IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 3, 2019, accepted May 27, 2019, date of publication June 10, 2019, date of current version June 28, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2921822

MBPSKA: Multi-Biometric and Physiological Signal-Based Key Agreement for Body Area Networks

MANA AL RESHAN[1,2], **HANG LIU**[1], **(Senior Member, IEEE)**, **CHUNQIANG HU**[1,3], **(Member, IEEE)**, **AND JIGUO YU**[4]

[1]Department of Electrical Engineering and Computer Science, The Catholic University of America, Washington, DC 20064, USA
[2]College of Computer Science and Information System, Najran University, Najran 55461, Saudi Arabia
[3]School of Big Data and Software Engineering, Chongqing University, Chongqing 400044, China
[4]School of Computer Science and Technology, Qilu University of Technology, Jinan 250353, China

Corresponding author: Mana Al Reshan (06alreshan@cua.edu)

ABSTRACT A body area network (BAN) consists of wireless sensors and actuators deployed on a patient's body for real-time health monitoring and personalized medical care. It is essential and challenging to secure wireless communications in a BAN to protect the patient's privacy while also allowing the authorized healthcare practitioners (e.g., emergency room doctors and nurses) to easily communicate with and configure the BAN devices transparent to the patient or even when the patient loses consciousness. With the existing schemes, the devices are based on a pre-installed secret password or a physiological signal feature to authenticate each other and to agree upon a cryptographic key for secure communications. The former requires a patient's input to access and configure the BAN, and the latter is not sufficiently reliable or secure due to signal dynamics. This motivates us to design a new key agreement scheme in this paper, called multi-biometric and physiological signal-based key agreement (MBPSKA), to achieve more secure and reliable authentication and communication session establishment between the BAN devices while providing flexibility to authorized personnel to access, control, and adjust the BAN without patient involvement. The proposed scheme exploits both the reliable biometric traits and the time-variant physiological signal features of a patient along with the efficient fuzzy crypto-algorithms and key distribution protocols. The devices use multiple biometric and physiological features for mutual authentication and cryptographic key protection. We analyze the security characteristics of MBPSKA, including its capabilities against various attacks. Our evaluation results using the real-world datasets demonstrate that MBPSKA outperforms the existing physiological signal-based key agreement schemes in terms of security, authentication reliability, and accuracy.

INDEX TERMS Body area network, secure communication, key agreement, biometric-based security, physiological signal.

I. INTRODUCTION

With the advances in wireless sensor and Internet of Things (IoT) technologies, numerous new applications are emerging, including those in healthcare and telemedicine. A body area network (BAN) is a network of wireless sensors and actuators worn on or implanted in one's body to monitor physiological signals and perform certain medical procedures [1]–[6]. It enables pervasive real-time health management and allows medical practitioners to perform timely diagnosis and treatment on patients [7]. BANs offer tremendous opportunities to broaden access to medical care, improve healthcare quality, reduce costs, and enhance public health. Note that for ease of explanation, we use the terms "sensor" and "device" interchangeably in this paper. Given the sensitive nature of the personal health data they deal with, BANs require strict security and privacy. A lack of security will not only cause patient privacy violations and legal liability but also pose risks and compromise patient safety, potentially leading to catastrophic consequences [8].

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

For example, the wrong diagnosis may be made if the patient data are modified by adversaries [9]. Wireless communications between the body sensors in a BAN are especially vulnerable to numerous security breaches or attacks. Securing inter-sensor data transfer plays a critical role in the BAN security. The sensors in a BAN should authenticate each other and agree upon a cryptographic key to establish a secure communication session for data confidentiality and integrity.

In addition, a BAN should be easily accessible by the authorized personnel without the patient's involvement while maintaining a high security. For example, doctors and nurses in an emergency room should be able to communicate with, add, remove and adjust the sensors on a patient's BAN even when the patient loses consciousness and cannot communicate with them. Secure, reliable, and flexible schemes are needed for mutual authentication and key agreement to enable secure communications between the sensors within a BAN.

Conventionally, to secure the communications in a BAN, the sensors need to be configured with a master key, password, or other shared secret before deployment, and then a key distribution protocol is used for the sensors to agree on a session key based on the pre-shared secret [10]–[15]. This approach is inflexible and requires the input of the patient or body sensor network administrator during network setup or any subsequent adjustments. Asymmetric cryptosystems such as Diffie-Hellman and its variants [16]–[18] have been proposed to avoid the pre-shared secret. However, they are prone to well-known man-in-the-middle attacks and require additional authentication mechanisms.

Recently, several physiological signal-based key agreement (PSKA) schemes for secure inter-sensor communication channel establishment have been proposed [19]–[22]. Although these schemes are different in use of physiological features, signal processing, and key delivery methods as discussed in the Related Work section, they follow the same principles. Two sensors at different parts of the body measure and extract secret features from physiological signals (e.g., photoplethysmograms (PPG) and electrocardiograms (ECG or EKG)) and use these features to agree upon a symmetric cryptographic key in an authenticated manner with a fuzzy cryptographic algorithm [23]. The PSKA protocols are based on the observation that the human body is dynamic and complex and that the physiological state of a subject is unique at any given time. Only two sensors on the same subject at the same time can obtain similar physiological features and use these unique features for mutual authentication and pairwise key agreement. The pre-configuration and distribution of secret key materials to the sensors are not required for the PSKA schemes. They are transparent to the patient. A sensor can simply be deployed in a BAN, and then can authenticate and establish secure communications with other sensors using the PSKA protocols. However, the security level of these schemes is not sufficiently high and they yield large false positive or false negative authentication rates due to the reliability and accuracy limitations placed on them by the feature dynamics, as analyzed later in the paper. In addition, when a single type of physiological signal is used, there is a risk that the entire system will be compromised if the attacker can obtain the physiological signal.

Authentication schemes using biometrics that employ a biometric feature, such as a fingerprint, iris, retina, and face, as a form of identification to authenticate a user and control access to a device have been widely studied [24]–[26], e.g., allowing a user to unlock his smartphone. Multi-biometric-based user authentication systems have also been proposed to improve the security performance [27]. However, physiological signal-based key agreement schemes in a BAN are fundamentally different from biometric user authentication systems in the following ways. 1) Biometric features such as fingerprints are unique to individuals and are invariant over time, i.e., the fingerprints of a person will not change with time. User authentication with biometric systems is based on whether there is a close match between the biometric sample presented by a person and the original template stored in the database. The two biometric measurements can occur at different times. Physiological signal-based features not only recognize the distinctiveness between individuals but also show temporal variance for the same person. The former ensures that only sensors on the same BAN can authenticate each other and agree on a shared key. The latter requires that the two sensors use a loosely synchronized measurement of physiological signals on the same subject to be successful in the authentication and key agreement process. Contrary to the possibility of using a forged fingerprint, the knowledge of the physiological signals at a given time will not help an attacker obtain or compromise any past or future keys agreed upon between the sensors. 2) The algorithms used for biometric-based user authentication are different from those for physiological signal-based key agreement schemes. The former compares the biometric sample of a subject with a stored identity template. Fuzzy commitment [28] and fuzzy vault [23] are two popular fuzzy biometric crypto-algorithms used to determine the closeness of a match for a successful authentication. However, the latter requires an efficient communication protocol between two sensors to exchange messages, in addition to fuzzy crypto-algorithms, to authenticate each other and establish a secure session. 3) Biometric-based authentication systems are more accurate and reliable for verifying an identity; in particular, the system performance can be significantly improved by using multiple biometric identifiers [27]. However, if one's biometric data, (e.g., fingerprints) are disclosed and forged, system's security will be compromised. One approach to mitigate the damage due to potential data disclosure and protect the privacy is to store the processed biometric identifier instead of the original biometric data. For example, the fingerprint features are extracted to generate a biometric identifier(i.e., a fixed-length binary string that is stored in the sensors). Even if the sensors are hacked, the original biometric data will not be leaked.

In this paper, we design a new key agreement scheme, termed Multi-Biometric and Physiological Signal-based Key Agreement (MBPSKA), to achieve more secure and reliable authentication and communication session establishment between the BAN devices while providing flexibility to caregiver or authorized personnel to access, control and adjust the BAN without patient involvement. The proposed design exploits both the reliable biometric traits and the time-variant physiological signal features of a subject along with efficient fuzzy crypto-algorithms and key distribution protocols. The devices use multiple biometric and physiological features for mutual authentication and cryptographic key protection to enhance BAN security performance. The main contributions of the paper are outlined as follows:

1) We propose MBPSKA, a secure and efficient scheme for mutual authentication and key agreement between sensors in a BAN based on biometric features and physiological signals without requiring the direct involvement of the subject.
2) We analyze the security characteristics of MBPSKA, including its capability of withstanding various attacks such as eavesdropping, brute force attacks, replay attacks, and man-in–the-middle attacks.
3) We evaluate and compare the performance of MBPSKA to that of the existing physiological signal-based key agreement schemes using the actual data sets of the most popular biometric feature, fingerprints, and the physiological signals from an electrocardiogram database. Our evaluation results show that MBPSKA outperforms the existing PSKA schemes in terms of security, authentication reliability (false positive rates), and accuracy (false negative rates).

The remainder of this paper is organized as follows. In Section II, the related work is overviewed. In Section III, the system model is presented. The detail design of MBPSKA is described in Section IV, followed by its security analysis and performance evaluation in Section V and Section VI, respectively. Finally, the conclusions are given in Section VII.

II. RELATED WORK

A variety of issues related to the security of wireless BANs have been studied in the literature, including potential security risks in practical applications of BANs [29]–[32], feature extraction from biometric data and physiological signals [20], [33]–[36], authentication, access control, key management, and encryption [37]–[46]. A crucial aspect of BAN security is device authentication and cryptographic key distribution for secure communications between sensors in a BAN. Wearable medical sensors generally have constrained computation capability and battery capacity. Many lightweight cryptographic mutual authentication and key agreement schemes have been proposed. An efficient multilayer authentication and secure session key generation scheme was recently designed based on the BAN network structure [47], which consists of a one-to-many group authentication and group key establishment algorithm between a hub node and each of the sensor nodes as well as an authentication protocol using the elliptic-curve cryptography (ECC) between the hub node and application provider. A lightweight anonymous mutual authentication and key agreement scheme for wireless BANs is proposed in [48] that allows sensors to authenticate with the local hub node and to establish a session key anonymously. The above algorithms had much lower computational and energy requirements than prior algorithms. Chen *et al.* [49] designed an mutual authenticated key agreement scheme for wearable sensors in wireless BANs that further improves the security of [48] against sensor node impersonation attack and hub node spoofing attack using a two-party protocol through a pairwise secret. However, these cryptography-based schemes require pre-configuration of the BAN devices with some form of secret credential materials, e.g., a password or a key that are not transparent to users [10]–[15].

Fuzzy cryptographic techniques have been proposed, which allow a witness that is close to the original encrypting witness in a suitable metric, but not necessarily identical to it, to decrypt the message [50], [51]. The error-tolerant characteristic of fuzzy cryptographic algorithms makes them suitable when using biometric data or physiological signals as inputs to cryptographic techniques for authentication and encryption because such data are subject to noise and two samples of the same person's biometric features or physiological signals are not completely identical. Fuzzy commitment [28] and fuzzy vault [23] are two popular fuzzy cryptographic algorithms that are based on the combined use of cryptography and error correction codes. For a fuzzy commitment system, a secret value can be concealed or committed with a set of elements that may be obtained from a person's biometric features or physiological signals. The secret value can be decommitted using a set of elements sufficiently close to the original set. The fuzzy commitment scheme requires that the set of elements used for decommitting maintain the same order as the set of committing elements. The fuzzy vault scheme has an order invariance property but incurs much higher computation complexity and storage/bandwidth overhead than the fuzzy commitment scheme [23], [36].

Physiological signals were employed for secure intersensor communications for BANs [52], [53], where the features derived from a physiological signal simultaneously measured at different parts of the body were directly used to generate the actual key shared between the sensors. The direct use of ECG for key generation was studied in [54], in which the sensors generated frequency domain features from the ECG and then exchanged them to generate common keys. However, the way that the features were extracted during the process tended to distort the original signal and cause errors [20]. In [52], it was proposed that the Interpulse Interval (IPI) feature of the ECG could be encoded into a 128-bit binary key for secure communications. IPIs could be extracted from the time interval between the R-wave of the ECG signals and the foot of the PPG pulses. However, this approach does not work well because translational and rotational errors can produce drastically different values when IPIs are naively encoded into binary. Even though error correction and fuzzy commitment techniques were used to correct the differences between the physiological features generated by different sensors on the same human body to achieve a common key, such a scheme is still not practical because the features in the time domain are susceptible to strict synchronization and reordering issues [19]. In addition, the Hamming distance of the keys generated between two sensors belonging to the same human body is not remarkably lower than that generated by sensors on different human bodies [52].

In [21], two more complex ECG-based cryptographic key generation approaches are proposed. One method is to use a pseudo-random number and consecutive IPI sequences to derive a secure key on the fly without requiring key predistribution; the other method is to utilize IPI as the seed generator in the Advanced Encryption Standard (AES) algorithm. The authors in [55] evaluated the strength of IPI-based security keys and investigated several aspects that should be considered in practice. They introduced an inter-multi-pulse interval (ImPI) method, extracting entropy and deriving the key by considering the time difference between nonconsecutive heartbeats. These more complex methods increase key strength in comparison to the conventional methods simply relying on IPIs, however, the execution times required to generate the cryptographic keys are increased. In [56], a method to improve the key generation time from ECG is proposed by implementing a multiple fiducial-points based binary sequence generation (MFBSG) algorithm, which detects the arrival time of the multiple ECG fiducial points, such as P, Q, R, S, and T peaks through discrete wavelet transforms and calculates the time intervals between them to form five feature representations from one heartbeat cycle and combine them for creating the security key. This algorithm can intrinsically be up to five times faster than the solely IPI-based methods. However, the algorithm may not perform optimally with irregular heartbeats. In addition, the total processing and encoding time is increased.

To address the limitations of direct key generation from ECG signals, several schemes such as physiological-signal-based key agreement (PSKA) plethysmograms, and Ordered-Physiological-Feature-based Key Agreement (OPFKA) [19], [20], [22], [57], have been proposed. These schemes focus on using physiological signal features for key delivery, rather than key generation, in which a key distribution protocol employs the extracted physiological signal features to securely transport a session key between two sensors. A sensor generates a random key and hides it using physiological signal features and sends the hidden key to another sensor that un-hides the key using its own features. Fuzzy vault or similar schemes have been utilized to deal with the fact that physiological signals have similar trends but are not completely identical. However, these schemes are not very reliable and have high false positive and false negative rates due to the dynamic nature of physiological signals which results in the reliability and accuracy limitations. The strength of their security is limited and depends on the vault size. The complexity of breaking the vault increases if the number of chaff points in the vault, i.e. the vault size, increases. Conversely, an increase in the vault size can cause high bandwidth overhead and introduce collisions between the features generated by one sensor and the chaff points generated by another sensor, which can lead to a false rejection.

Biometric-based authentication systems using fingerprints or iris images have been developed and studied [26], [58]. These systems employ the fuzzy commitment and fuzzy vault techniques to determine the degree of the match between the biometric sample presented by the subject and the original template stored to authenticate the subject. Non-variant biometric templates are more reliable and accurate for authentication. However, they expose users to attacks involving template modification [59]. Biometric user authentication systems based on multiple types of biometric features have been proposed to enhance the level of security [27] that allow the disclosure of some biometric traits without destroying biometric privacy [60]. However, these systems are more complex and their security performance depends on the model and algorithms used to incorporate the multiple biometric features. In addition, biometric features do not change with time. As shown in [61], correlation attacks against these schemes may occur. For example, an attacker can intercept two fuzzy vaults generated from the same biometric data with different chaff points and correlate them to reveal the hidden biometric features. These attacks are not possible with schemes using physiological signal features because the feature values in the fuzzy vaults generated in two iterations are significantly different due to the temporal variance property of the physiological signals used. Therefore, trying to tamper with a physiological signal-based vault or correlate two vaults will not yield the attacker any key information.

In this paper, we propose a multi-biometric and physiological signal-based key agreement scheme that takes advantage of both types of features by combining the more reliable time-invariant biometric identifiers and the time-variant physiological signals to improve BAN security without sacrificing flexibility and transparency when accessing and modifying the BAN.

III. SYSTEM MODEL

We consider a BAN that consists of implanted or wearable physiological sensing devices on a human subject. These sensors are capable of collecting the health and contextual information of a human body at regular intervals and transmitting the information to a sink node over a multi-hop wireless network. The sink node may process the information further and send it to outside devices or to the Internet. Given advances in electronics, many medical devices are multimodal with the capability to sense multiple types of signals and perform multiple actions. Thus, some of the sensors may also be able to receive commands and perform medical procedures.

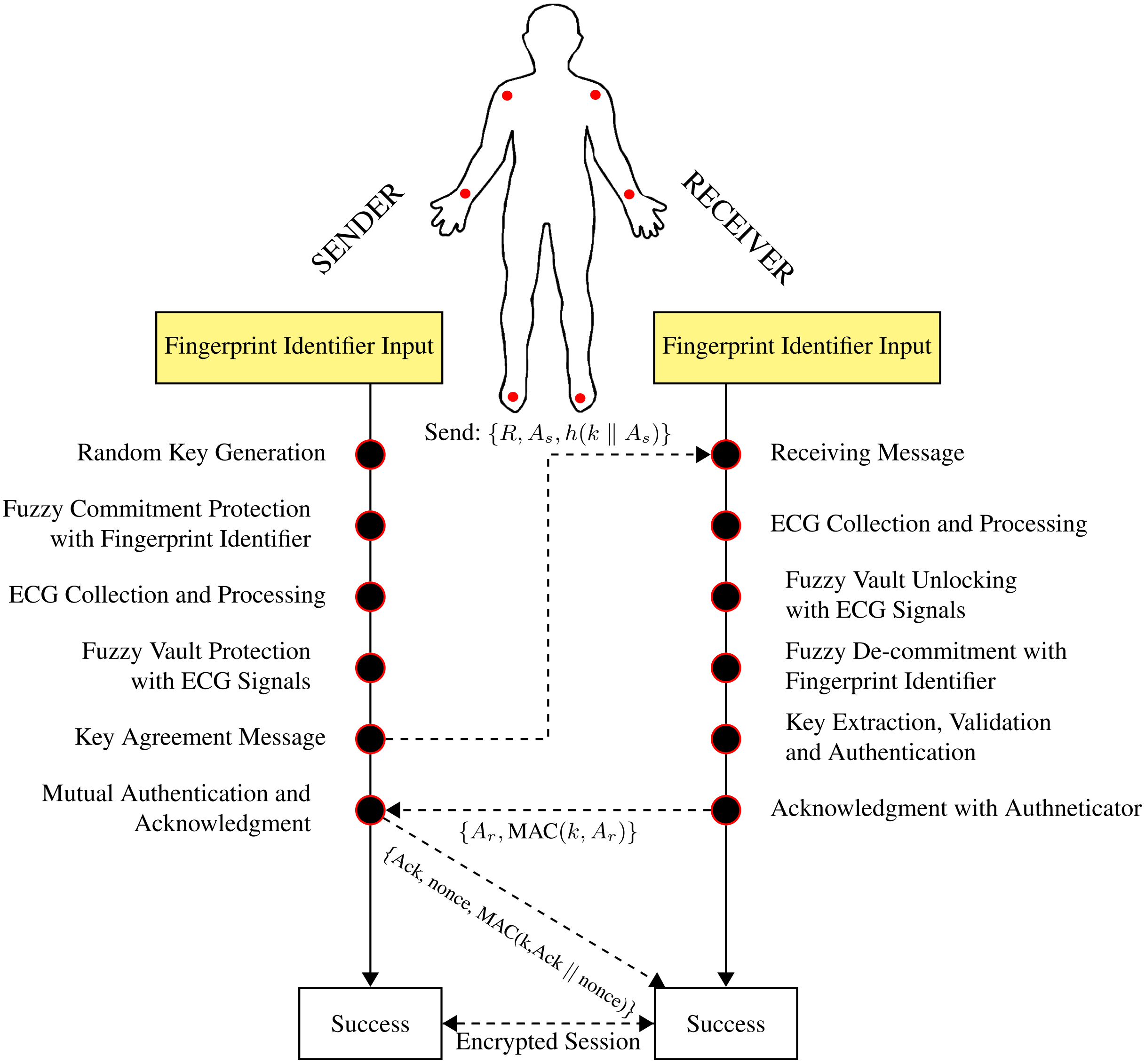

SENDER
RECEIVER
Fingerprint Identifier Input
Fingerprint Identifier Input
Random Key Generation
Fuzzy Commitment Protection with Fingerprint Identifier
ECG Collection and Processing
Fuzzy Vault Protection with ECG Signals
Key Agreement Message
Mutual Authentication and Acknowledgment
Send: $\{R, A_s, h(k \parallel A_s)\}$
Receiving Message
ECG Collection and Processing
Fuzzy Vault Unlocking with ECG Signals
Fuzzy De-commitment with Fingerprint Identifier
Key Extraction, Validation and Authentication
Acknowledgment with Authneticator
$\{A_r, \mathrm{MAC}(k, A_r)\}$
{Ack, nonce, MAC(k,Ack || nonce)}
Success
Success
Encrypted Session

FIGURE 1. A schematic overview of the MBPSKA scheme, $A_s = ID_s \parallel ID_r \parallel AD_s \parallel AD_r \parallel T_s \parallel$ lifetime $\parallel$ Nonce1 and $A_r = ID_r \parallel ID_s \parallel AD_r \parallel AD_s \parallel T_s \parallel$ lifetime $\parallel$ Nonce2.

We focus on the communications between the sensors in a BAN, including the sink device. Communication between the sink device and outside devices is beyond the scope of this paper. Symmetric cryptography is typically used for communication between the sensors in a BAN due to its low computation and communication overhead. The sensors need to authenticate each other and agree on a pairwise secret key to be used for data transmission.

Fig. 1 illustrates a schematic overview of the proposed MBPSKA scheme, which incorporates a biometric-based fuzzy commitment module and a physiological signal-based fuzzy vault module for authentication and key agreement. The sensors, wearable or implanted, are assumed to be in contact with the subject and able to measure the appropriate physiological signals, e.g., ECG. A sensor without direct contact to the human body is not able to measure such physiological signals. These sensors can be configured and can store one or more biometric identifiers. Here, a biometric identifier is a string of bits extracted by processing a biometric feature of a person [51], [62]–[73]. We use fingerprints as the biometric feature and ECG as the physiological signal in our scheme because they are commonly used and are easily acquired.

To secure inter-sensor communications with MBPSKA, one sensor initiates the authentication and key agreement protocol, which is called the sender here. The sender generates a random symmetric key. First, the random key is encoded with the pre-stored biometric identifier using the fuzzy commitment algorithm. Then, the real-time extracted physiological signal features are used to further protect the key based on the fuzzy vault mechanism. The protected key is transmitted along with an authenticator from the sender to the receiving sensor. The authenticator contains the identification of the sender and receiver, key lifetime, and timestamp. The receiver uses its own collected and processed physiological features to unlock the vault, and then employs its stored biometric identifier for fuzzy decommitment to recover the key. The receiver authenticates the message and sends a reply back to the sender for mutual authentication and secure session establishment. Fuzzy commitment is used with the biometric identifier because it incurs a low overhead and is time invariant. The physiological signals are measured in real time and are dynamic. Fuzzy vault is used with these dynamic signals because it can handle reordering of the signal feature samples and the presence of additional or missing features between the samples measured by the sending and receiving sensors.

MBPSKA offers several advantages for key agreement, namely, (i) the keys are random and long enough to prevent brute force attacks; it is efficient in terms of communication, computational, and storage overhead; and it possesses the properties of time variance and distinctiveness. (ii) The scheme allows the authorized personal, e.g., medical practitioners, to add, remove, and adjust a sink node or a sensor on the patient's body and communicate with the patient's BAN without the direct involvement of the patient or asking the patient for the secret password. To be more flexible, it is possible that multiple processed identifiers from different biometric features, e.g. fingerprint and iris are stored in the sensors. If one biometric identifier is not available, another one can be used for authentication. (iii) With multiple biometric and physiological signals for authentication and key protection, MBPSKA improves the security performance and decreases the ability of an unauthorized person to eavesdrop and compromise the BAN compared to existing PSKA schemes.

An adequate threat/attack model is important when designing a security scheme to ensure appropriate priorities to prevent or mitigate attacks. In this paper, we consider security threats related to inter-sensor wireless communications. Adversaries may eavesdrop on the traffic of a BAN, spoof sensor identities, inject malicious messages, or replay old messages. In addition, an attacker may compromise the key distribution process by using another person's physiological data to masquerade as a legitimate sensor. We assume that attackers cannot physically deploy malicious sensors in contact with the subject and steal a subject's biometric identifier without being detected because these sensors are constantly managed by the patient or the caregiver.

IV. MULTI-BIOMETRIC PHYSIOLOGICAL SIGNAL-BASED KEY AGREEMENT

In this section, we present the design details of the MBPSKA scheme including fingerprint-based fuzzy commitment, ECG signal-based fuzzy vault, and authentication and key agreement protocols. Table 1 summarizes a list of notations employed in the system along with their meanings.

TABLE 1. Notations and their definitions.

Notation	Definition
f	Fingerprint template for encoding
σ	ECG signal for encoding
k	Secret key for encoding
f'	Fingerprint template for decoding
σ	ECG signal for decoding
k'	Secret key for decoding
F_C	$(\kappa, f) \mapsto \delta$ denotes the fingerprint fuzzy commitment
F_ν	$(S, \Lambda) \mapsto R$ denotes the ECG fuzzy vault
F	$F_\nu \cdot F_C$ Denotes composition of the two cryptosystems
R	Vault
h	A cryptographic hash function
A_s	Sender authenticator
ID_s	Sender identification
AD_s	Sender address
A_r	Receiver authenticator
ID_r	Receiver identification
AD_r	Receiver address
T_s	Timestamp
MAC	Message Authentication Code
$lifetime$	Key lifetime
$Nonce$	Random nonce

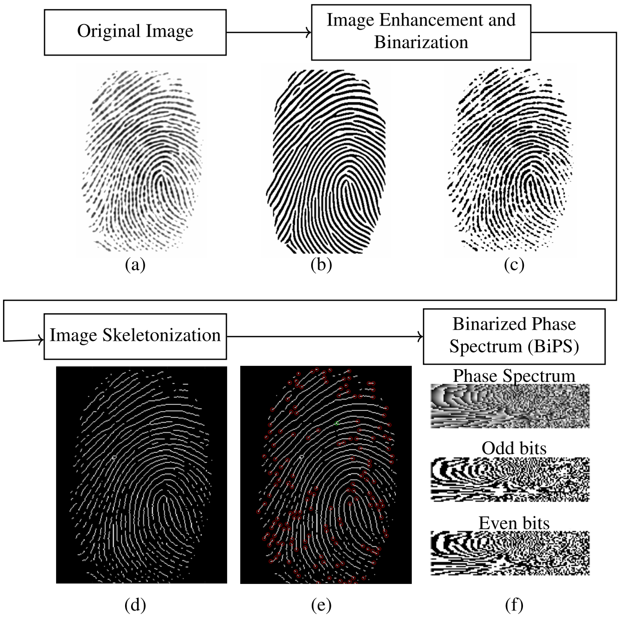


FIGURE 2. Fingerprint identifier extraction. (a) Original Image. (b) Enhancement. (c) Binarization. (d) Skeletonization. (e) Minutiae Extraction. (f) BiPS.

A. FINGERPRINT IDENTIFIER EXTRACTION

First, we describe how to obtain and input the fingerprint identifier. This paper focuses on the system design, and we modify the existing methods [74]–[81] for extracting fingerprint identifiers to fit in our system. The fingerprint identifier extraction is divided into two stages, as shown in Fig. 2.

1) PRE-PROCESSING STAGE

The pre-processing stage of the fingerprints includes procedures to ensure that the fingerprint image is adequately prepared to enable the extraction of clean fingerprint features or minutiae from the image after noise removal and

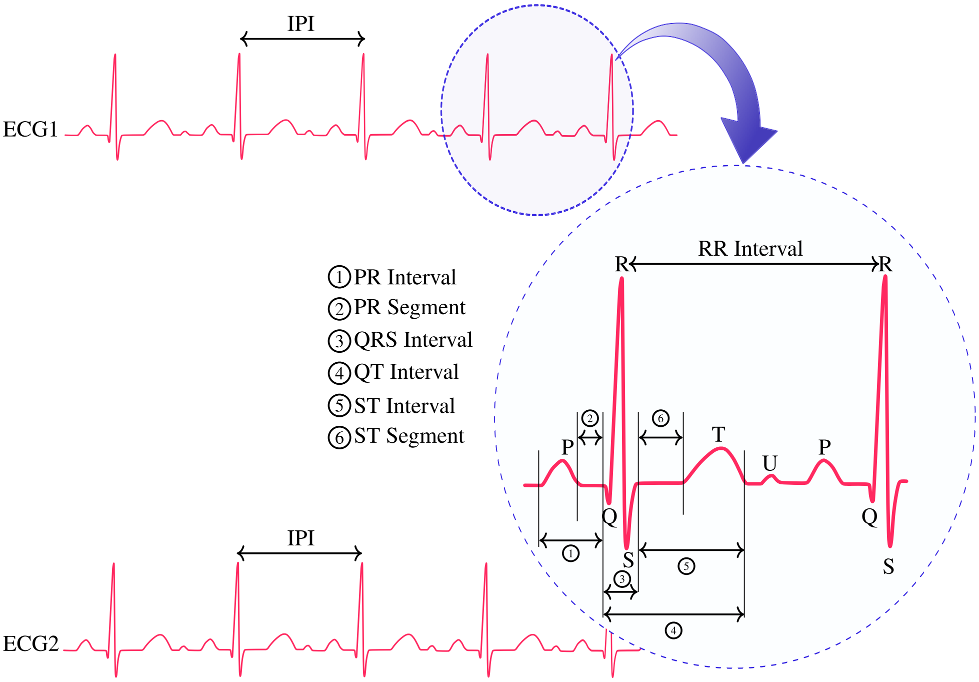


FIGURE 3. The basic shape of an ECG heartbeat signal. It shows the major waves within an ECG trace. The interpulse interval (IPI) is defined as the time interval between two consecutive *R* peaks.

distortion minimization. This step is critical to ensure that suitable minutiae can be extracted from the users' biometric data. There are several pre-processing steps that are performed on the fingerprint image before the acquisition of the feature points. Within this study, the pre-processing steps include the following:

a) **Image enhancement**: This operation allows for the transformation of the image from the spatial to frequency domains, which results in the removal of superficial connections between ridges and the repair of broken lines within the fingerprint as shown in Fig. 2(b).
b) **Image binarization**: This operation converts a fingerprint image from eight-bit grayscale to a binary image as shown in Fig. 2(c).
c) **Morphological thinning or image skeletonization**: This operation reduces the thickness of the individual lines and curves within the finger data to a single pixel thickness as shown in Fig. 2(d).

2) POST-PROCESSING STAGE

The minutiae set is quantized and then its Fourier phase spectrum is obtained [35]. The phase spectrum of the fingerprint minutiae is binarized to a fixed-length binary string representing the extracted fingerprint features as shown in Fig. 2(f). The binarized phase spectrum (BIPS) is used as the biometric identifier to conceal the secret key with a fuzzy commitment scheme in our system. The BIPS can be obtained offline using an external device. It can then be input into the BAN sensors via a wirelessly paired device. Alternatively, a BAN sink device or sensor can directly acquire the fingerprints as input and generate the BIPS.

B. ECG FEATURE EXTRACTION

We use ECG signals to further protect the symmetric session key during its initial distribution from the sender to the receiver. The ECG signals are unique to an individual and time variant due to the different physiological and geometrical features of the heart [20], [82]. They indicate the heart's electrical activity and are a measure of its changes over time. The electrical activity is dependent on the impulses traveling through the heart.

The ECG signals of a heartbeat consist of a P-wave, a QRS complex, and a T-wave [83], as shown in Fig. 3. The accuracy of the ECG feature generation affects the effectiveness of our proposed scheme. The ECG signals measured at the sending and receiving sensors are not exactly the same. Therefore, it is necessary to choose an effective method to generate these features to cope with the high level of noise and errors associated with the original ECG signals. We extract the interpulse intervals (IPIs) to generate the feature vector, similar to the method used in [22] and [44]. IPIs are the time gaps between two adjacent R–R peaks, as shown in Fig. 3. The use of IPIs has been justified in detail in [52], which indicates the benefits of this method, including that it can be obtained with different types of sensors and from different physiological signals, as well as that it can be measured without much variation from different body parts. Algorithm 1 shows the extraction of IPIs at the sender and receiver, where a series of digital signal processing techniques are used to detect R peaks and each of the IPI samples is extracted between two consecutive R peaks [84]. The last 4 bits of an IPI sample are chosen as its binary representation, and four adjacent IPI samples are concatenated to form a 16-bit IPI feature value.

Algorithm 1 IPI Feature Generation

1: The ECG signals are collected simultaneously at the sender and the receiver.
2: The peak detection function is employed to extract IPI samples from the collected signals.
3: Each IPI sample is quantified, and the last 4-bits of each sample is used as its binary representation.
4: Four consecutive IPI samples are concatenated to form a 16-bit feature.
5: The sender and receiver each output a feature vector of length D : $F_s = \{f s^1, f_s^2, f_s^3, \ldots, f_s^D\}$ and $F_r = \{f r^1, f_r^2, f_r^3, \ldots, f_r^D\}$, respectively.

Algorithm 2 Algorithm for Fuzzy Commitment Using Fingerprint Identifier

1: Generate a random number as the secret key κ.
2: The key κ is passed through an error-correcting (Reed–Solomon) encoder to obtain a code word C_κ.
3: The fingerprint identifier f is XORed with C_κ to obtain $\delta = f \oplus C_\kappa$.

This procedure is performed simultaneously at the sending and receiving sensors, each generating a feature vector for the sender and the receiver, $F_s = \{f s^1, f_s^2, f_s^3, \ldots, f_s^D\}$ and $F_r = \{f r^1, f_r^2, f_r^3, \ldots, f_r^D\}$, respectively

C. FUZZY COMMITMENT

In our design, the sending sensor generates a random pairwise key κ with a size of $|\kappa|$ bits and the key is first hidden by the fuzzy commitment scheme [28] using the patient's fingerprint identifier f. The following steps are performed on the key κ and the fingerprint identifier f to obtain an encoded output δ. i) The secret key κ is passed through a Reed–Solomon error-correcting coder [85] to obtain a code word C_κ. The size of the code word, $|C_\kappa|$, is the same as the size of fingerprint identifier, $|f|$. ii) The XOR function is used to bind the fingerprint identifier f and the code word C_κ, which results in an output of δ, $\delta = f \oplus C_\kappa$. Algorithm 2 summarizes the fuzzy commitment process.

At the receiver, the fuzzy-decommitment process is performed to recover the secret key κ based on the output δ' of the process from the message received from the sender. The receiver uses its stored fingerprint identifier f'. Note that δ' may not be the exact same as δ due to message transmission errors and that the fingerprint identifier f' at the receiver may or may not be equal to the original fingerprint identifier f used for the commitment at the sender. To perform the decommitment, C_κ, is computed using the XOR function between the fingerprint identifier f' and the output data δ' at the receiver, $C_{\kappa'} = f' \oplus \delta'$. The code word $C_{\kappa'}$ is decoded using a Reed–Solomon error-correcting decoder to obtain the recovered key κ'. If the hash value of the recovered key κ' and the authenticator A_s is equal to the hash value of the original key and the authenticator, i.e., if $h(\kappa' \parallel A_s) = h(\kappa \parallel A_s)$, the recovered key is considered to be the true secret key transmitted by the sender. The authenticator A_s is carried in the message from the sender to the receiver as discussed later. The error correction capability of the Reed–Solomon code determines the level of the difference between $C_{\kappa'}$ and C_κ that can be corrected and impacts the robustness and accuracy of the fuzzy commitment scheme, which we examine in the next section. Algorithm 3 illustrates the fuzzy-decommitment process.

Algorithm 3 Algorithm for Fuzzy Decommitment Using Fingerprint Identifier

1: The fingerprint identifier f' is stored in the sensor.
2: δ', obtained from the received message, is XORed with the fingerprint identifier f' to obtain the code word $C_{\kappa'} = f' \oplus \delta'$.
3: The code word C'_κ is passed through a (Reed–Solomon) error-correcting decoder to obtain a recovered key κ', which may or may not be equal to κ.
4: If hash $h(k) = h(k')$, the secret key k is decoded successfully and the key k is given as output.

D. FUZZY VAULT

Another primary component involved in our proposed system is a fuzzy vault-based crypto-scheme [23]. This scheme locks a secret value S in a construct called a vault using a set of samples. The vault can be unlocked to extract the original secret with another set of samples only if it has substantial overlap with the original set used to lock it. The steps in fuzzy vault locking include the following. i) Given a secret value S in a Galois field of order $F_q = 2^q$ (we are using $F_q = 2^{16}$), generate a $(v-1)$-degree polynomial p by encoding the secret $S = (s_0||s_1||\ldots||s_{v-1})$, $S \in F_q$, in the coefficients of the polynomial $y = p(x) = s_0 + s_1x + \cdots + s_{(v-1)}x^{(v-1)}$. ii) For a set of t sample values, $\Lambda = \{\alpha_1, \ldots, \alpha_i, \ldots, \alpha_t\}$, $\alpha_i \in F_q$, $i = 1, 2, \ldots, t$, $v \le t$, compute a set of genuine points based on the polynomial, where $R = \{(x_i = \alpha_i, y_i = p(x_i))\}$. iii) Select $r - t$ random values that do not belong to the set Λ, $x_i \in F_q \backslash \Lambda$, $i = t + 1, \ldots, r$, $v \le t \le r$, and randomly pick a set of y corresponding values, $y_i \in F_q \backslash U_{j=1}^{t}\{p(x_j)\}$, $i = t + 1, \ldots, r$. iv) Add points, called chaff points, $\{(x_i, y_i)\}$ $i = t + 1, \ldots, r$ to the set, $R \longleftarrow R \cup \{(x_i, y_i)\}$. v). Randomly permute R to ensure that the genuine points and the chaff points are indistinguishable. The output of fuzzy vault is $R \longleftarrow RandomPermute\{R\}$. R includes t genuine points with their projections onto the polynomial and $r - t$ chaff points that are not on p. Algorithm 4 outlines the fuzzy vault locking process.

Once the secret has been locked in the vault, it can be unlocked using a second set that has a sufficient number of significant points that lie on the polynomial by following the steps given in Algorithm 5.

Various methods can be used to reconstruct the polynomial and obtain the secret S, such as Lagrangian interpolation,

Algorithm 4 Algorithm for Vault Encoding Using ECG Data

```
1: The ECG signal $\sigma$ is converted to a set of points over $GF = 2^{16}$ after calculating IPI from the signal at the sender side, followed by conversion to binary vector representation and division into $N - bit$ segments with each segment corresponding to a point in $GF$.
2: The secret $S$ is converted to a polynomial $P$ of degree $(v-1)$ by encoding the secret $S = (s_0||s_1||\ldots||s_{v-1})$, $S \in F_q$, in the coefficients of polynomial $y = p(x) = s_0 + s_1x + \cdots + s_{(v-1)}x^{(v-1)}$
3: For a set of t sample values, $\Lambda = \{\alpha_1, \ldots, \alpha_i, \ldots, \alpha_t\}$, $\alpha_i \in F_q$, $i = 1, 2, \ldots, t, v \leq t$, compute a set of genuine points, based on the polynomial, where $R = (x_i = \alpha_i, y_i = p(x_i))$, by mapping the points via the polynomial associated with $S$
4: Form a set of chaff points by randomly selecting $r - t$ values that do not belong to the set $\Lambda$, $x_i \in F_q\ \Lambda$, $i = t+1, \ldots, r$, $v \leq t \leq r$, and randomly pick a set of corresponding $y$ values, $y_i \in F_q\ U_{j=1}^{t}\{p(x_j)\}$, $i = t+1, \ldots, r$.
5: Add the chaff points, $\{(x_i, y_i)\}\ i = t+1, \ldots, r$ to the set, $R \longleftarrow R \cup \{(x_i, y_i)\}$.
6: Randomly permute $R$ to ensure genuine points and chaff points that are indistinguishable, and the output of a fuzzy vault is $R \longleftarrow RandomPermute\{R\}$.
```

Algorithm 5 Algorithm for Fuzzy Vault Decoding Using ECG Data

```
1: ECG signal $\sigma'$ is converted into a set of feature sample values, $B = \{\beta_1, \beta_2, \ldots, \beta_t\}$, over Galois Field $GF = 2^{16}$ at the receiver by calculating IPI from the ECG signal and performing the same processing technique as the sender, which is used as the evaluation points.
2: To unlock the vault that was locked with the sender feature sample points $R = \{(x_i, y_i)\}$, $i = 1, 2, \ldots, r$, use the set $B = \{\beta_1, \beta_2, \ldots, \beta_t\}$ obtained in 1). For each $\beta_i$, retrieve the corresponding point from $R$, $\{(x_j = \beta_i, y_j = p(\beta_i))\}$.
3: Use the set of evaluation points, $Q = \{(x_j = \beta_i, y_j = p(\beta_j))\}$, which is a subset of $R$, $Q \subset R$, to reconstruct the polynomial $p$, such that the coefficients of $p$ correspond to the secret $S$.
```

matrix inversion, or $[t, v]_q$ Reed–Solomon decoding [85]. If there are fewer than $(t - v)/2$ errors between the sets Λ and B, the secret S can be correctly decoded. Otherwise, the decoding algorithm will generate a null output or a wrong output. The correct polynomial cannot then be reconstructed, and the secret will remain inaccessible. More chaff points make it more difficult to reconstruct the correct polynomial; thus, they provide stronger security against brute force attacks, as shown in section V. In our design, we use the IPI features extracted from the ECG signals at the sending and receiving sensors to lock and unlock the secrets for the authentication and key agreement.

Algorithm 6 Algorithm for Encoding MBPSKA

```
1: The key $\kappa$ and the fingerprint template $f$ are passed through the fingerprint fuzzy commitment $F_C$ to obtain the helper data $\delta$.
2: $\delta$ is passed through the ECG fuzzy vault module to obtain a fuzzy vault output of $R : F_v : (\delta, \sigma) \longmapsto R$.
3: The original key k is concatenated with the authenticator $A_s = ID_s \parallel ID_R \parallel AD_s \parallel AD_R \parallel T_s \parallel lifetime \parallel$ Nonce and hashed to generate$h(\kappa \parallel A_s)$.
4: The transmitted message contains $\{R, A_s, h(k \parallel A_s)\}$.
```

E. PROPOSED MULTI-BIOMETRIC AND PHYSIOLOGICAL SIGNAL-BASED KEY AGREEMENT (MBPSKA) SCHEME

In this section, we present the design of the proposed MBPSKA scheme, which integrates the fingerprint-based fuzzy commitment, the ECG-based fuzzy vault, and the mutual authentication and key agreement protocol between the sender and the receiver. We describe how the different components are used and incorporated into the system, as well as the input and output interfaces of the individual components and the protocol to establish a secure session.

Fig. 4 shows the encoding operation at the sender. The randomly generated secret key, k, $k \in F_q$, and the fingerprint identifier, f, $f \in F_q$, are provided as input to the fuzzy commitment module. In the fuzzy commitment module, the secret key k is converted into a code word C_k using a Reed–Solomon encoder; this code word C_k is XORed with the fingerprint identifier f to generate the output δ, $\delta \in F_q$.

The output of the fuzzy commitment process δ is used as an input to the fuzzy vault for further protection before being transmitted to the receiver. Let $S = \delta$ and the coefficients of the fuzzy vault $(v-1)$-degree polynomial $p(x)$ consist of $S = (s_0 \parallel s_1 \parallel \cdots \parallel s_(v-1))$, as described previously. A series of t consecutive IPI values, $\Lambda = \alpha_1, \ldots, \alpha_i, \ldots, \alpha_t, \alpha_i \in F_q$, $i = 1, 2, \ldots t$, extracted from the ECG signals over the time by the sending sensor are employed to produce the genuine points on the polynomial $p(x)$ to lock the vault, and $r - t$, $v \leq t \leq r$ chaff points are added to the dataset. The dataset is randomly permuted to generate the fuzzy vault output, R, which contains t genuine points and $r - t$ chaff points in a random order. Algorithm 6 summarizes the encoding process of the proposed system.

The sender transmits a key agreement request (KeyAgreeReq) message containing $\{R, A_s, h(k \parallel A_s)\}$ to the receiver, where A_s is the authenticator that is the concatenation of several information elements, including the sender identification (ID_s), the receiver identity (ID_r), the sender address (AD_s), the receiver address (AD_r), the timestamp (T_s) of the first physiological signal sample used in the fuzzy vault, the key lifetime, and a random nonce,

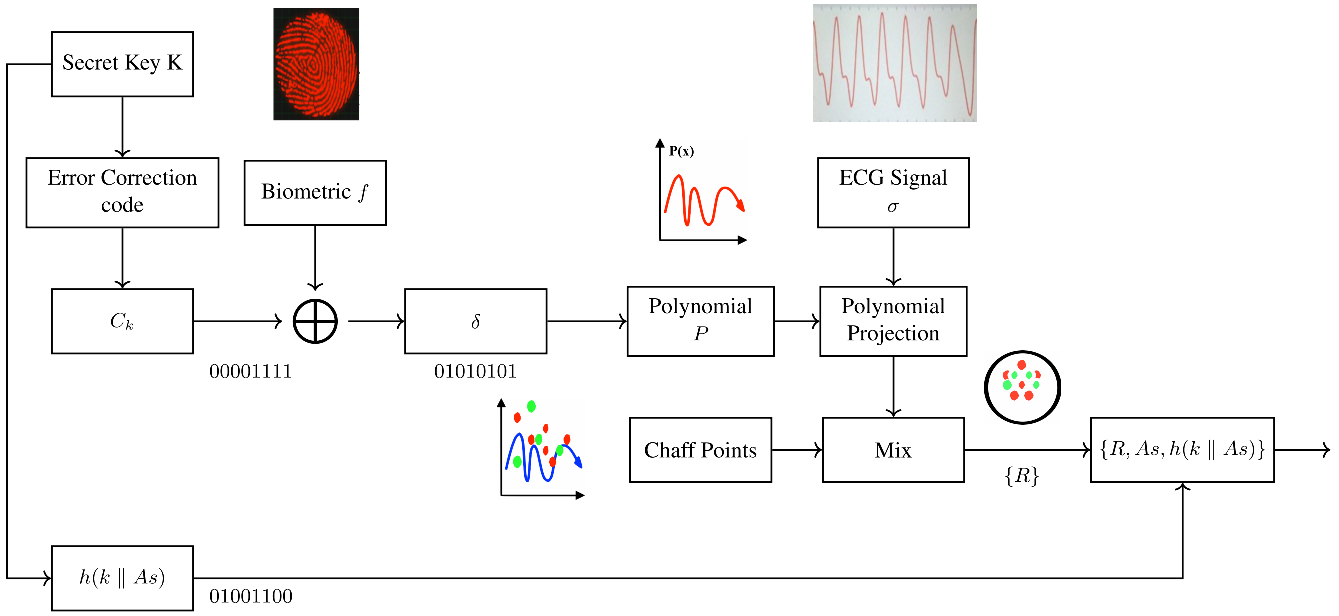


FIGURE 4. Sender process.

i.e., $A_s = ID_s \parallel ID_R \parallel AD_s \parallel AD_R \parallel T_s \parallel lifetime \parallel Nonce$. The authenticator is concatenated with the original random key and hashed using a cryptographic hash function, e.g., SHA-1, to produce $h(k \parallel A_s)$, which will be transmitted with the message. The hashed value $h(k \parallel A_s)$ is different in each message process because the timestamp and nonce change. It will be used by the receiver to check the key correctness. Moreover, the authenticator provides additional information in the mutual authentication process and helps enhance the capability of the system to defend against replay attacks, as discussed in the next section.

As shown in Fig. 5, the receiving sensor takes readings of the ECG signal at the same time as the sending sensor and applies the same processing techniques to generate a series of IPI values over time. The receiver obtains the starting point of the IPI value series based on the signal timestamp T_s in the authenticator A_s of the received message and an array of consecutive points $B = \{\beta_1, \beta_2, \ldots \beta_t\}$ based on its own IPIs starting at T_s. For each β_i, the receiver retrieves the corresponding point from R and generates the set $Q = \{(x_i = \beta_i, y_i = p(\beta_i))\}$, $Q \subseteq R$. In other words, the receiver filters out the chaff points, such that only the genuine points remain in Q. Then, the receiver uses this set of evaluation points to reconstruct the polynomial and obtain the secret using the algorithm described in Subsection V.D through vault decoding. If the sending and receiving sensors are monitoring the same user, the IPIs extracted from the ECG signals around the same time will be nearly identical or very similar. As discussed previously, when the number of errors between sets Λ and B is less than $(r - t)/2$, the recovered secret S' at the receiver will be equal to the secret S sent by the sender, i.e., $S' = S$. If an attacker has a set B' of IPIs obtained from a different person or the same person but at a different time, there will likely be more than $(r - t)/2$ errors between Λ and B'. The attacker will not be able to obtain a correct set of evaluation points and unlock the vault successfully to obtain the secret. Similarly, if the sender is an attacker with a set Λ' of IPIs obtained from a different person or the same person but at a different time, the number of errors between Λ' and B will likely be greater than $(r - t)/2$, so that the recovered secret S' at the receiver will not be the same as the secret S sent by the sender. The pairwise key will not be obtained and the authentication will fail at the receiver, as described below.

The receiver uses the secret S' recovered from its fuzzy vault unlocking process as the input for the fuzzy-decommitment process. Let $\delta' = S'$. As described previously, in the fuzzy decommitment, the helper data δ' and the fingerprint identifier stored at the receiver are XORed to retrieve the code word $C_{\kappa'}$ and then a decoding process is performed on the code word $C_{\kappa'}$ by a Reed–Solomon decoder to correct the errors and obtain the key κ'. If the hash value of the recovered key and the authenticator $h(\kappa' \parallel A_s)$ is equal to the hash value of the actual $h(\kappa \parallel A_s)$ that is carried in the message from the sender, the process is considered to be successful. Therefore, the receiver authenticates the sender, and $\kappa' = \kappa$ is the pairwise key between the sender and the receiver. Otherwise, the receiver will not be able to authenticate the sender and obtain the pairwise key for secure communication. Algorithm 7 summarizes the decoding process at the receiver.

If the key recovery process is successful, the receiver will send a key agreement reply (KeyAgreeRpl) message to the sender that contains $\{A_r, MAC(\kappa, A_r)\}$, as shown in Fig. 2, where A_r is the receiver authenticator, $A_r = ID_r \parallel ID_s \parallel AD_r \parallel AD_s \parallel T_s \parallel lifetime \parallel Nonce$, and $MAC(\kappa, A_r)$ is the message authentication code generated using a cryptographic

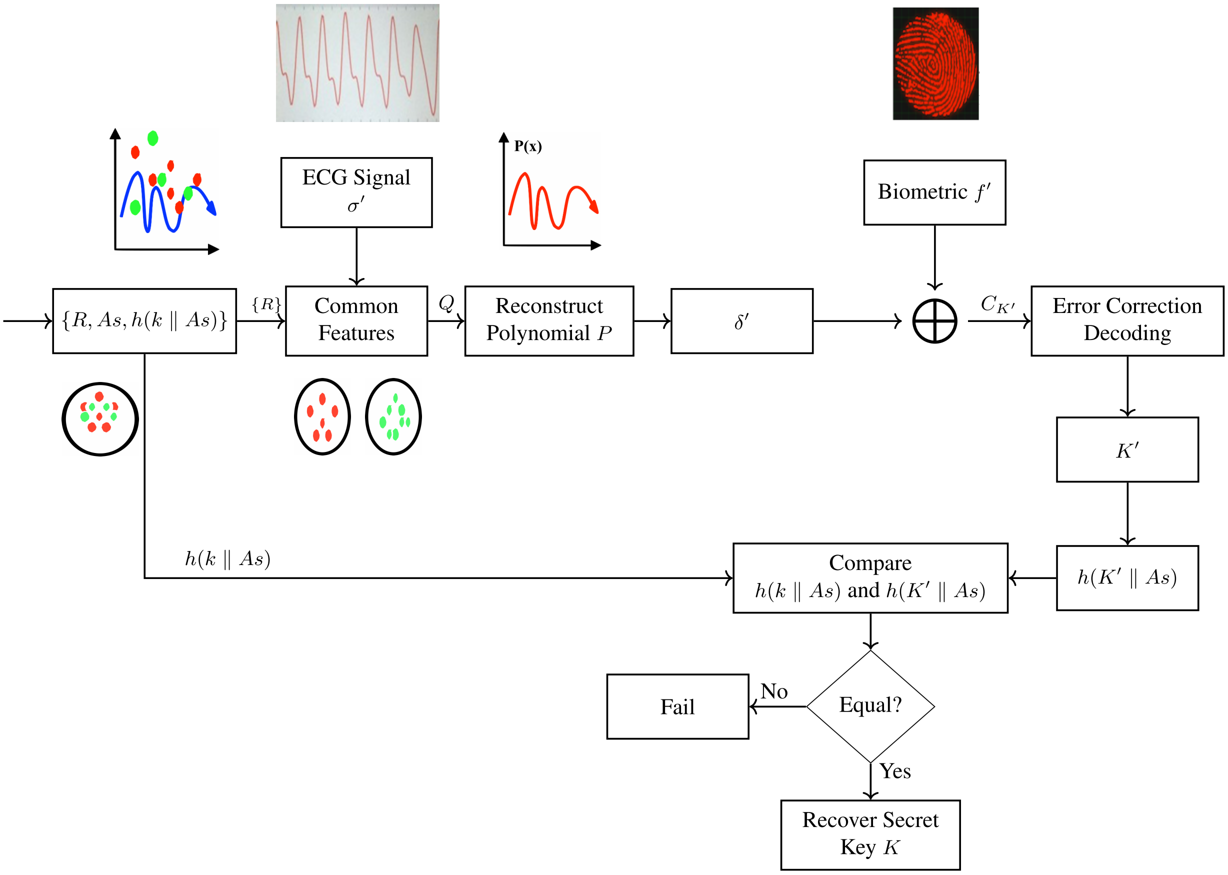


FIGURE 5. The receiver process.

Algorithm 7 Algorithm for Decoding MBPSKA

```
The received fuzzy vault data $R$ is passed through the decoding process of the fuzzy vault module at the receiver to obtain $\delta' : F_v^{-1} : (R, \sigma') \longmapsto \delta'$.
$\delta'$ is passed through the decoding process of the fuzzy decommitment module to obtain a recovered key $\kappa' : F_c^{-1} : (\delta', f') \longmapsto \kappa'$.
If $h(\kappa' \parallel A_s) = h(\kappa \parallel A_s)$, then the process is successful. $\kappa'$ is the correct key.
```

hash function, e.g., SHA-1, with the pairwise key recovered by the receiver. The key agreement reply message allows the sender to authenticate the receiver by ensuring that the receiver has recovered the pairwise key correctly. The sender sends a key agreement acknowledge (KeyAgreeAck) to the receiver if the receiver is authenticated successfully and the pairwise key is validated. A secure communication session is then established with the pairwise key between the sender and the receiver. If the receiver key recovery process fails, the receiver sends a key agreement reject (KeyAgreeRjt) message to the sender. If the sender receives a key agreement reject or receives a key agreement reply message but cannot authenticate the receiver, it may reinitiate the authentication and key agreement process.

In our proposed MBPSKA scheme, the secret key is first protected by a fuzzy commitment module based on the users's fingerprint identifier and then by a fuzzy vault module with the same user's ECG signal. Let $F_c : (\kappa, f) \longmapsto \delta$ denote the fingerprint fuzzy commitment and $F_v : (S, \Lambda) \longmapsto R$ denote the ECG fuzzy vault. The MBPKSA scheme is essentially $F := F_v \circ F_c$, the combination of these two algorithms. We analyze the security of MBPSKA in the next section.

V. SECURITY OF MBPSKA

In this section, we discuss the security principles implemented in the MBPSKA scheme that aim to enable authentication and secure wireless communications between the sensors in a BAN. The proposed scheme is able to defend against brute force attacks, eavesdropping, impersonation, man-in-the-middle-attacks, and replay attacks. Denial-of-service attacks (DOS), such as jamming and battery depletion, are not considered in this paper.

A key feature of MBPSKA is the integration of the biometric identifier-based fuzzy commitment and physiological signal-based fuzzy vault that act synergistically to protect against various attacks. Fuzzy vault uses real-time ECG signals, which are distinctive for different individuals and time variant for each individual person. Two sensors on the same target at the same time are required to obtain a minimum of *v* common points to reconstruct a polynomial with a degree of v and establish an authenticated secure session. However, the fuzzy vault scheme is vulnerable to brute force attacks and it is theoretically possible to eavesdrop on a transmission and unlock the vault through repeated random attempts at polynomial unlocking [86]. Increasing the degree of the polynomial and/or adding more chaff points will increase the total computational cost required to break the vault and reduce its vulnerability to a brute force attack; however, this will come at the cost of potential false negatives.

Meanwhile, fingerprints with fuzzy commitment cannot easily be compromised using brute force attacks because it is not feasible to recreate the appropriate BIPS string without the original fingerprint. However, it is well known that fingerprints are prone to template-based attacks, e.g., stealing or duplicating someone's fingerprints [33], because they are time invariant. Combining ECG-based fuzzy vault and fingerprint-based fuzzy commitment schemes takes advantage of both mechanisms and makes the system very robust against various attacks. Even if an attacker has a brute force algorithm and the ability to eavesdrop, they still require the same or a similar fingerprint to recover the secret key. Likewise, possession of a fingerprint template alone is not sufficient to unlock the system without the ability to eavesdrop and conduct brute force attacks. Therefore, the two mechanisms function in tandem to create a robust double lock with stronger security than a single mechanism. Next, we discuss the security characteristics of each component.

A. SECURITY OF FINGERPRINT-BASED FUZZY COMMITMENT

We first analyze the similarity of fingerprint impressions of the same person and those of different people by measuring their Hamming distance. We used a dataset of fingerprints from 100 different people with 8 impressions for each fingerprint, yielding a total of 800 impressions. This dataset was obtained from the FVC2002-DB1A database [87]. Each fingerprint impression was transformed into a fingerprint identifier, i.e., a fixed-length binary string of 128 bits based on the binarized phase spectrum algorithm [35], as discussed previously. Then, we measured the Hamming distance between any two fingerprint identifiers belonging to the same person to obtain the Hamming distance distribution of fingerprints for the same person. The Hamming distance is the number of bit errors between two binary strings. Similarly, we measured the Hamming distance between the fingerprint identifiers of different people and obtained their distribution. Fig. 6 shows the probability density function (PDF) of the Hamming distance distribution for fingerprint identifiers of the same person and different people. For the same person's fingerprint identifiers, most of the Hamming distance values are near 40, while for the fingerprint identifiers of different people, most of the Hamming distance values are near 70.

If we use a fuzzy commitment scheme with a certain error correction capability for authentication, false positives may occur, that is, when two fingerprint identifiers from different people are used for the fuzzy commitment and decommitment processes, respectively, the fuzzy commitment scheme considers them to be from the same person and the fuzzy-decommitment process is successful. False negatives may occur as well when two fingerprint identifiers from the same person are used for the fuzzy commitment and decommitment processes and the fuzzy commitment scheme considers them to be from two different people causing the fuzzy-decommitment process to fail. The false positive rate and the false negative rate can be controlled by adjusting the error correction capability of the fuzzy commitment scheme, i.e., the maximum number of errors or the Hamming distance threshold that the error correction code used in the fuzzy commitment scheme can correct. Fig. 7 shows the false positive rate and the false negative rate versus the maximum Hamming distance of two fingerprint identifiers that the error correction code can correct when a fingerprint-based fuzzy commitment scheme is used for authentication. If we choose an appropriate

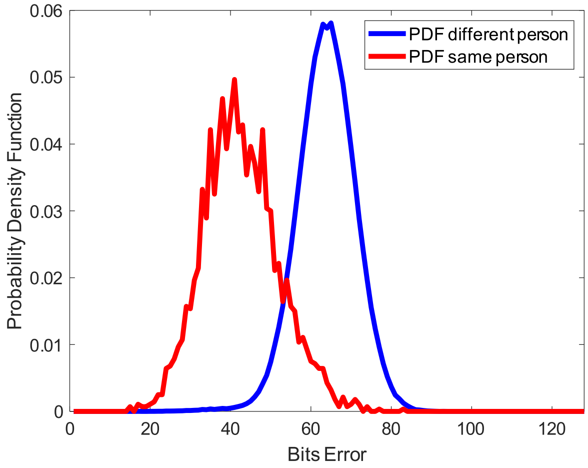


FIGURE 6. PDFs of the Hamming distance distribution for the same person's fingerprint identifiers and the fingerprint identifiers of different persons.

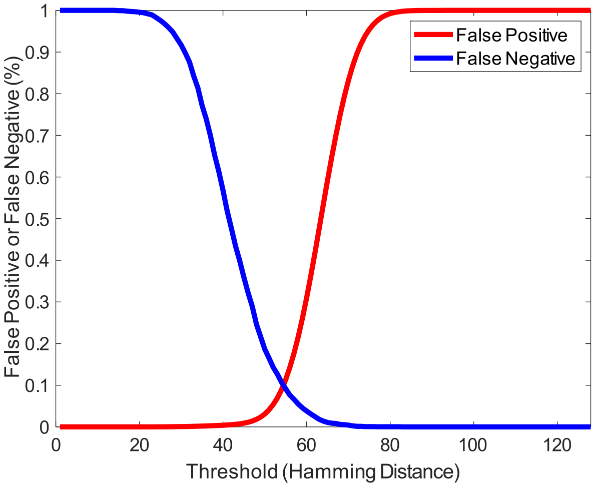


FIGURE 7. False positive rate and false negative rate versus the maximum Hamming distance of two fingerprint identifiers that the error correction code can correct when a fingerprint-based fuzzy commitment scheme is used for authentication.

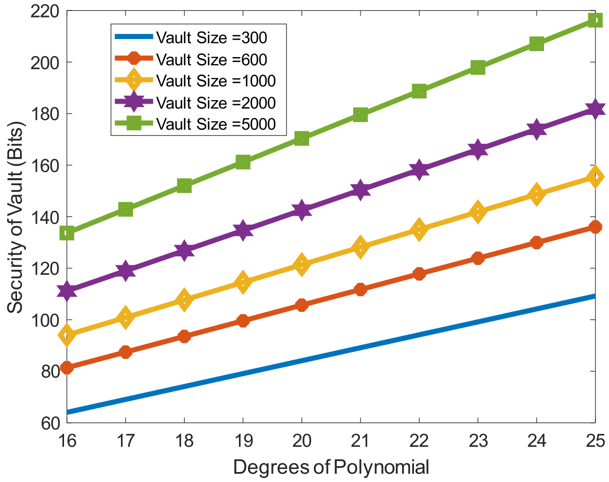


FIGURE 8. The security strength of fuzzy vaults versus the polynomial degree for different vault sizes.

error correction threshold in the fuzzy commitment scheme, a good performance with good reliability (low false positive rate) and accuracy (low false negative rate) is obtained.

B. SECURITY OF THE ECG-BASED FUZZY VAULT

Fuzzy vault security depends on the complexity of the vault polynomial reconstruction. The original IPI feature points projected on the v-degree polynomial are hidden among many chaff points that are randomly generated and are not on the polynomial. An attacker needs to try the combinations of $v+1$ points in the vault to be able to reconstruct the polynomial correctly and obtain the secret polynomial coefficients. The security strength of the vault depends on the number of combinations an attacker has to try to obtain at least $v + 1$ genuine points out of a total of r points (the genuine and chaff points) in the vault [23]. Fig. 8 shows the vault security strength against brute force attacks with regard to the polynomial degree for different vault sizes. The security strength is measured by the required amount of computation equivalent to a brute force attack on a random key of a particular bit size. As expected, the security strength increases as the vault size (the number of chaff points) increases. Similarly, a higher degree polynomial will provide a higher security strength.

C. CONFIDENTIALITY

Confidentiality refers to preventing the unauthorized disclosure of data to attackers. We used two forms of authentication and key protection in the initial key agreement, fingerprint-based fuzzy commitment and ECG-based fuzzy vault, which possess different properties to prevent attacks, as discussed previously. This ensures the security when the cryptographic session key is exchanged between two sensors. Once the authentication is successful and the secret pairwise session key is agreed on between the sender and the receiver via the proposed MBPSKA scheme, future messages will be encrypted by the pairwise key to ensure confidentiality. The proposed scheme is thus able to protect against eavesdropping and brute force attacks.

D. AUTHENTICITY

Authenticity here refers to the fact that the recipient of the data can trust and verify that the data were transmitted by the genuine sender and ensures that this sender is not an illegitimate entity claiming to be genuine. The proposed MBPSKA employs fingerprint-based fuzzy commitment and ECG-based fuzzy vault as well as the authenticator and message exchanges to provide mutual authentication between the receiver and the sender. It is difficult for an attacker to forge both the fingerprint identifier and ECG features. In addition, the ECG signal is time variant. If an attacker wants to use the physiological data for an impersonation attack, the vault would have to be broken fast enough for the physiological feature values to still match with the original transmission. Therefore, the proposed scheme provides protection against the impersonation attacks.

E. INTEGRITY

Message integrity refers to the fact that the data in the message are not modified or tampered with during transmission and that the message is correctly received by the intended entity [88]. The proposed MBPSKA scheme uses a cryptographic hash of the concatenated key and authenticator to ensure integrity in the transmission of the pairwise session key. The sender and receiver conduct mutual authentication using fingerprints and ECG signals and then agree on a secret pairwise key. The receiver compares the hashed value of the reconstructed key and authenticator to the hashed value of the original key and authenticator to ensure its integrity. Once the pairwise key is agreed upon, the message authentication code generated by the pairwise key ensures the integrity of future message exchanges. Therefore, MBPSKA provides the protection against message corruption attacks.

In addition, the proposed scheme can maintain key backward/forward secrecy, and detect and prevent other attacks such as replay and man-in-the-middle attacks.

- Backward/forward secrecy is maintained because each session key is generated independently by a pseudo-random generator. Different pairwise keys are used for different pairs of sensors, and the pairwise key is updated periodically for each communication session between two sensors. An attacker that knows an old session key cannot decrypt the messages encrypted with a new session key. Similarly, an attacker that knows the current session key cannot decrypt the messages encrypted with a previous session key. Furthermore, the keys are protected by time-variant ECG features in the key agreement protocol messages. An attacker who knows the old ECG features cannot recover the keys protected by the current ECG features.
- The time stamp and the nonce in the authenticator are unique for each transmitted message. This allows the receiver to detect duplicated messages and delayed messages and prevent replay attacks.
- During a man-in-the-middle attack, the attacker acts as a middleman who sniffs the traffic between two

communicating devices and launches an attack [89]. In the proposed scheme, chaff points and genuine points are mixed in the transmitted messages, which makes it difficult for an attacker to distinguish legitimate data via sniffing. In addition, the key is protected by both fuzzy commitment and fuzzy vault, which makes it more secure than if only one technique was used.

VI. EVALUATION

In this section, we present the simulation results to evaluate and compare the performance of MBPSKA with that of the existing PSKA schemes [19], [57] using actual fingerprints and ECG data. The fingerprints were obtained from the public domain FVC2002-DB1A database [87], which consists of 100 fingers, each with eight impressions. The ECG data from the MIT PhysioBank database [90], [91] were used in our experiments, including MIT-BIH Normal Sinus Rhythm (NSRDB), MIT-BIH Arrhythmia (MITDB), and European ST-T (EDB). Evaluation was conducted starting with feature extraction from the fingerprint and ECG data as described above. The performance of a biometric-based security scheme can be evaluated with three important metrics, namely, the false non-match rate (FNMR), the false match rate (FMR), and the genuine acceptance rate (GAR) [19]. FNMR, i.e. false negative rate, represents a measure of the inability of the receiver to decrypt a message from the sender protected by the fingerprint-based fuzzy commitment and ECG-based fuzzy vault with the features extracted from the same subject. FMR, i.e. false positive rate, measures the possibility that the receiver uses the fingerprint identifier and ECG data of a different subject to decrypt a secret message from the sender. GAR is the measure of the probability that a message from the sender is decrypted successfully using the correct fingerprint identifier and ECG data from the same subject, where FNMR is equal to 1-GAR. ECG data were collected for approximately 1 minute from each subject and were obtained from two leads on each person. We assumed that the two communicating sensors would use the signals from different leads for the key agreement. Fingerprint identifiers are extracted based on BIPS as described in IV.A. The MBPSKA scheme is implemented and tested with different secret key lengths and different vault sizes using MATLAB.

We compared the performance of our proposed MBPSKA system to that of the existing PSKA key agreement protocol [19] and the FPA algorithm [57], including authentication and key agreement operation performance and communication overhead. PSKA uses the IPIs extracted from physiological signals with a fuzzy vault for key distribution and allows two sensors to agree on a shared symmetric key in an authenticated manner. FPA uses the bio-inspired flower pollination algorithm to create the chaff points along with the extracted features from the ECG signals to generate the genuine points to be used with a fuzzy vault to secure communications in a wireless BAN.

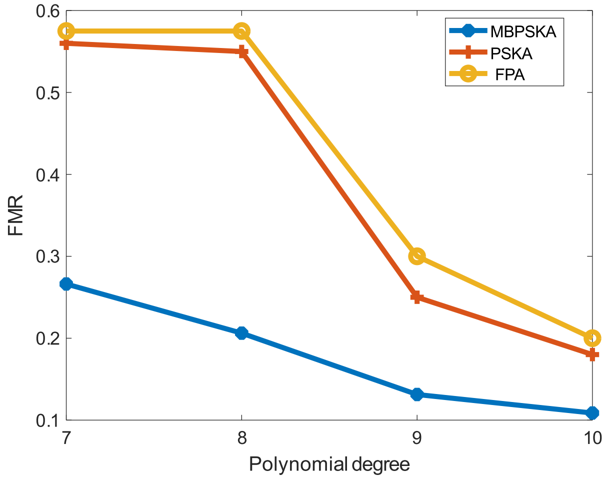


FIGURE 9. FMR versus the polynomial degree for three different schemes: MBPSKA, PSKA, and FPA.

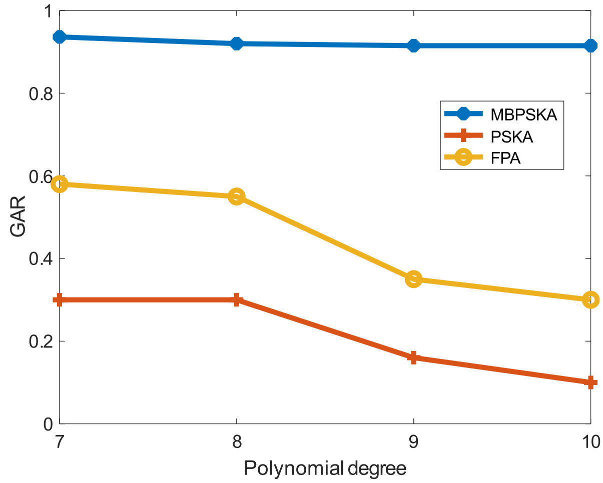


FIGURE 10. GAR versus the polynomial degree for three different schemes: MBPSKA, PSKA, and FPA.

A. KEY AGREEMENT OPERATION PERFORMANCE

Fig.9 illustrates the FMRs of the above three schemes for different polynomial degrees of the fuzzy vault. We can see that the FMR decreases for all three schemes as the polynomial degree increases. This is because it becomes more difficult to decode the coefficients hidden in a vault, i.e. the specificity of the receiver/decoder increases with a higher order polynomial. Further, we can see that the performance of our proposed MBPSKA scheme is much better than that of the two baselines. The FMR of the exiting PSKA decreases from 56% to 18% as the polynomial degree increases from 7 to 10. However, its GAR also decreases from 30% to approximately 10% as shown in Fig. 10. Similarly, FPA has an initial FMR of 57%, which gradually decreases to 20% as the polynomial degree increases from 7 to 10 with a GAR reduced from 58% to 30%. In comparison, the FMR of MBPSKA decreases from 26% to 10% with the polynomial degree increased from 7 to 10, while the GAR is kept above 90%. This is because PSKA and FPA only depend on the ECG features with a fuzzy vault which is not very reliable due to dynamic signal variation [23], [27]. MBPSKA combines ECG-based fuzzy vault and fingerprint-based fuzzy commitment with error correction capability.

Similarly, Fig. 11 shows that the proposed MBPSKA scheme outperforms the baseline PSKA and FPA schemes with respect to FNMR, which demonstrates that the security of key distribution and agreement in a BAN can be enhanced by exploiting both the reliable biometric traits and the time-variant physiological signals and integrating them into a system along with fuzzy commitment and fuzzy vault algorithms.

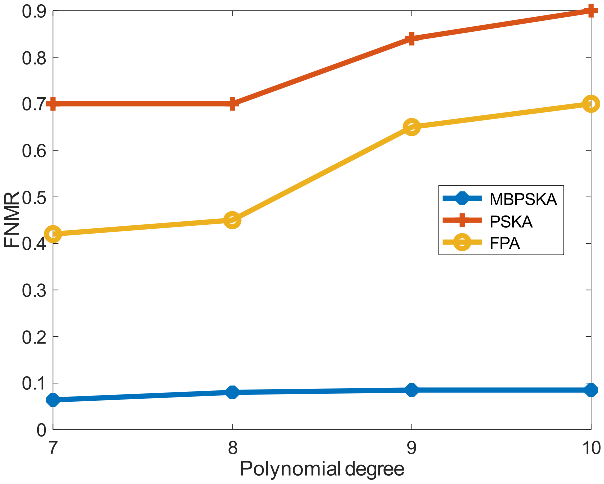


FIGURE 11. FNMR versus the polynomial degree for three different schemes: MBPSKA, PSKA, and FPA.

TABLE 2. Comparison of MBPSKA, PSKA and FPA in terms of HTER under different fuzzy vault polynomial degrees.

Poly Degree	HTER MBPSKA	HTER PSKA	HTER FPA
7	0.165	0.63	0.4975
8	0.1431	0.625	0.5125
9	0.10815	0.545	0.475
10	0.09685	0.54	0.45

In addition, the half total error rate (HTER), defined as (FMR + FNMR)/2, represents the performance of a system in terms of the overall key agreement error rate. Table 2 compares the HTER values of MBPSKA, PSKA, and FPA under different polynomial degrees of the fuzzy vault. MBPSKA performs better than PSKA and FMR in terms of HTER because it yields the lower FNMR and FMR values than PSKA and FPA, respectively.

Moreover, a receiver operating characteristic curve, or ROC curve, provides a useful tool for assessment of the system diagnostic ability and analysis of its relative operating characteristic by comparing two system characteristics GAR and FMR. For our biometric-based authentication and key agreement system, the ROC curve can be created by plotting the GAR against the FMR and it can also be considered as a plot of the successful key agreement probability or success rate as a function of the false positive rate or fall-out rate.

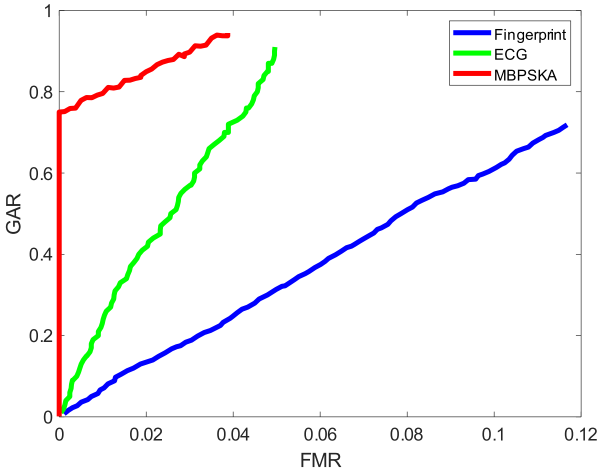


FIGURE 12. GAR versus FMR ROC curve for fingerprint fuzzy commitment, ECG fuzzy vault, and MBPSKA.

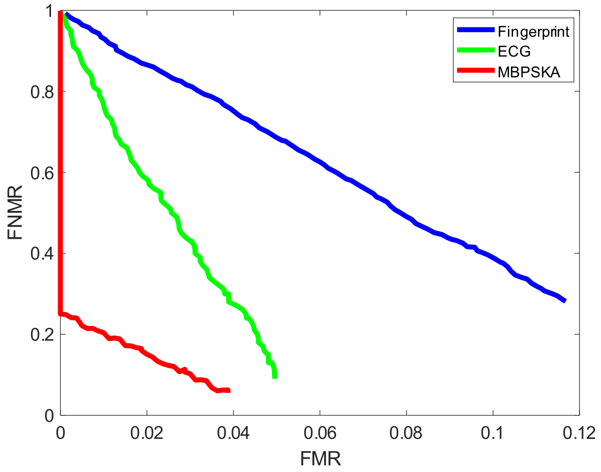


FIGURE 13. FNMR versus FMR ROC curve for fingerprint fuzzy commitment, ECG fuzzy vault, and MBPSKA.

We examined the operating characteristic of each module in our proposed MBPSKA system, i.e. only fingerprint-based fuzzy commitment and only the ECG-based fuzzy vault, as well as the system by integrating them. The GAR versus FMR ROC curve is illustrated in Fig. 12. In addition, the ROC curves of FNMR versus FMR are also plotted for the above three schemes in Fig. 13. The results from the ROC curves indicate that our proposed system by appropriately integrating fingerprint-based fuzzy commitment and the ECG-based fuzzy vault schemes offers much better performance than each individual scheme. As seen in Figs. 12 and 13, the proposed MBPSKA system achieved 93% GAR, 4% FMR, and 7% FNMR, while fingerprint fuzzy commitment had 72% GAR, 11% FMR and 28% FNMR, and the ECG fuzzy vault achieved 90% GAR, 5% FMR, and 10% FMNR.

B. COMMUNICATION OVERHEAD

We follow the method described in [22] to show the relationship between the communication overhead and the security strength for MBPSKA and PSKA. Essentially, FPA has the

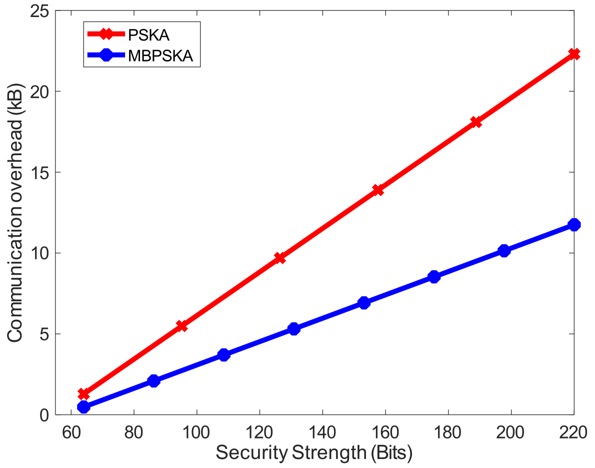


FIGURE 14. Communication overhead of PSKA and MBPSKA.

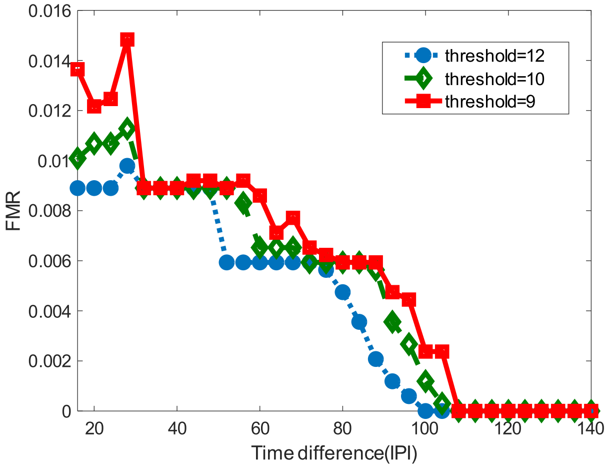


FIGURE 15. FMR versus the time difference between the IPI feature set for vault unlocking and the IPI feature set for vault locking.

same communication overhead as PSKA when given the same security strength. As mentioned in Section V, the security strength can be measured by the required amount of computation equivalent to a brute force attack on a random key of a particular bit size. In Fig. 14, as expected, the communication overhead increases with the security strength because more chaff points' data are transmitted from the sender to the receiver. Further, MBPSKA performs better than PSKA. As discussed before, the size of fuzzy commitment depends on the error correction code used, and the size of fuzzy vault depends on the number of chaff points. Thus, the overhead of fuzzy vault is much larger than that of fuzzy commitment although it has advantages such as data order invariance. PSKA only uses fuzzy vault, on the other hand, MBPSKA seamlessly integrates fuzzy commitment and fuzzy vault to protect the pairwise key in the key agreement protocol, which increases the security strength. If PSKA wants to achieve the same level of security as MBPSKA, many more chaff points are needed so that it incurs much larger communication overhead.

C. ECG SIGNAL TEMPORAL VARIANCE

The level of physiological signal temporal variance indicates the signal data randomness over time. A high level of signal temporal variance makes more difficult for an attacker to launch replay attacks using the messages protected by the features obtained from the previous physiological signals and also limits the attacker's ability to conduct offline analysis of multiple messages protected by the signal features. We analyzed the temporal variance of ECG signal features of the same subject, specifically, the false match rate (FMR) of the ECG-based fuzzy vaults. FMR here represents the possibility that one unlocks a fuzzy vault using the features extracted from the ECG signal of the same subject, but at a different time than the signal used for the fuzzy vault locking. As described before, our experiments involve extracting 4-bits from each of the 4 consecutive IPIs to form a 16-bit feature by employing the proposed IPI extraction method similar to that proposed in [44]. Fig. 15 depicts the FMR of a fuzzy vault when two sets of IPI features extracted from the ECG signals of the same subject at different times, are used for vault locking and unlocking, respectively. The X-axis represents the time difference between these two sets of asynchronous ECG signals in the number of IPIs. For example, a value of 25 on the X-axis represents a time difference of 25 IPIs, i.e. the signal features used for vault unlocking at the receiver have 25 IPIs of time delay from the signal features used for the vault locking at the sender. The FMR for several threshold values in the IPI extraction process are shown in the figure. It can be observed that the FMR decreases as the time difference between the IPI feature set for vault unlocking and the IPI feature set for vault locking because the correlation of these two sets of IPIs decreases with their time difference. On the other hand, the threshold values used in the IPI extraction process do not have much impact on the FMR. As shown in Fig. 15, FMR approaches zero as the time difference between the IPI feature sets for fuzzy vault locking and unlocking is above 100 IPIs (approximately equivalent to 1.5 minutes). Our results in Fig. 15 are consistent with the results presented in [22], [44].

VII. CONCLUSIONS

In this paper, we have presented the design of a new key agreement scheme, Multi-Biometric and Physiological Signal-based Key Agreement (MBPSKA), which exploits fingerprint-based fuzzy commitment and ECG-based fuzzy vault to enable two sensors to authenticate each other and to agree upon a shared cryptographic key for secure communications in a BAN. First, the analysis of the security characteristics demonstrates that MBPSK is robust against various attacks such as eavesdropping, brute force attacks, replay attacks, and man-in-the-middle attacks. Further, the performance of MBPSKA is evaluated and compared with that of the existing PSKA schemes such as PSKA and FPA using actual datasets of ECG signals and fingerprint images. The evaluation results show (i) the MBPSKA scheme can achieve a much higher Genuine Acceptance Rate (GAR) (93% with a fuzzy vault polynomial degree of 7) than that of PSKA (30%) and FPA (58%). The false match rate (FMR) is much lower for the proposed scheme (26% with a fuzzy vault polynomial degree of 7) than PSKA (56%) and FPA (57%). (ii) The communication overhead of MBPSKA is low while maintaining a high level of security. (iii) The ECG signals exhibits good temporal variance, which is consistent with other studies. The better performance of the proposed MBPSKA scheme is seen because it takes advantage of both the reliable biometric traits and the time-variant physiological signals to enhance the security and employs two layers of fuzzy cryptographic algorithms for authentication and key distribution in a BAN. In addition to superior security performance, MBPSKA can still provide the flexibility that allows the authorized people like doctors and nurses in an emergency room, to communicate with, control and reconfigure a patient's BAN devices without the direct input of the patient who might be unconscious or unable to communicate, which is an important feature for many life-saving scenarios. In summary, our studies show that MBPSKA is a secure, reliable and flexible intersensor key agreement scheme for BANs that outperforms the existing PSKA schemes.

For future work, we plan to build a prototype of the proposed MBPSKA scheme and conduct the experiments to validate our design in realistic scenarios. The actual performance as well as the computation and memory cost of MBPSKA will be evaluated using the prototype and compared with those of the existing schemes such as PSKA and FPA to understand the tradeoffs between the performance and complexity. Experimental studies will also be conducted to better understand the distinctiveness and temporal variance properties as well as energy consumption of the proposed scheme.

REFERENCES

[1] K. K. Venkatasubramanian and S. K. S. Gupta, "Security for pervasive health monitoring sensor applications," in *Proc. 4th Int. Conf. Intell. Sens. Inf. Process.*, Dec. 2006, pp. 197–202.

[2] L. Schwiebert, S. K. S. Gupta, and J. Weinmann, "Research challenges in wireless networks of biomedical sensors," in *Proc. 7th Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*, 2001, pp. 151–165.

[3] R. Schmidt, T. Norgall, J. Mörsdorf, J. Bernhard, and T. von der Grün, "Body area network BAN–a key infrastructure element for patient-centered medical applications," *Biomedizinische Technik/Biomed. Eng.*, vol. 47, no. s1a, pp. 365–368, 2002.

[4] J. Penders, J. van de Molengraft, L. Brown, B. Grundlehner, B. Gyselinckx, and C. Van Hoof, "Potential and challenges of body area networks for personal health," in *Proc. Annu. Int. Conf. IEEE Eng. Med. Biol. Soc.*, Sep. 2009, pp. 6569–6572.

[5] K. K. Venkatasubramanian, S. K. S. Gupta, R. P. Jetley, and P. L. Jones, "Interoperable medical devices," *IEEE Pulse*, vol. 1, no. 2, pp. 16–27, Sep./Oct. 2010.

[6] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao, and V. C. M. Leung, "Body area networks: A survey," *Mobile Netw. Appl.*, vol. 16, no. 2, pp. 171–193, Aug. 2010.

[7] G. Zheng, G. Fang, R. Shankaran, M. A. Orgun, and E. Dutkiewicz, "An ECG-based secret data sharing scheme supporting emergency treatment of implantable medical devices," in *Proc. Int. Symp. Wireless Pers. Multimedia Commun. (WPMC)*, Sep. 2014, pp. 624–628.

[8] M. Rostami, W. Burleson, F. Koushanfar, and A. Juels, "Balancing security and utility in medical devices?" in *Proc. 50th ACM/EDAC/IEEE Design Autom. Conf. (DAC)*, 2013, pp. 1–6.

[9] C. Li, A. Raghunathan, and N. K. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," in *Proc. IEEE 13th Int. Conf. e-Health Netw., Appl. Services*, Jun. 2011, pp. 150–156.

[10] M. R. Alshammari and K. M. Elleithy, "Efficient key distribution protocol for wireless sensor networks," in *Proc. IEEE 8th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2018, pp. 980–985.

[11] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proc. 9th ACM Conf. Comput. Commun. Secur.* New York, NY, USA: ACM, 2002, pp. 41–47.

[12] S. Zhu, S. Setia, and S. Jajodia, "LEAP+: Efficient security mechanisms for large-scale distributed sensor networks," *ACM Trans. Sensor Netw. (TOSN)*, vol. 2, no. 4, pp. 500–528, 2006.

[13] F. Liu, X. Cheng, L. Ma, and K. Xing, "SBK: A self-configuring framework for bootstrapping keys in sensor networks," *IEEE Trans. Mobile Comput.*, vol. 7, no. 7, pp. 858–868, Jul. 2008.

[14] F. Liu and X. Cheng, "LKE: A self-configuring scheme for location-aware key establishment in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 1, pp. 224–232, Jan. 2008.

[15] L. Ma, X. Cheng, F. Liu, F. An, and J. Rivera, "iPAK: An in-situ pairwise key bootstrapping scheme for wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 18, no. 8, pp. 1174–1184, Aug. 2007.

[16] M. Ahmed, B. Sanjabi, D. Aldiaz, A. Rezaei, and H. Omotunde, "Diffie-hellman and its application in security protocols," *Int. J. Eng. Sci. Innov. Technol.*, vol. 1, no. 2, pp. 69–73, 2012.

[17] S. Kumar and R. K. Singh, "Secure authentication approach using diffie-hellman key exchange algorithm for WSN," *Int. J. Commun. Netw. Distrib. Syst.*, vol. 17, no. 2, pp. 189–201, Jan. 2016. doi: 10.1504/IJCNDS.2016.079102.

[18] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, Nov. 1976.

[19] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "PSKA: Usable and secure key agreement scheme for body area networks," *IEEE Trans. Inf. Technol. Biomed.*, vol. 14, no. 1, pp. 60–68, Jan. 2010.

[20] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "Plethysmogram-based secure inter-sensor communication in body area networks," in *Proc. MILCOM IEEE Mil. Commun. Conf.*, Nov. 2008, pp. 1–7.

[21] S. R. Moosavi, E. Nigussie, S. Virtanen, and J. Isoaho, "Cryptographic key generation using ECG signal," in *Proc. 14th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2017, pp. 1024–1031.

[22] C. Hu, F. Zhang, X. Liao, X. Cheng, D. Wu, and D. Chen, "OPFKA: Secure and efficient ordered-physiological-feature-based key agreement for wireless body area networks," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 2274–2282.

[23] A. Juels and M. Sudan, "A fuzzy vault scheme," *Designs, Codes Cryptography*, vol. 38, no. 2, pp. 237–257, Feb. 2006.

[24] R. Paranjape, J. Mahovsky, L. Benedicenti, and Z. Koles, "The electroencephalogram as a biometric," in *Proc. Can. Conf. Elect. Comput. Eng. Conf.*, May 2001, pp. 1363–1366.

[25] M. Poulos, M. Rangoussi, and E. Kafetzopoulos, "Person identification via the EEG using computational geometry algorithms," in *Proc. 9th Eur. Signal Process. Conf. (EUSIPCO)*, Sep. 1998, pp. 1–4.

[26] U. Uludag, S. Pankanti, and A. K. Jain, "Fuzzy vault for fingerprints," in *Proc. Audio-Video-Based Biometric Person Authentication, 5th Int. Conf. AVBPA*, T. Kanade, A. Jain, and N. K. Ratha, Eds. Berlin, Germany: Springer, 2005, pp. 310–319.

[27] A. Nagar, K. Nandakumar, and A. K. Jain, "Multibiometric cryptosystems based on feature-level fusion," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 255–268, Feb. 2012.

[28] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proc. 6th ACM Conf. Comput. Commun. Secur.*, 1999, pp. 28–36.

[29] W. Burleson, S. S. Clark, B. Ransford, and K. Fu, "Design challenges for secure implantable medical devices," in *Proc. 49th Annu. Design Autom. Conf.*, 2012, pp. 12–17.

[30] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel, "Security and privacy for implantable medical devices," *IEEE Pervas. Comput.*, vol. 7, no. 1, pp. 30–39, Jan./Mar. 2008.

[31] N. Leavitt, "Researchers fight to keep implanted medical devices safe from hackers," *Computer*, vol. 43, no. 8, pp. 11–14, Aug. 2010.

[32] G. Venkatesan and C. Selvaraj, "Bio-sensor authentication for medical applications using WBAN," in *Proc. Int. Conf. Soft. Comput. Syst.* New Delhi, India: Springer, Dec. 2015, pp. 457–467.

[33] R. Cappelli, D. Maio, A. Lumini, and D. Maltoni, "Fingerprint image reconstruction from standard templates," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 9, pp. 1489–1503, Sep. 2007.

[34] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 561–572, Apr. 2007.

[35] K. Nandakumar, "A fingerprint cryptosystem based on minutiae phase spectrum," in *Proc. IEEE Int. Workshop Inf. Forensics Secur.*, Dec. 2010, pp. 1–6.

[36] F. Miao, S. Bao, and Y. Li, "A modified fuzzy vault scheme for biometrics-based body sensor networks security," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Dec. 2010, pp. 1–5.

[37] C. C. Tan, H. Wang, S. Zhong, and Q. Li, "Body sensor network security," in *Proc. 1st ACM Conf. Wireless Netw. Secur. (WiSec)*, 2008, pp. 148–153.

[38] D. J. Malan, M. Welsh, and M. D. Smith, "A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography," in *Proc. 1st Annu. IEEE Commun. Soc. Conf. Sensor Ad Hoc Commun. Netw.*, Oct. 2004, pp. 71–80.

[39] C. C. Tan, H. Wang, S. Zhong, and Q. Li, "IBE-lite: A lightweight identity-based cryptography for body sensor networks," *Trans. Inf. Technol. Biomed.*, vol. 13, no. 6, pp. 926–932, Jun. 2009.

[40] S. L. Keoh, E. Lupu, and M. Sloman, "Securing body sensor networks: Sensor association and key management," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun.*, Mar. 2009, pp. 1–6.

[41] M. Li, S. Yu, W. Lou, and K. Ren, "Group device pairing based secure sensor association and key management for body area networks," in *Proc. IEEE INFOCOM*, Mar. 2010, pp. 1–9.

[42] Y. W. Law, G. Moniava, Z. Gong, P. Hartel, and M. Palaniswami, "KALwEN: A new practical and interoperable key management scheme for body sensor networks," *Secur. Commun. Netw.*, vol. 4, no. 11, pp. 1309–1329, Dec. 2010.

[43] M. Li, S. Yu, J. D. Guttman, W. Lou, and K. Ren, "Secure ad hoc trust initialization and key management in wireless body area networks," *ACM Trans. Sensor Netw.*, vol. 9, no. 2, pp. 1–35, Mar. 2013.

[44] F. Xu, Z. Qin, C. C. Tan, B. Wang, and Q. Li, "IMDGuard: Securing implantable medical devices with the external wearable guardian," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 1862–1870.

[45] C. Hu, N. Zhang, H. Li, X. Cheng, and X. Liao, "Body area network security: A fuzzy attribute-based signcryption scheme," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 37–46, Sep. 2013.

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

[47] J. Shen, S. Chang, J. Shen, Q. Liu, and X. Sun, "A lightweight multi-layer authentication protocol for wireless body area networks," *Future Gener. Comput. Syst.*, vol. 78, pp. 956–963, Jan. 2018.

[48] 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. Netw.*, vol. 129, pp. 429–443, Dec. 2017.

[49] C.-M. Chen, B. Xiang, T.-Y. Wu, and K.-H. Wang, "An anonymous mutual authenticated key agreement scheme for wearable sensors in wireless body area networks," *Appl. Sci.*, vol. 8, no. 7, p. 1074, Jul. 2018.

[50] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.* Interlaken, Switzerland: Springer, 2004, pp. 523–540.

[51] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," *IEEE Trans. Comput.*, vol. 55, no. 9, pp. 1081–1088, Sep. 2006.

[52] C. C. Y. Poon, Y.-T. Zhang, and S.-D. Bao, "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health," *IEEE Commun. Mag.*, vol. 44, no. 4, pp. 73–81, Apr. 2006.

[53] S. Cherukuri, K. K. Venkatasubramanian, and S. K. S. Gupta, "Biosec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body," in *Proc. Int. Conf. Parallel Process. Workshops*, Oct. 2003, pp. 432–439.

[54] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "EKG-based key agreement in body sensor networks," in *Proc. IEEE INFOCOM Workshops*, Apr. 2008, pp. 1–6.

[55] R. M. Seepers, C. Strydis, I. Sourdis, and C. I. D. Zeeuw, "Enhancing heart-beat-based security for mHealth applications," *IEEE J. Biomed. Health Inform.*, vol. 21, no. 1, pp. 254–262, Jan. 2017.

[56] G. Zheng, G. Fang, R. Shankaran, M. A. Orgun, J. Zhou, L. Qiao, and K. Saleem, "Multiple ECG fiducial points-based random binary sequence generation for securing wireless body area networks," *IEEE J. Biomed. Health Inform.*, vol. 21, no. 3, pp. 655–663, May 2017.

[57] M. Karthikeyan and J. M. L. Manickam, "A novel fast chaff point generation method using bio-inspired flower pollination algorithm for fuzzy vault systems with physiological signal for wireless body area sensor networks," Biomed. Res. Int. J. Med. Sci., London, U.K., Tech. Rep. Special Issue: S242-S254, 2017.

[58] E. S. Reddy and I. R. Babu, "Authentication using fuzzy vault based on iris textures," in *Proc. 2nd Asia Int. Conf. Modelling Simulation (AMS)*, May 2008, pp. 361–368.

[59] W. J. Scheirer and T. E. Boult, "Cracking fuzzy vaults and biometric encryption," in *Proc. Biometrics Symp.*, Sep. 2007, pp. 1–6.

[60] B. Fu, S. X. Yang, J. Li, and D. Hu, "Multibiometric cryptosystem: Model structure and performance analysis," *IEEE Trans. Inf. Forensics Secur.*, vol. 4, no. 4, pp. 867–882, Dec. 2009.

[61] A. Kholmatov and B. Yanikoglu, "Realization of correlation attack against the fuzzy vault scheme," *Proc. SPIE*, vol. 6819, Mar. 2008, pp. 1–7.

[62] J. Bringer, H. Chabanne, G. Cohen, and B. Kindarji, "Theoretical and practical boundaries of binary secure sketches," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 4, pp. 673–683, Dec. 2008.

[63] M. van der Veen, T. Kevenaar, G.-J. Schrijen, T. H. Akkermans, and F. Zuo, "Face biometrics with renewable templates," *Proc. SPIE*, vol. 6072, Feb. 2006, Art. no. 60720J.

[64] H. Lu, K. Martin, F. Bui, K. N. Plataniotis, and D. Hatzinakos, "Face recognition with biometric encryption for privacy-enhancing self-exclusion," in *Proc. 16th Int. Conf. Digital Signal Process.*, Jul. 2009, pp. 1–8.

[65] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP J. Inf. Secur.*, vol. 2011, no. 1, p. 3, Sep. 2011.

[66] E. Maiorana, P. Campisi, and A. Neri, "IRIS template protection using a digital modulation paradigm," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, May 2014, pp. 3759–3763.

[67] Y. Zhu, T. Tan, and Y. Wang, "Biometric personal identification based on iris patterns," in *Proc. 15th Int. Conf. Pattern Recognit. (ICPR)*, Sep. 2000, pp. 801–804.

[68] C. M. Dharanesh, R. Prasad, and C. M. Patil, "Feature extraction classification for personal identification using iris," in *Proc. Int. Conf. Current Trends Comput., Electr., Electron. Commun. (CTCEEC)*, Sep. 2017, pp. 431–435.

[69] V. Conti, C. Militello, F. Sorbello, and S. Vitabile, "A frequency-based approach for features fusion in fingerprint and iris multimodal biometric identification systems," *IEEE Trans. Syst., Man, Cybern., C (Appl. Rev.)*, vol. 40, no. 4, pp. 384–395, Jul. 2010.

[70] M. Elhoseny, E. Essa, A. Elkhateb, A. E. Hassanien, and A. Hamad, "Cascade multimodal biometric system using fingerprint and iris patterns," in *Proc. Int. Conf. Adv. Intell. Syst. Inform.* Cairo, Egypt: Springer, Aug. 2017, pp. 590–599.

[71] Y. Wang, T. Tan, and A. K. Jain, "Combining face and iris biometrics for identity verification," in *Lecture Notes in Computer Science*. Berlin, Germany: Springer, 2003, pp. 805–813.

[72] D. Peralta, M. Galar, I. Triguero, D. Paternain, and S. García, E. Barrenechea, J. M. Benítez, H. Bustince, and F. Herrera, "A survey on fingerprint minutiae-based local matching for verification and identification: Taxonomy and experimental evaluation," *Inf. Sci.*, vol. 315, pp. 67–87, Sep. 2015.

[73] M. M. H. Ali, V. H. Mahale, P. Yannawar, and A. T. Gaikwad, "Fingerprint recognition for person identification and verification based on minutiae matching," in *Proc. IEEE 6th Int. Conf. Adv. Comput. (IACC)*, Feb. 2016, pp. 332–339.

[74] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. London, U.K.: Springer, 2009.

[75] L. Hong, Y. Wan, and A. Jain, "Fingerprint image enhancement: Algorithm and performance evaluation," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 20, no. 8, pp. 777–789, Aug. 1998.

[76] S. Chikkerur, C. Wu, and V. Govindaraju, "A systematic approach for feature extraction in fingerprint images," in *Biometric Authentication*. Berlin, Germany: Springer, 2004, pp. 344–350.

[77] D. Rutovitz, "Pattern recognition," *J. Roy. Stat. Soc. Ser. A (General)*, vol. 129, no. 4, p. 504, 1966. doi: 10.2307/2982255.

[78] A. Joshua, K. Paul, and G. Junbin, "Fingerprint matching using a hybrid shape and orientation descriptor," in *State of the art in Biometrics*. Rijeka, Croatia: InTech, 2011.

[79] X. Liang and T. Asano, "Fingerprint matching using minutia polygons," in *Proc. 18th Int. Conf. Pattern Recognit. (ICPR)*, 2006, pp. 1046–1049.

[80] H. Xu, R. N. J. Veldhuis, A. M. Bazen, T. A. M. Kevenaar, T. A. H. M. Akkermans, and B. Gokberk, "Fingerprint verification using spectral minutiae representations," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 3, pp. 397–409, Sep. 2009.

[81] K. Nandakumar, A. K. Jain, and S. Pankanti, "Fingerprint-based fuzzy vault: Implementation and performance," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 4, pp. 744–757, Dec. 2007.

[82] E. Marin, E. Argones-Rúa, D. Singelée, and B. Preneel, "A survey on physiological-signal-based security for medical devices," IACR Cryptol. ePrint Arch., Tech. Rep. 2016/867, Sep. 2016, vol. 2016, p. 867. [Online]. Available: ia.cr/2016/867

[83] S. A. Israel, J. M. Irvine, A. Cheng, M. D. Wiederhold, and B. K. Wiederhold, "ECG to identify individuals," *Pattern Recognit.*, vol. 38, no. 1, pp. 133–142, Jan. 2005.

[84] M. Rostami, A. Juels, and F. Koushanfar, "Heart-to-heart (H2H): Authentication for implanted medical devices," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2013, pp. 1099–1112.

[85] I. S. Reed and G. Solomon, "Polynomial codes over certain finite fields," *J. Soc. Ind. Appl. Math.*, vol. 8, no. 2, pp. 300–304, Jun. 1960.

[86] P. Mihailescu, "The fuzzy vault for fingerprints is vulnerable to brute force attack," Aug. 2007, *arXiv:0708.2974*. [Online]. Available: https://arxiv.org/abs/0708.2974

[87] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "FVC2002: Second fingerprint verification competition," in *Proc. 16th Int. Conf. Pattern Recognit.*, vol. 3. 2002, pp. 811–814.

[88] L. Yao, B. Liu, K. Yao, G. Wu, and J. Wang, "An ECG-based signal key establishment protocol in body area networks," in *Proc. 7th Int. Conf. Ubiquitous Intell. Comput. 7th Int. Conf. Autonomic Trusted Comput.*, 2010, pp. 233–238.

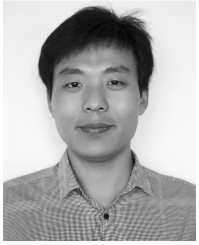
[89] J. Liu, Q. Li, R. Yan, and R. Sun, "Efficient authenticated key exchange protocols for wireless body area networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2015, no. 1, p. 188, Jul. 2015.

[90] A. L. Goldberger, L. A. Amaral, L. Glass, J. M. Hausdorff, P. C. Ivanov, R. G. Mark, J. E. Mietus, G. B. Moody, C.-K. Peng, and H. E. Stanley, "PhysioBank, PhysioToolkit, and PhysioNet: Components of a new research resource for complex physiologic signals," *Circulation*, vol. 101, no. 23, p. E215–E220, 2000.

[91] A. Taddei, G. Distante, M. Emdin, P. Pisani, G. B. Moody, C. Zeelenberg, and C. Marchesi, "The European ST-T database: Standard for evaluating systems for the analysis of ST-T changes in ambulatory electrocardiography," *Eur. Heart J.*, vol. 13, no. 9, pp. 1164–1172, Sep. 1992.

MANA AL RESHAN received the B.S. degree in information systems from King Khalid University, Abha, Saudi Arabia, in 2007, the M.S. degree (Hons.) in computer, information, and network security from DePaul University, Chicago, USA, in 2011, and the Ph.D. degree in computer science from The Catholic University of America (CUA), Washington, DC, USA, in 2019. He was a Teaching Assistant with the College of Computer Science and Information System, Najran University, Saudi Arabia, from 2007 to 2009. He was a Lecturer with the College of Computer Science and Information System, Najran University, in 2012, where he is currently an Assistant Professor. His current research interests include computer network and security, system security, wireless and mobile security, body area networks, and cloud security.

HANG LIU (M'98–SM'05) received the Ph.D. degree in electrical engineering from the University of Pennsylvania, Philadelphia, PA, USA. He joined The Catholic University of America (CUA), Washington, DC, USA, in 2013, where he is currently a Professor with the Department of Electrical Engineering and Computer Science. Prior to joining CUA, he had more than ten years of research experience in networking industry and was in senior research and management positions for several companies. He was an Adjunct Professor with the WINLAB, Department of Electrical and Computer Engineering, Rutgers University, from 2004 to 2012. His research interests include wireless communications and networking, Internet of Things, mobile computing, future Internet architecture and protocols, content distribution, video streaming, and network security. He was an Active Participant in the IEEE 802 wireless standards and 3GPP standards.



CHUNQIANG HU (M'13) received the B.S. degree in computer science and technology from Southwest University, Chongqing, China, in 2006, the M.S. and Ph.D. degrees in computer science and technology from Chongqing University, Chongqing, in 2009 and 2013, respectively, and the Ph.D. degree in computer science from The George Washington University, Washington, DC, USA, in 2016, where he was a Visiting Scholar, in 2011. He was a Postdoctoral Researcher with The Catholic University of America, Washington, DC, USA. He is currently a Researcher with the School of Software Engineering, Chongqing University. His current research interests include privacy-aware computing, big data security and privacy, wireless and mobile security, applied cryptography, and algorithm design and analysis. He is a member of ACM. He received the Best Paper Award in the ACM PAMCO 2016 and honored with the Hundred-Talent Program.

JIGUO YU received the Ph.D. degree from Shandong University, in 2004. He became a Full Professor with the School of Computer Science, Qufu Normal University, Shandong, China, in 2007. He is currently a Full Professor with the Qilu University of Technology (Shandong Academy of Sciences), Shandong Computer Science Center (National Supercomputer Center in Jinan), and a Professor with the School of Information Science and Engineering, Qufu Normal University. His research interests include privacy-aware computing, wireless networking, distributed algorithms, peer-to-peer computing, and graph theory. He is a member of ACM and a Senior Member of CCF.