorization model is formulated in Eq. 5 and illustrated in Fig. 5:

$$Y(i) = \Psi_m(i)X(i) + \Pi_m(i) \tag{5}$$

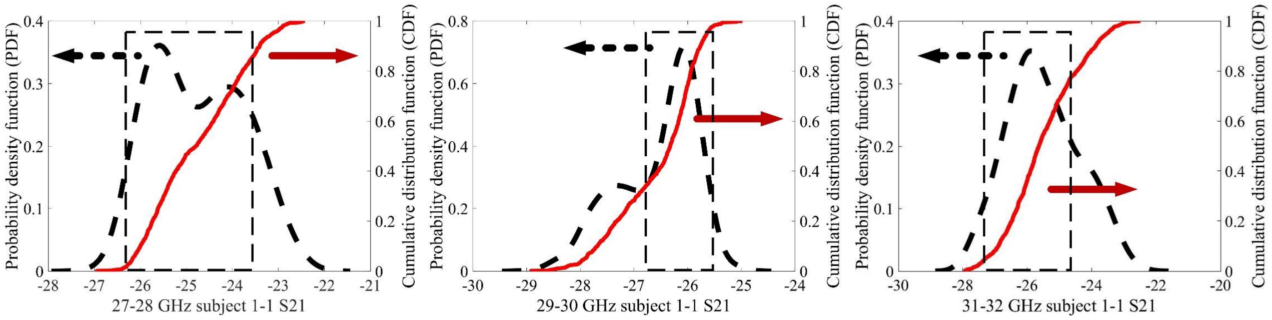


Fig. 4. Data feature probability density function (PDF) and probability cumulative distribution function (CDF) for S21 in different frequency bands.

where $X(i)$ is main B-CSAI channel input, $Y(i)$ is the signature authorization channel output, $\Psi_m(i)$ and $\Pi_m(i)$ are the effects of creeping waves and surface waves, respectively. The P_{sign1}, P_{sign2}, P_{signn} from the user's body are independent but identically distributed signatures in the time-frequency domain. In formal applications, this type of signal is transmitted through coding, and some distortion (such as digital analog conversion) occurs. It makes the signal as X^n which then passes through the body-centric channel composed of Ψ_m^n (creeping wave) and Π_m^n (surface wave) components, coupled with the body characteristics. At this point, the signal becomes Y^n. A possible decoder will guarantee the establishment of the communication itself. A highly abstract logical model will include all effects from normal communications to possible malicious attacks. The resulting reconstructed signal $P_{\widehat{sign}}$ will reflect the influence of the body-centric loss. Whether such reconstruction can be performed will become a criterion. This type of reconstruction has been defined in Eq. 5 and is termed as "authentic".

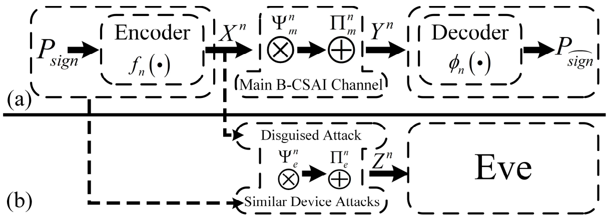


Fig. 5. (a) B-CSAI system model. The original signal P_{sign} passes through the creeping wave Ψ_m^n and the surface wave Π_m^n channel, and is coupled to the body-centric time-frequency characteristics. The resulting $P_{\widehat{sign}}$ can be used as an authorized signature, (b) B-CSAI attack paradigm.

In the absence of scattering scenes, the de-correlation resulting from the natural spatial separation of legitimate users and adversary channels may be slower than expected by the mathematical model. If there is a Line-of-Sight (LOS) channel, then the radio wave will have priority in choosing the mode of propagation. From the point of view of communication establishment in the weak scattering environment, the communication signal quality is more stable and also conforms to experimental observation. This is a widely used assumption in physical layer security channel key agreement studies. The deployment scenario has therefore more complicated conditions to help both communicating parties better extract secret bits from channel changes. Slightly different in B-CSAI, the signature authorization scenario is simple, the stability of the LOS channel makes the protocol robust, and the added user hand impact introduces a rich channel change adding lots of fresh identity features.

In this section, we started with the microwave security potential, established the B-CSAI physical channel model according to the classic method of radio wave propagation, and explained the principle of signature authorization preliminarily.

IV. B-CSAI Security Principle

The availability of physical layer security dual-threshold algorithm in the health monitoring body-centric network is studied in [36]. In [37], a theoretically optimal conclusion is given from the information theory point of view, indicating that unconditional secure keyless authentication is feasible if and only if the legitimate channel for extracting wireless fingerprints cannot be simulated by the attacker. In the previous section, we have elucidated the principle of B-CSAI wave propagation from the perspective of the classical body-centric antenna propagation. It includes not only the details of the body-centric time-frequency domain, but also the subject's specificities. In this section, we will discuss the security principles of our solution around the optimal conclusion of keyless authentication theory.

A. B-CSAI Security Background

The one-way authentication problem was defined in 1976 by [10], making it clear that a digital phenomenon with the same attributes as a written signature is needed for a secure link. It should be easy for anyone to realize that the signature is true, but it is impossible for anyone other than the legal signer to produce a signature. This is the first time that the signature authority has been proposed systematically, according to the authors' knowledge. In fact, Shannon's work is more biased towards symmetric key cryptography. Perhaps a more relevant development is Wyner's work on eavesdropping channel. He introduced the idea of providing security through the channel itself, rather than the secret shared by both parties.

$$R_K = \frac{1}{T} I\left(\tilde{h}_{AB};\tilde{h}_{BA}\right) = \frac{1}{2T}\log\left(1+\frac{\sigma_1^4 P^2 T^2}{4\left(\sigma^4+\sigma^2\sigma_1^2 P\ T\ \right)}\right) \tag{6}$$

In a recent landmark development [7], Eq. 6 has been given stating that the key rate R_K depends on the transmit power P and the coherence time T. It is also concluded that the key generation rate increases with increase in the transmit power. The coherence time however affects oppositely by reducing the key rate when P being increased. It is therefore deduced that from the perspective of key generation, a rapidly changing channel environment is advantageous, as a slow or almost stable channel environment will lead to a slow key generation. Discussion in [16] looks at the issue with a different. In the low transmit power state, the use of low mm-wave frequencies can achieve better security performance. On increasing the transmit power, a transition from the low mm-wave frequency to the high mm-wave frequency provides higher confidentiality. This is also in line with our experimental observations path loss is frequency dependent and more sensitive in high frequencies. Providing more secure bits needs to be considered when the power is increased.

Many asymmetric encryption schemes have been proposed for the one-way authentication problem identified by [10]. However, asymmetric cryptography is often considered to demanding in terms of processing power [8]. This is not a constraint on many occasions, such as desktop computers, but it is a serious problem in the increasingly growing wearable sensor networks that require low complexity, energy efficiency, and scalability.

The wireless body-centric communication is an open property to the wireless medium that makes it easy to be intercepted by an attacker or subject to spoofing. However, the body-centric fading channel is rich in user time-frequency features that introduce uncertainty and can contribute well to security. The standard layering method has many shortcomings, therefore, in order to guarantee the authenticity and confidentiality of wireless data transmission need physical layer security [17]. Traditional password security is based on the eavesdropper's lack of computing resources and ability to successfully attack the system. Moreover, the overhead associated with key management and distribution is huge.

Wireless body area network IEEE 802.15.6 standard aims to provide confidentiality, authentication, and privacy for the user. However, according to the protocol analysis in [23], the researchers are failed to find any instructions to ensure that this standard can provide the required security functions. In [17] a keyless authentication is proposed. In such a keyless scheme, certain characteristics of a particular channel between sending devices or legitimate users are utilized in order to authenticate the transmission. In particular, features are identified using the initial trusted transmission and then detected during the next transmission. Some of the authors' related health monitoring initial trust work can be seen in [36].

B. B-CSAI Security Analysis

A theoretical optimal solution is proposed in [38], which quantifies the necessary conditions for feasibility of certification to both parties. It shows that secure authentication is possible when the legitimate transmitter noise channel and receiver behavior cannot be completely simulated by the attacker. An interesting conclusion from the research on the statistical model of the body-centric channel is also useful [28] [39]. One type of uncertainty occurs in the actual measurement of the body center, due to changes in the radiation pattern of the transmitting and receiving antennas in the human body vicinity. In Fig. 5, when there are no pre-shared keys for legitimate parties making $R_k = 0$, signature is totally completed by the body-centric channel $Sign = Y\left(\Psi,\Pi\right)$. Security authorization is only possible if the attacker is not able to completely simulate the body-centric channel $Z^n \not\equiv Y^n$. Whilst the attacker cannot fully simulate the time-frequency characteristics of the copied body-centric channel. Thus, B-CSAI satisfy the secure certification requirements even from the strictest information theory point of view.

$$H\left(P_{\overset{\frown}{sign}}\middle|Y\left(\Psi,\Pi\right)\right) = H\left(P_{sign}\right) \tag{7}$$

From Eq. 7 and Fig. 5, we can see that the body-centric signature's main variable depends upon $\left(\Psi,\Pi\right)$, creeping wave Ψ and surface wave Π components. In this mm-wave time-frequency domain study, we are concerned with the B-CSAI having a wavelength of 11.1mm (@27 GHz) to 9.4mm (@32 GHz). The human body's influence is huge due to its comparatively very large electrical size. Even the hands, which are focus on this study, will impact the path loss exponent and shadowing factor greatly due to its large size.

Fig. 6 shows the apparent pathloss exponent and shadowing factor observation (First measurement data of three participants). There is a clear degree of change in either the time domain (S_{21}) or the frequency domain (phase). Sufficient body-centric related feature information is effectively extracted. The use of B-CSAI for signature authorization is similar to writing with different handwriting styles during a real time communication. In the experiment, the subjects are all bare handed to replicate real life scenarios. Gloves will change the channel response due to change in the electric properties of the human hand and hence, would be easily traceable.

More generally, positive trends can be seen in MAC address randomization in 802.11 systems, but physical layer security design in the more emerging 5G systems and future 802.11 (ai/aq/ax) has not yet been introduced [40]. In fact, the physical layer security technology with broad space will further consolidate the classic security. We can say that B-CSAI based on the time-frequency characteristics of the body centric can be used as an alternative to a solid, effective signature authorization guarantee.

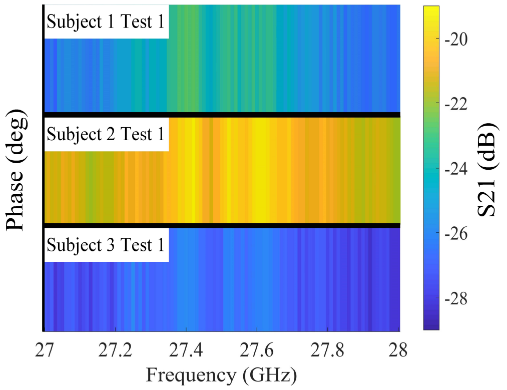


Fig. 6. Time-frequency characteristics of B-CSAI small sample.

In [41], link signature explores the use of rich channel characteristics, but the uncontrolled nature of the wireless environment can lead to loopholes. For example, the widely used assumption that the half-wavelength region is sufficient to remove the coupling between the attacker and the legitimate user. If the assumption failure, which can impact significantly in some studies. More specifically, the widely used half wavelength decorrelation assumption is established in a scattering-rich environment. From another point of view, this may be a problem for key agreement, but it is an advantage for signature authorization, which means more stable features, and the time-frequency characteristics of B-CSAI are mainly derived from the controllable user's hand palm. In the related work [39], the researchers have recommended careful investigation of the channel correlation in deployment environment, which has been done in Sections III. The same attention was paid to the work [42] that brought security enhancements from keystroke, and a careful examination of the possible authentication schemes for keystroke habits. It is a very interesting conclusion that the mobile device relies on the authentication scheme implemented by the key dynamics. The security performance is limited and it is not recommended to use at its own. Also, that keystrokes are biological characteristics of certain behavioral attributes but are not combined with intrinsic attributes of users, making the coupling with subjects rather weak. On the other hand, our proposed B-CSAI scheme is closely related to the composition of the user's hand (dielectric properties), which can effectively improve security.

V. Implementation and Evaluation

In this section, a detailed experimental implementation, comprehensive data acquisition, and analysis are presented to measure the efficacy of the proposed B-CSAI scheme.

A. Experimental Setup

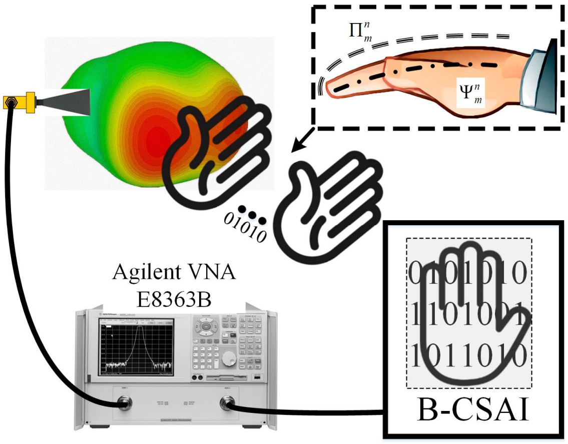


Fig. 7. Schematic diagram of body-centric time-frequency feature acquisition. The VNA is equipped with horn antennas to generate a directional beam to irradiate the hand palm, and obtains the B-CSAI original data, which containing rich feature information.

The measurement set-up for the body-centric channel observation is illustrated in Fig. 7. An Agilent E8363 Vector Network Analyzer is used to acquire frequency-domain data in multiple frequency bands (27-28 GHz, 29-30 GHz, and 31-32 GHz). In the middle of the receiving and sending channel, the human subject's right hand acts as the main scattering source. Although we only considered the right hand of the users, this approach is equally applicable to the left hand due to symmetry of the shapes and tissue properties. A total of 6 healthy volunteers participated in the experiment (including 5 males and 1 female, aged 25 to 30 years), and the main body local channel hand palm length ranged from 16 cm to 22 cm with an average of 19 cm. It is worth noting that as the initial confirmation of bornprint, it is appropriate to set a smaller number of subjects. Expanding the number of experimental samples will be carried out in further work. The signal received at the receiving port passes through the body-centric wireless channel coupling with hand's signature.

The Fig. 7 also illustrates potential contribution of the surface wave Π_m^n and the creeping wave Ψ_m^n components. For a very large number of application scenarios, the signature authorization system always has great interest in those characteristics, which can always generate reconstruction by itself properties. However, it is obvious that the quality of certification itself will be degraded as a result of continuous processing to content. Due to device dependencies, RF fingerprinting is a known and static input/output characteristic of the transmitter's RF chain, independent of time factors such as user's location, or channel propagation characteristics [37]. These are different from wireless channel based fingerprints. The channel fingerprint is a random mapping that does not depend on the transmitter characteristics and depends on the user's location and channel propagation characteristics. Therefore, wireless channel based authentication systems requires a strong premise assumption that users will remain stable, which makes them unsuitable in many practical situations. Undoubtedly, both two approaches have their own weaknesses, and the collection of physical features is expected to complement them well. It is to verify this theoretical derivation, we have designed and implemented experiments.

B. Data and Statistics

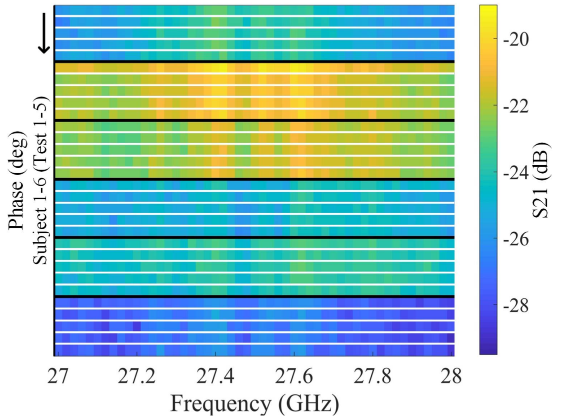


Fig. 8. Frequency and time domain data of multiple subjects in the 27-28 GHz band with 5 experiments (subject 1 test 1-5 from top to bottom according to arrows).

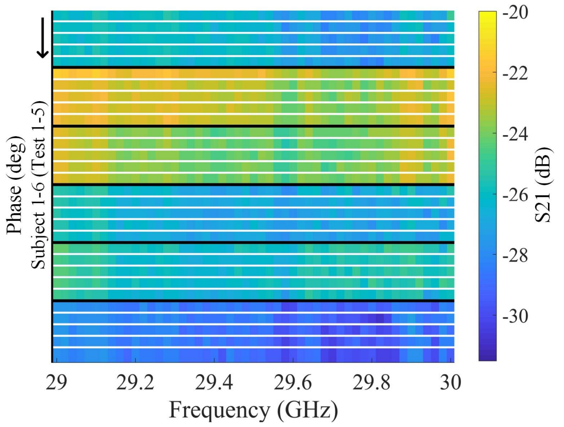


Fig. 9. Frequency and time domain data of multiple subjects in the 29-30 GHz band with 5 experiments (subject 1 test 1-5 from top to bottom according to arrows).

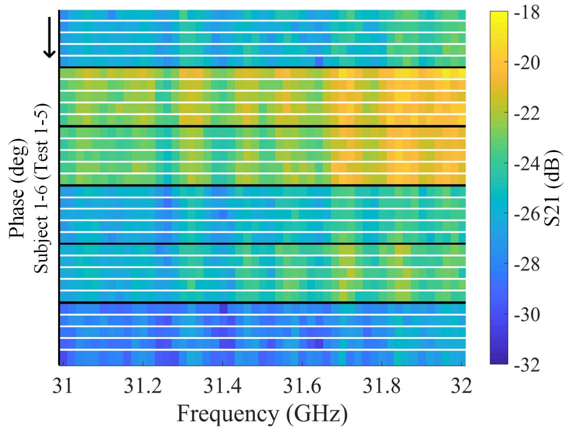


Fig. 10. Frequency and time domain data of multiple subjects in the 31-32 GHz band with 5 experiments (subject 1 test 1-5 from top to bottom according to arrows).

Fig. 8 shows the B-CSAI data for the six subjects in the 27-28 GHz band (subject 1 is at the top of the Y-axis). The data has been uniformly dimensioned and S21 is displayed in the same color gamut. Obviously, the basic strength has been greatly differentiated by the naked eye. In each row, 50 sample points are extracted with excellent reproducibility, both in the frequency domain and the time domain.

It is evident from Fig. 9 that high frequency (29-30 GHz) brings better discrimination between different subjects. More detailed points are coupled by the electromagnetic wave to be represented (a more subdivided detail change occurs compared to the small or similar color segments in Fig. 8). Fig. 10, using the highest frequency band (31-32 GHz), observation with even richer details is made. The gamut distribution is also the widest (color bar).

TABLE I
NET BODY LOSS IN MULTI-BAND B-CSAI

$\eta\,(dB)$	Test 1-5				
27-28 GHz Subject 1-6	-25.1	-25.1	-25.1	-25.1	-25.1
	-29.0	-28.3	-28.4	-28.4	-28.5
	-27.8	-27.7	-27.8	-27.9	-27.9
	-25.2	-25.0	-24.8	-25.0	-24.9
	-26.0	-25.8	-25.9	-25.8	-25.5
	-22.7	-22.8	-22.6	-22.6	-22.5
29-30 GHz Subject 1-6	-23.9	-23.9	-23.9	-23.9	-23.9
	-28.0	-27.3	-27.4	-27.4	-27.4
	-26.7	-26.6	-26.6	-26.7	-26.8
	-24.0	-23.8	-23.6	-23.8	-23.6
	-24.9	-24.5	-24.7	-24.7	-24.4
	-21.7	-21.8	-21.6	-21.6	-21.5
31-32 GHz Subject 1-6	-25.5	-25.5	-25.6	-25.5	-25.5
	-29.8	-29.0	-29.1	-29.1	-29.2
	-28.6	-28.5	-28.5	-28.7	-28.7
	-25.8	-25.7	-25.5	-25.6	-25.5
	-26.6	-26.3	-26.4	-26.4	-26.2
	-23.3	-23.4	-23.3	-23.2	-23.2

The net body loss, referred here as the B-CSAI radiation efficiency can be calculated from the total radiated power for the source in free-space (simulated or calculated by empirical formula) P_{FS} and enable P_{B-CSAI} in the body-centric network. Due to the gain of creeping and surface waves, the net body loss in practice will change, compared with free space. Therefore, B-CSAI radiation efficiency can be defined as:

$$\eta = \frac{P_{B-CSAI}}{P_{Free-Space}} \tag{8}$$

Table I shows that the calculated net body loss η from the Eq. 8 for the multi-band B-CSAI. The data has a high degree of autocorrelation for the same subject. For example, the first dataset for 27-28 GHz showing 5 tests of subject 1, net body loss is maintained at -25.1 dB. In the same frequency band, different subjects also have very good distinguishability, which is consistent with the time-frequency domain visualization diagrams in Figs. 8-10. It is numerical evidence of B-CSAI signature authorization good properties.

TABLE II
PATHLOSS EXPONENT AND SHADOWING FACTOR VALUES FOR DIFFERENT MULTI-BAND B-CSAI SUBJECTS

	Test 1-5 (Pathloss Exponent, Shadowing Factor)				
27-28 GHz Subject 1-6	(-0.50,0.99)	(-0.55,0.98)	(-0.53,0.98)	(-0.57,0.99)	(-0.49,0.99)
	(0.14,0.65)	(0.26,0.78)	(0.21,0.75)	(0.16,0.73)	(0.13,0.71)
	(0.61,0.58)	(0.69,0.59)	(0.67,0.58)	(0.59,0.57)	(0.62,0.57)
	(0.40,0.48)	(0.64,0.60)	(0.45,0.50)	(0.43,0.51)	(0.41,0.51)
	(0.60,0.48)	(0.63,0.47)	(0.65,0.50)	(0.81,0.52)	(0.79,0.51)
	(-0.48.0.65)	(-0.62.0.70)	(-0.59.0.68)	(-0.67.0.73)	(-0.68.0.73)
29-30 GHz Subject 1-6	(-1.65,0.74)	(-1.68,0.74)	(-1.58,0.70)	(-1.60,0.72)	(-1.59,0.71)
	(-1.15,0.61)	(-1.05,0.58)	(-1.11,0.61)	(-1.09,0.60)	(-1.03,0.61)
	(-0.38,0.61)	(-0.39,0.61)	(-0.42,0.61)	(-0.47,0.60)	(-0.44,0.58)
	(-0.76,0.63)	(-1.06,0.60)	(-0.98,0.62)	(-1.04,0.62)	(-0.99,0.63)
	(0.07,0.59)	(0.10,0.56)	(0.10,0.58)	(0.09,0.58)	(0.07,0.57)
	(-1.48,0.73)	(-1.51,0.72)	(-1.66,0.74)	(-1.57,0.75)	(-1.61,0.72)
31-32 GHz Subject 1-6	(2.36,1.12)	(2.47,1.16)	(2.41,1.14)	(2.29,1.09)	(2.40,1.15)
	(2.98,1.16)	(2.87,1.11)	(2.93,1.14)	(2.94,1.14)	(2.92,1.13)
	(3.50,1.31)	(3.44,1.29)	(3.35,1.27)	(3.34,1.27)	(3.43,1.29)
	(2.86,1.17)	(3.03,1.20)	(2.84,1.17)	(2.84,1.17)	(2.75,1.14)
	(3.53,1.30)	(3.21,1.21)	(3.49,1.29)	(3.50,1.30)	(3.50,1.30)
	(2.10,1.14)	(1.95,1.09)	(2.00,1.16)	(1.99,1.11)	(2.02,1.12)

Table II summarizes the path loss exponent and shadowing factor values for five independent signatures from six subjects. It can be seen that the six datasets for the same frequency band have good distinguishability. The two parameters also exhibits a good level of robustness and repeatability. Across the different frequency bands, the difference between the subjects is very obvious. From the sample statistics shown in Table II, it can be established that the shadowing factor of the same subject has a strong stability attribute. This has been theoretically illustrated in Fig. 2 of the Section III. The dispersion degree of the data itself is highly dependent on the subject's impact on the body-centric channel in terms of Ψ_m^n and Π_m^n.

C. *Security Evaluation*

As a natural extension, the attack paradigm to the B-CSAI is analyzed as shown in Fig. 5(b). Attackers can launch active attacks through two types of channels, similar device attacks from the source of the wireless signal, and disguised attacks from the time-frequency characteristics of the subject's physical center. For similar device attacks, an attacker cannot obtain a terminal device used by a legitimate user, and can only generate P_{sign} signal using the same type or similar hardware and perform subsequent attacks accordingly. For the disguised attack, the attacker may obtain legitimate equipment (social engineering attack, etc.), and only need to simulate the B-CSAI primary channel to perform the attack, such as:

$$Z(i)=\Psi_e(i)X(i)+\Pi_e(i) \tag{9}$$

For similar device attacks that require a high level of technology, an attacker could use RF signal waveform generator to simulate the B-CSAI feature or simply use the SDR as a generic platform to emulate a legal terminal device. Such attacks are often tentative, due to the enormous workload that scans and attempts to identify vulnerable nodes for more targeted intrusions. The signal acquired at this time is not $X(i)$, but is defined by the attacker. At this point, due to the double security standards of the possession (legal terminal equipment) and time-frequency characteristics of the physical center (hand palm), the attack cannot be established. The signature generated by the attacker cannot achieve authorization. For a more threatening disguised attack, the attacker may obtain P_{sign} or the encoded output X^n. At this time, the security based on the possession has been breached. In reality, due to the lost device, this scenario is entirely possible. Our B-CSAI time-frequency information now plays a key role. Because the body-centric loss that is closely coupled with the skin, fat, and muscles of the user's hand, from Eq. 5, the attacker cannot construct a suitable prosthesis, and therefore cannot implement forged signatures. For passive attacks, due to the high path loss in millimeter wave band (as shown in Table II) and the body-centric channel specificity, the attacker cannot monitor and obtain signature authorization features.

From the Section III single trial experiment and the Section IV security discussion, it is known that secure signature authorization is feasible if and only if the legitimate transmitter noise channel and receiver behavior cannot be fully simulated by the attacker. The presented analysis of time-frequency domain characteristics to the B-CSAI, fully satisfies this strict requirement from the perspective of information theory. B-CSAI also offers low complexity, energy efficiency, and scalability, these can equally be efficient in other paradigms of the wireless communication systems may all suitable. It is also effective in anti downgrade attacks due to the user specific physical attributes, as 2G-5G coexists for a long time and there are unknown security risks.

Radiometric fingerprinting is a recently explored technique that uniquely identifies wireless devices [25]. The basic assumption of a radiation fingerprinting based security scheme is that the unique characteristics of hardware cannot be copied or copied from one device to another, just as it is impossible to replicate human nature/behavior. The advantages of the solution are obvious. This type of signature scheme uses inherent hardware flaw features. It is difficult to deceive signatures by using off-the-shelf wireless devices. However, the disadvantages are also obvious. The signature scheme from radiation measurement can be used to simulate and replay attacks if the attacker is more powerful. Specifically, if an attacker is equipped with a software defined radio or high-end RF waveform generator, it can simulate radiation characteristics. In addition, such schemes are only applicable to static situations, meaning that signal properties can be reliably extracted without being affected by other factors such as mobility or interference.

The time-frequency characteristics of the body-centric channel and the nature of the dielectric structure of the individual person increase the degree of isolation at the time of signature authorization effectively. Hardware-based security solutions can always suffer higher-level technical threats, but combining the essential characteristics of the human body can effectively overcome this hidden danger. Regarding the moving situation, such problems do exist at low frequencies such as the S band, due to the characteristics of the radio wave propagation. The B-CSAI implements signatures for hand-held cellphone scenes at high frequencies for 5G and beyond applications. The length of 11.1mm (27 GHz) to 9.4mm (32 GHz) is also a fist-long even if it is expanded ten times. In fact, the above experiments did not require the subjects to remain still. Fig. 8-10 and Tables I-II confirm the robustness of the scheme.

Another common problem with existing physical layer signature schemes requires expensive RF analyzers to map and verify radiometric signatures. The widespread deployment of expensive vector network analyzers in unsafe and harsh physical environments is not feasible. There have been gratifying advances to deal with this problem though. Liu et al. [43] have implemented a practical Ka-band antenna-in-package structure and discussed the antenna element design and implementation tradeoffs. High-frequency antenna packages and radio wave transceivers are optimized, at the same time. More specifically, Gu et al. [44] have produced an organic based multi-layered phased-array antenna package in 28 GHz for 5G radio access applications. These industrial advances and device miniaturization have eliminated technical obstacles to the B-CSAI practical application in near-future applications. However, more practical scenarios would be considered in our following studies to explore the full potential of this scheme.

VI. Conclusion

A new body-centric time-frequency signature authorization technique for health monitoring B-CSAI has been proposed, and validated by radio wave propagation model and security analysis. The identity-based attacks are considered to be the first step in an intruder's attempt to launch various attacks. From the information theory view, theoretical discussions suggest that secure certification is possible when the behavior of the legitimate transmitter cannot be completely simulated by the attacker. It is shown through detailed experimental observations of physical centric wave modeling that body-centric radiation performances are subject-specific. Although the fading curve of the channel magnitude statistical perspective can be obtained, each user's unique time-frequency domain variation cannot be simulated and replicated by others. This is due to the contribution of creeping waves and surface waves over the human body that would be highly dependent on the shape and composition of the body tissues. Hence, distinct for each user which undoubtedly satisfies the basic condition of the security signature and shows that our proposed B-CSAI have great potential, especially for IEEE 802.15.6 protocol with extremely high security risk.

A detailed measurement campaign is carried out to evaluate the performance of time-frequency channel response and radiation efficiency, employing 6 human subjects. The statistical analysis has shown that the proposed technique offers a high degree of correlation within the same frequency band (with a difference of the order 0.01) and exhibits excellent repeatability. This research just presented initial results as a proof of concept. To obtain a generalized path loss probability security model, it is necessary to provide different people with accurate link budget assessments. A thorough investigation of changes in body shape and clothing path loss will be carried out as an extension of this study. We have not seen publications dealing with this issue, so we cannot give a comparative analysis of performance. Finally, although the security necessary conditions are not falsifiable, further studies are always necessary.

ACKNOWLEDGMENTS

The authors would like to thank the anonymous reviewers and the associate editor for their valuable comments on the paper, which enriches the content of the work.

REFERENCES

[1] A. K. Triantafyllidis, C. Velardo, D. Salvi, S. A. Shah, V. G. Koutkias and L. Tarassenko, "A Survey of Mobile Phone Sensing, Self-Reporting, and Social Sharing for Pervasive Healthcare," in IEEE Journal of Biomedical and Health Informatics, vol. 21, no. 1, pp. 218-227, Jan. 2017.

[2] F. Meneghello, M. Calore, D. Zucchetto, M. Polese and A. Zanella, "IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8182-8201, Oct. 2019.

[3] I. c. Jeong, D. Bychkov and P. C. Searson, "Wearable Devices for Precision Medicine and Health State Monitoring," in IEEE Transactions on Biomedical Engineering, vol. 66, no. 5, pp. 1242-1258, May 2019.

[4] M. Zhang, A. Raghunathan and N. K. Jha, "MedMon: Securing Medical Devices Through Wireless Monitoring and Anomaly Detection," in IEEE Transactions on Biomedical Circuits and Systems, vol. 7, no. 6, pp. 871-881, Dec. 2013.

[5] M. Seyedi, B. Kibret, D. T. H. Lai and M. Faulkner, "A Survey on Intrabody Communications for Body Area Network Applications," in IEEE Transactions on Biomedical Engineering, vol. 60, no. 8, pp. 2067-2079, Aug. 2013.

[6] D. He, S. Chan, Y. Zhang and H. Yang, "Lightweight and Confidential Data Discovery and Dissemination for Wireless Body Area Networks," in IEEE Journal of Biomedical and Health Informatics, vol. 18, no. 2, pp. 440-448, March 2014.

[7] Poor, H. Vincent, and Rafael F. Schaefer. "Wireless physical layer security." Proceedings of the National Academy of Sciences 114.1 (2017): 19-26.

[8] A. Mukherjee, "Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality Under Resource Constraints," in Proceedings of the IEEE, vol. 103, no. 10, pp. 1747-1761, Oct. 2015.

[9] E. Martinian, G. W. Wornell and B. Chen, "Authentication with distortion criteria," in IEEE Transactions on Information Theory, vol. 51, no. 7, pp. 2523-2542, July 2005.

[10] W. Diffie and M. Hellman, "New directions in cryptography," in IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654, Nov 1976.

[11] Q. Jiang, X. Huang, N. Zhang, K. Zhang, X. Ma and J. Ma, "Shake to Communicate: Secure Handshake Acceleration-Based Pairing Mechanism for Wrist Worn Devices," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 5618-5630, June 2019.

[12] P. A. Regalia, A. Khisti, Y. Liang and S. Tomasin, "Secure Communications via Physical-Layer and Information-Theoretic Techniques," in Proceedings of the IEEE, vol. 103, no. 10, pp. 1698-1701, Oct. 2015.

[13] K. Kittichokechai and G. Caire, "Secret Key-Based Identification and Authentication With a Privacy Constraint," in IEEE Transactions on Information Theory, vol. 62, no. 11, pp. 6189-6203, Nov. 2016.

[14] N. Zhang, Y. Zang, X. Yang, X. Jia and J. Tian, "Adaptive Orientation Model Fitting for Latent Overlapped Fingerprints Separation," in IEEE Transactions on Information Forensics and Security, vol. 9, no. 10, pp. 1547-1556, Oct. 2014.

[15] J. Zheng, J. Tian, K. Deng, X. Dai, X. Zhang and M. Xu, "Salient Feature Region: A New Method for Retinal Image Registration," in IEEE Transactions on Information Technology in Biomedicine, vol. 15, no. 2, pp. 221-232, March 2011.

[16] Y. Zhu, L. Wang, K. K. Wong and R. W. Heath, "Secure Communications in Millimeter Wave Ad Hoc Networks," in IEEE Transactions on Wireless Communications, vol. 16, no. 5, pp. 3205-3217, May 2017.

[17] E. Jorswieck, S. Tomasin and A. Sezgin, "Broadcasting Into the Uncertainty: Authentication and Confidentiality by Physical-Layer Processing," in Proceedings of the IEEE, vol. 103, no. 10, pp. 1702-1724, Oct. 2015.

[18] P. S. Hall et al., "Antennas and propagation for on-body communication systems," in IEEE Antennas and Propagation Magazine, vol. 49, no. 3, pp. 41-58, June 2007.

[19] M. Ur Rehman, Y. Gao, Z. Wang, J. Zhang, Y. Alfadhl, X. Chen, C.G. Parini, Z. Ying, T. Bolin and J.W. Zweers, "Investigation of on-body bluetooth transmission", IET Microwaves, Antennas and Propagation, Vol. 4, No. 7, Jul. 2010.

[20] Y. Hao, A. Brizzi, R. Foster, M. Munoz, A. Pellegrini and T. Yilmaz, "Antennas and propagation for body-centric wireless communications: Current status, applications and future trend," 2012 IEEE International Workshop on Electromagnetics: Applications and Student Innovation Competition, Chengdu, Sichuan, 2012, pp. 1-2.

[21] M. Ur Rehman, Q.H. Abbasi, M. Akram and C.G. Parini, "Design of band-notched UWB antenna for indoor and wearable wireless communications", IET Microwaves, Antennas & Propagation, Vol. 9, No. 3, Feb. 2015.

[22] Q.H. Abbasi, M. Ur Rehman, A. Alomainy and K. Qaraqe (Ed.), "Advances in Body-Centric Wireless Communication: Applications and State-of-the-art", The IET (UK), 2016

[23] Toorani, Mohsen. On Vulnerabilities of the Security Association in the IEEE 802.15.6 Standard. Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2015:245-260.

[24] M. Ur Rehman, N.A. Malik, X. Yang and Q.H. Abbasi, "A low profile antenna for millimetre-wave body-centric applications", IEEE Transactions on Antennas and Propagation, Vol. 65, No. 12, pp.6329-6337, Dec. 2017.

[25] K. Zeng, K. Govindan and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks [Security and Privacy in Emerging Wireless Networks]," in IEEE Wireless Communications, vol. 17, no. 5, pp. 56-62, October 2010.

[26] Konstantina S. Nikita, "Security and Privacy in Biomedical Telemetry: Mobile Health Platform for Secure Information Exchange," in Handbook of Biomedical Telemetry, Chapter 13, IEEE, 2014, pp 384.

[27] H. Kim and E. A. Lee, "Authentication and Authorization for the Internet of Things," in IT Professional, vol. 19, no. 5, pp. 27-33, 2017.

[28] N. Zhao et al., "Authentication in Millimeter-Wave Body-Centric Networks Through Wireless Channel Characterization," in IEEE Transactions on Antennas and Propagation, vol. 65, no. 12, pp. 6616-6623, Dec. 2017.

[29] Campisi, Patrizio. "Security and Privacy in Biometrics" Springer, 2013.

[30] A. Yener and S. Ulukus, "Wireless Physical-Layer Security: Lessons Learned From Information Theory," in Proceedings of the IEEE, vol. 103, no. 10, pp. 1814-1825, Oct. 2015.

[31] A. Sani, A. Alomainy and Y. Hao, "Numerical Characterization and Link Budget Evaluation of Wireless Implants Considering Different Digital Human Phantoms," in IEEE Transactions on Microwave Theory and Techniques, vol. 57, no. 10, pp. 2605-2613, Oct. 2009.

[32] Q. H. Abbasi, A. Sani, A. Alomainy and Y. Hao, "Numerical Characterization and Modeling of Subject-Specific Ultrawideband Body-Centric Radio Channels and Systems for Healthcare Applications," in IEEE Transactions on Information Technology in Biomedicine, vol. 16, no. 2, pp. 221-227, March 2012.

[33] O. G. Martinsen, S. Clausen, J. B. Nysaether and S. Grimnes, "Utilizing Characteristic Electrical Properties of the Epidermal Skin Layers to Detect Fake Fingers in Biometric Fingerprint Systems—A Pilot Study," in IEEE Transactions on Biomedical Engineering, vol. 54, no. 5, pp. 891-894, May 2007.

[34] A. F. Demir et al., "Anatomical Region-Specific In Vivo Wireless Communication Channel Characterization," in IEEE Journal of Biomedical and Health Informatics, vol. 21, no. 5, pp. 1254-1262, Sept. 2017.

[35] M. Ur Rehman, M. Adekanye and Hassan Tariq Chattha, “Tri-band millimetre-wave antenna for body-centric networks”, Journal of Nano Communication Networks, Vol. 18, pp 72-81, Dec. 2018.

[36] N. Zhao et al., "Double Threshold Authentication Using Body Area Radio Channel Characteristics," in IEEE Communications Letters, vol. 20, no. 10, pp. 2099-2102, Oct. 2016.

[37] O. Gungor and C. E. Koksal, "On the Basic Limits of RF-Fingerprint-Based Authentication," in IEEE Transactions on Information Theory, vol. 62, no. 8, pp. 4523-4543, Aug. 2016.

[38] S. Jiang, "Keyless Authentication in a Noisy Model," in IEEE Transactions on Information Forensics and Security, vol. 9, no. 6, pp. 1024-1033, June 2014.

[39] A. Brizzi, A. Pellegrini, L. Zhang and Y. Hao, "Statistical Path-Loss Model for On-Body Communications at 94 GHz," in IEEE Transactions on Antennas and Propagation, vol. 61, no. 11, pp. 5744-5753, Nov. 2013.

[40] H. Rahbari and M. Krunz, "Secrecy beyond encryption: obfuscating transmission signatures in wireless communications," in IEEE Communications Magazine, vol. 53, no. 12, pp. 54-60, Dec. 2015.

[41] X. He, H. Dai, W. Shen, P. Ning and R. Dutta, "Toward Proper Guard Zones for Link Signature," in IEEE Transactions on Wireless Communications, vol. 15, no. 3, pp. 2104-2117, March 2016.

[42] P. Campisi, E. Maiorana, M. L. Bosco and A. Neri, "User authentication using keystroke dynamics for cellular phones," in IET Signal Processing, vol. 3, no. 4, pp. 333-341, July 2009.

[43] D. Liu, X. Gu, C. W. Baks and A. Valdes-Garcia, "Antenna-in-Package Design Considerations for Ka-Band 5G Communication Applications," in IEEE Transactions on Antennas and Propagation, vol. 65, no. 12, pp. 6372-6379, Dec. 2017.

[44] X. Gu et al., "A multilayer organic package with 64 dual-polarized antennas for 28GHz 5G communication," 2017 IEEE MTT-S International Microwave Symposium (IMS), Honolulu, HI, 2017, pp. 1899-1901.

Nan Zhao received the B.Eng. and Ph.D. degrees from Xidian University, Xi'an, China, in 2017 and 2020, respectively. He is currently with the Xidian University, China, as a Lecture. His research interests include body-centric communication, biometrics, and bornprint.

Zhi-Ya Zhang was born in Jiangsu, China, in 1985. He received his B.S. degree in electrical engineering and and Ph.D. degree in electromagnetic field and microwave technology from the Xidian University, Xi’an, China, in 2007 and 2012, respectively. He works as an associate professor in the National Key Laboratory of Antennas and Microwave Technology, Xidian University, Xi’an, China. His current research interests include broadband antennas, millimeter-wave antennas, and antenna arrays.

Xiaodong Yang has published over 100 papers in peer-reviewed journals. His main research area is Body Area Networks. Dr. Yang received the Young Scientist Award from the International Union of Radio Science in 2014. He is on the editorial board of several IEEE and IET journals. He has a global collaborative research network in the related fields. He is a Senior Member of IEEE.

Aifeng Ren was born in Hebei, China, on Nov 1, 1974. He received his B.S. degree in Automatic Control and M.S. degree in Circuit and System from XiDian University, He received his Ph.D. degree in Information and Telecommunication Engineering from Xi’an JiaoTong University. He currently works as an Associate Professor with the School of Electronic Engineering, XiDian University, Xi’an, China. His research interests include signal and image processing, complex brain network, and embedded wireless sensor networks. He has published many papers in some leading journals and conferences.

Jianxun Zhao (Member, IEEE) received the B.S. degree in radio techniques from Xi’an Jiaotong University, Xi’an, China, in 1995, the M.S. degree in bioelectronics from Xidian University, Xi’an, in 1998, and the Ph.D. degree in radio physics from Shanghai University, Shanghai, China, in 2002. In 2002, he joined the School of Electronic Engineering, Xidian University, where he is currently a Professor with the Department of Biomedical Engineering. Since 2007, he has been in charge of the national funded project “Research on the Experimental Dosimetry for In Vitro Study on Effects of Electromagnetic Exposure.” He has authored or co-authored over 30 international journal and conference articles on bioelectromagnetics and ten books concerning signal detection and estimation, electronics, and RF circuits. His current research interests include electromagnetics, electronics, software and hardware development for accurate and efficient time-domain computation, exposure apparatus for dosimetry study, and smart antenna systems for biomedical applications.,Dr. Zhao is a Senior Member of the Biomedical Engineering Society of China.

Masood Ur Rehman (SM’16) received the B.Sc. degree in electronics and telecommunication engineering from University of Engineering and Technology, Lahore, Pakistan in 2004 and the M.Sc. and Ph.D. degrees in electronic engineering from Queen Mary University of London, London, UK, in 2006 and 2010, respectively. He worked at Queen Mary University of London as a Post-doctoral Research Assistant till 2012 before joining the Centre for Wireless Research at University of Bedfordshire, University Square, Luton, UK, as a Lecturer. He is now with the School of Engineering, University of Glasgow, Glasgow G12 8QQ, UK. His research interests include compact antenna design, radiowave propagation and channel characterization, satellite navigation system antennas in cluttered environment, electromagnetic wave interaction with human body, body-centric wireless networks and sensors, remote health care technology, mmWave and nano communications for body-centric networks and D2D/H2H communications. He has worked on a number of projects supported by industrial partners and research councils. He has contributed to a patent and authored/co-authored 4 books, 7 book chapters and more than 75 technical articles in leading journals and peer reviewed conferences. Dr. Ur Rehman is a Fellow of the Higher Education Academy (UK), a member of the IET and part of the technical program committees and organizing committees of several international conferences, workshops and special sessions. He is acting as an Associate Editor of the IEEE Access and Lead Guest Editor of numerous special issues of renowned journals. He also serves as a reviewer for book publishers, IEEE conferences and leading journals.