Efficient Key Agreement Algorithm for Wireless Body Area Networks Using Reusable ECG-Based Features

Yasmeen Al-Saeed ¹, Eman Eldaydamony ¹, Ahmed Atwan ², Mohammed Elmogy ¹*, and Osama Ouda ¹,³*,

¹ Information Technology Department, Faculty of Computers and Information, Mansoura University, Mansoura 35516, Egypt; yasmeensaeed1654@gmail.com (Y.A.-S.); eman.8.2000@gmail.com (E.E.)
² Faculty of Computer Sciences and Information Technology, Northern Border University, Arar 9280, Saudi Arabia; atwan_2@yahoo.com
³ College of Computer and Information Sciences, Jouf University, Al-Jouf 2014, Saudi Arabia
* Correspondence: melmogy@mans.edu.eg (M.E.); omalsayed@ju.edu.sa (O.O.);
Tel.: +20-10-9888-9791 (M.E.); +966-56-001-6541 (O.O.)

Abstract: Wireless Body Area Networks (WBANs) are increasingly employed in different medical applications, such as remote health monitoring, early detection of medical conditions, and computer-assisted rehabilitation. A WBAN connects a number of sensor nodes implanted in and/or fixed on the human body for monitoring his/her physiological characteristics. Although medical healthcare systems could significantly benefit from the advancement of WBAN technology, collecting and transmitting private physiological data in such an open environment raises serious security and privacy concerns. In this paper, we propose a novel key-agreement protocol to secure communications among sensor nodes of WBANs. The proposed protocol is based on measuring and verifying common physiological features at both sender and recipient sensors prior to communicating. Unlike existing protocols, the proposed protocol enables communicating sensors to use their previous session pre-knowledge for secure communication within a specific period of time. This will reduce the time required for establishing the shared key as well as avoid retransmitting extracted features in the medium and hence thwarting eavesdropping attacks while maintaining randomness of the key. Experimental results illustrate the superiority of the proposed key agreement protocol in terms of both feature extraction and key agreement phases with an accuracy of 99.50% and an error rate of 0.005%. The efficacy of the proposed protocol with respect to energy and memory utilization is demonstrated compared with existing key agreement protocols.

Keywords: key agreement; Wireless Body Area Network (WBAN); inter-sensor communication; physiological feature-based key agreement; Electrical Cardiogaph (ECG); secure communication; resource saving algorithm; pattern recognition

1. Introduction

Wireless Body Area Networks (WBAN) are a wearable sensing and monitoring node with some processing and computing abilities. The primary purpose of WBAN is to improve the quality of life. Network sensors are either implanted or placed on the subject’s body. Each sensor consists of a sensing element, an analog-to-digital converter, wireless communication stack, processor, and memory. WBAN nodes can be divided into two types based on processing abilities. The first type is sensing and monitoring nodes, which are used to collect physiological and contextual data [1]. The second type is the sink node or sometimes called a personal server (PS), which is considered the most powerful part of the network in terms of processing, power, and storage. A personal server is mainly used as a network gateway (i.e., connects the network to the internet). WBAN uses wireless technology to enable sensor communication. The currently used wireless technology standard is IEEE 802.15.6. The connection within a WBAN (i.e., between two nodes or between nodes and PS) is called intra-WBAN communication. On the other
hand, the connection between PS and remote server through the internet is considered inter-WBAN communication. Figure 1 shows a WBAN contains two types of nodes, PS and physiological signal sensors; the sensors cannot send any data to a remote server except through PS.

![Figure 1. A Wireless Body Area Network (WBAN) contains two types of nodes, personal server (PS) and physiological signal sensors; the sensors cannot send any data to a remote server except through PS.](image)

WBAN applications are generally divided into two main categories: Medical and non-medical applications [2–6]. Medical applications are mainly associated with healthcare systems for patient tele-monitoring and disease detection. Medical applications can be subdivided into wearable WBAN, implanted WBAN, and remote control of medical device applications. Non-medical applications include WBAN applications, which are used mainly for entertainment and gaming purposes, such as virtual reality applications.

Information transmitted among WBAN sensors are private and hence should not be disclosed to adversaries. As a result, such information must be encrypted before transmission using a symmetric or asymmetric key. A symmetric key is a single unique key that is kept secret for both ciphering and deciphering operations. Thus, securing key distribution among communicating nodes is required. On the other hand, schemes that use an asymmetric key employ two complementary and mathematically related keys, public and private keys. The public key is assumed to be available (i.e., not kept as a secret), while the private key is kept a secret. Symmetric keys schemes are considered much faster and more efficient in key generation complexity than asymmetric schemes [7–9]. Asymmetric schemes have the advantages of eliminating the need for key distribution and are considered more secure, but it is computationally complex in terms of public/private keys generation. Due to WBAN’s sensors’ limited capabilities, symmetric-key schemes are used to secure sensor communication. To overcome symmetric algorithm limitations, key distribution algorithms are used [10].

Symmetric key schemes can be classified into three categories based on the source of the key: Pre-deployed keys, wireless channel characteristics-based keys, and biometric-based keys. Pre-deployed key is a procedure in which keying information is pre-distributed over the network sensors. This type benefits from eliminating key generation computations overhead, limiting losing efficiency as new sensors are added to the network [11]. The second type is a key generation based on wireless channel characteristics. This method is complex and costly in terms of computations overhead needed for the key establishment process [12]. Still, it has the advantage of avoiding processing overhead imposed during the
key generation in dynamic key generation schemes. The third type is key generation based on biometric data, such as iris and fingerprint (i.e., static biometric) or electrocardiogram (ECG) signals or any other dynamic biometric [13,14]. Biometric-based key agreement algorithms have the advantage of removing the need for key pre-distribution (i.e., plug and play) and noticed less memory consumption than the second type. The proposed method is considered a biometric-based key generation algorithm.

Existing biometric key agreement algorithms such as Physiological-Signal-Based Key Agreement (PSKA) [15] and Ordered-Physiological-Feature-Based Key Agreement (OPFKA) [16] assume that two communicating ends need to complete a new key agreement cycle to establish a secure connection session. The key agreement cycle consists of three stages: Signal collection and filtering features extraction and exchange, and finally, common features identification and key generation. Completing a key agreement cycle to generate a new random key is unavoidable, which wastes some WBAN resources in terms of processing, memory, and energy capabilities. Proposing a key agreement scheme that consumes less WBAN is highly required.

This paper’s main objective is to propose a key agreement that consumes low time and resources through the key agreement process without compromising security level or security key aspects. The proposed method algorithm enables two sensors that regularly connect to use some information from their previous connection to agree upon a new security key to secure their current communication for a specified period of time. The proposed method’s effect is supposed to last for a specific period of time specified by validation time. Validation time can be identified by an adaptive timer, which is mainly affected by the two communicating ends’ power levels.

The proposed method meets the design goals stated by Venkatasubramanian et al. [17] for biometrical and physiological based key agreement algorithms. It preserves the randomness, length, and efficiency of the generated keys. This paper’s main contribution is proposing a fast and light key agreement algorithm that saves resources between two regularly communicating sensors. This paper assumes that the communication medium is not secure. Hence, attackers can eavesdrop on WBAN’s connections, replay old messages, or inject messages. It does not consider sink-to-server communication security, jamming attacks, or electromagnetic interference.

The rest of this paper is organized as follows. Section 2 discusses the related work in terms of key agreement methods and physiological signals to be used. Section 3 describes the main steps of the proposed method in detail. The security analysis of the proposed method is presented in Section 4. The experimental results, along with the discussion, are presented in Section 5. Conclusions and future work are elucidated in Section 6.

2. Related Work

In this section, we will describe some related concepts, which are used in the proposed system. First, physiological signals concepts will be introduced in the first subsection. Then, key agreement categories are discussed in terms of the source of the security key.

2.1. Physiological Signal

This paper uses electrocardiogram (ECG) signal [18] as the main physiological signal. ECG is a descriptive signal for the heart’s electrical activity. Normal ECG signal consists of three parts. The first part is the P wave, which represents the heart’s atria depolarization. The second part is the QRS complex, which represents the ventricle depolarization. The last part is the T wave, which represents the relaxation of the heart at ventricle repolarization. Figure 2 shows an example of ECG signal main waves.
ECG signal attracted several researchers as prominent biometric due to its several properties of being universal, distinctive (i.e., discriminative characteristic between subjects), permanent (i.e., invariant for a person except in case of abnormalities), and easily collected with no user participation [19]. ECG signal has a wide range of applications, such as user identification and patient heart monitoring [20].

2.2. Key Agreement Methods

WBAN applications had been built on the same concept; that sensors collect and exchange data between them. WBAN is considered a very attractive target for attackers due to the sensitive nature of collected data and wireless technology used for communication. Thus, enabling security algorithms to secure WBAN communications is highly required.

Securing WBAN communications means preserving confidentiality, integrity, and authenticity for any WBAN connection. The usage of secret keys can ensure those security services encrypt WBAN communications. WBAN secret keys can be classified into three categories based on the source of the key: Pre-deployed keys, wireless channel characteristics-based keys, and biometric-based keys.

Pre-distributed security algorithms allow communicating sensors to use preinstalled keys to secure their communications. In these methods, keys are preinstalled/distributed in sensors memory before their deployment [21,22]. All key pre-distribution methods go through the same implantation path. The first stage is the key generation and distribution. At this stage, keys are generated and placed into the sensor’s memory before deploying sensors to a network. The second stage is the common key identification. At this step, both communicating ends search their memories for at least one common key to approve the connection. Finally, a secure link is established using that common key. Existing key pre-distribution schemes differ from each other by their superiority in one or more parameters. Those parameters are hardware cost, computational cost, local connectivity, global connectivity, and resiliency.

Key pre-distribution algorithms have the advantage of eliminating the overhead imposed by real-time key generation algorithms in terms of memory, computations, and energy consumption. Key pre-distribution algorithms have many limitations that limit their applicability in WBAN. First, wasted resources, such as memory consumed to store keys in each sensor. Furthermore, communicating ends may not identify common keys. Random key pre-distribution scheme [23], composite random key pre-distribution scheme [24], and the multipath reinforcement scheme [25] are examples of key pre-distribution algorithms.

Channel characteristics-based security keys were first proposed to replace public-key algorithms in network security. Those methods are physical layer security methods, which exploit signal randomness characteristics to generate a security key. The rapidly used channel characteristics are Received Signal Strength (RSS) [26], Channel State Information (CSI) [27], and Committed Information Rate (CIR) [28].

The key generation cycle based on channel characteristics can be divided into four stages: Channel sensing, quantization, information reconciliation, and privacy amplification. Channel sensing is the most important stage at which both communicating sensors

Figure 2. Electrocardiogram (ECG) signal main waves.
measure some randomness characteristic of the channel, such as the RSS time series \[29–31\]. In multi-bit quantization, gray coding may be used to reduce the key disagreement \[32\]. At the reconciliation stage, key bit mismatches or discrepancies at the two ends are discarded or corrected by employing information reconciliation protocols \[33\]. Finally, privacy amplification is performed. Privacy amplification aims to strengthen the matching keys by increasing key entropy and obfuscating any partial information an attacker may have gathered. Practically, it is hard to identify the amount of leaked information. This algorithm has the advantage of removing overhead posed on the sensors to identify the common features between them to generate a real-time key. However, this algorithm is infeasible in WBAN due to its high cost.

The usage sage of physiological signal-based key agreement algorithms to secure sensors’ communications was first introduced by \[17,34\]. They stated some basic assumptions. First, two communicating sensors must collect the same type of physiological signal simultaneously. Second, extracted features from collected signals form the basis of the key generation process. Finally, key agreement can be achieved if the communicating sensors have some common features. Due to the human body’s dynamic nature, physiological signals collected by sensors at different body locations tend to have similar trends rather than identical values. To deal with this fact, fuzzy vault-based schemes were proposed, such as PSKA \[15\] and OPFKA \[16\]. A fuzzy vault’s basic idea is to conceal legitimate features as they form the key’s basis by adding noisy data. The vector that contains legitimate features along with noisy data is called ‘the vault’.

Many key agreement algorithms were proposed based on the fuzzy vault idea, such as PSKA and Plethysmogram Key Agreement (PKA). PKA is a fuzzy vault key agreement scheme that uses the PPG signal as the main physiological signal. PKA algorithm performance was evaluated using two security aspects: Distinctiveness and temporal variance. The results showed that the PKA method had the advantages of being distinctive among subjects and maintained the freshness of the features at a given time (i.e., temporal variance). PKA suffered from two main limitations: The security level is fully dependable upon the generated vault’s size, and the acceptable security level is at the ninth polynomial. Vault size can be defined as the amount of noisy data added to legitimate features to make it harder for the adversary to recognize them; as vault size increases, security increases as well. The large vault size and high polynomial order imposed higher computation overhead, which was acceptable with the limited resources of the WBAN.

PSKA algorithm was proposed to extend the PKA algorithm and used ECG signal instead of PPG signal to enable two sensors to agree upon a symmetric key. Just as the PKA, the PSKA algorithm preserved the distinctiveness of the key among subjects along with a temporal variance of the features. PSKA suffered from requiring high polynomial order to maintain an acceptable security level (i.e., polynomial order of 12). Fuzzy vault algorithms’ security level mainly depends on the vault size. Unfortunately, vault size imposes more complexity in terms of computation and communication overheads, which is not preferred with WBAN limited resources.

To deal with fuzzy vault limitations, OPFKA was proposed. OPFKA reduced false rejection rates (FRR) resulting from large vault size usage to maintain an acceptable security level. This improvement was achieved using an ordering algorithm only known by communicating ends to order features inside the vault. OPFKA assumes that sensors use an ordering mechanism that is known only by the sensors generating features. OPFKA uses a noisy data addition technique to ensure features security. Thus, it has the same drawback as PSKA. OPFKA had the advantages of maintaining key distinctiveness, the temporal variance of the features, and lower computation overhead to discover common features between receiver’s features and received vault. Compared to PKA and PSKA methods, the OPFKA method archived a higher security level with much lower computations.

Symmetric-Key Generation Protocol (SGenP) \[35\] was proposed to generate a security key by applying two functions. First, Hash Message Authentication Code Feature Exchange (HMAC-FE) to secure feature exchange in the medium; then, Secret Key Construction func-
tion (SKC) to construct a secret key and secure communications between two ends. SGenP algorithm performance was mainly evaluated by energy consumption analysis through different agreement stages between two communicating ends. The results showed that SGenP generated security keys were of the length 128-bit. It offered some WBAN essential features such as plug-n-play, replaceability, scalability, flexibility, and easy refreshment of the security keys. SGenP has a fixed message size through the agreement process. This resulted in better energy consumption when compared with fuzzy vault algorithms with large vault size.

Tang et al. [36] proposed using a control unit to deal with the authentication process instead of communicated sensors themselves. They assumed that the control unit was holding a secret master key. This master key was used along with physiological signals and some random numbers to generate session security keys to secure connections between two sensors. This method performance was evaluated using several security aspects such as true recognition rates (TRR), the overhead imposed by communication and processing during the agreement process, and total energy consumed. Theoretically, the control unit saves much of the sensors’ resources, and its security is proven under decisional bilinear Diffie-Hellman (DBDL).

The key agreement based on key pre-distribution and channel characteristics methods is not widely used in WBAN, and the most used approach is a key agreement based on the physiological signal. This is basically due to the limited capabilities of sensor networks versus methods of implantation requirements.

3. The Proposed Method

3.1. WBAN Topology and Wireless Standard

WBAN is a short-range network, and its range is the human body. The preferred WBAN communication range is around 3 to 6 m. With a limited communication range, the most convenient topology is a simple star topology. By using star topology, two communicating sensors cannot communicate directly and need PS to proceed with their connection. This option is not considered by our proposed method. The proposed method assumes that two communicating sensors can connect directly without PS help. The usage of mesh topology can achieve this assumption. Due to limitations in the nature of WBAN in terms of short space, network architecture, transmission techniques, and communication protocols, the number of nodes in a WBAN is limited. Different standards are used in WBANs to enable the communications between WBAN sensors and sensors-PS communications. The most used standard is IEEE 802.15.6, which is a low-power wireless technology intended for short-range transmissions of WBANs, with around 10 Mbps of data rates. This standard provides capabilities to reduce the signal radiation absorption rate (SAR) caused by body movements.

3.2. The Proposed Key Agreement Method

The proposed method aims to enable two regularly communicating sensors to agree upon a new symmetric key using some previous connection features. The proposed method has the advantages of saving time and sensor resources without compromising security. The initial key agreement process between two sensors works as follows. First, two communicating sensors collect the same physiological signal type for a specified period, \( t \), simultaneously. Both sensors independently extract features from the collected signal and store them in two independent feature vectors. Each feature vector’s size is typically in the range of 12 to 24 features [37]. Extracted features at both sensors are dynamic (extracted in real-time) and ordered using an ordering algorithm known by the two sensors. After that, the sender sensor sends a validation time value and a noisy version of its feature vector. The validation time refers to the time period by which the collected features will be valid for subsequent communications. Since the two sensors collect the same signal type, the
receiver identifies the common features with a simple set intersection process between two feature vectors (i.e., the received noisy feature vector and receiver’s feature vector).

The intersection process outputs are common features’ values along with their indices in the receiver’s feature vector. The receiver uses the hash of identified common features as a key. The receiver sensor sends indices of identified features to the sender. The sender uses received indices to identify common features then hashing them to generate the key. Both sensors save the common features along with their indices for the timer validation period. In later communications between sensors that connected before, the sender sensor must check for timer validation first. If the timer period is valid, the sender sends a vector that contains common features’ indices, which are randomly permuted along with the hash of the new key generated. The new key is simply the output of hashing of features belong to indices permutation. The receiver simply uses the received indices and identifies the features, and then regenerates the key. Algorithm 1 demonstrates the basic idea of the proposed scheme, whose steps are discussed in detail later. Table 1 demonstrates the basic notations for the first/later connection. Our proposed method applies to any physiological signal. The only constraint on the communicating ends is they should collect the same type of physiological signal with a high synchronization level. Using different physiological signals will make no difference at the feature extraction stage as long as it is frequency domain with FFT. FFT features are the peaks of the frequency transformed signal. This paper uses the ECG signal to construct feature vectors used in the key agreement process.

Algorithm 1. The proposed method.

Step 1. Check the validation of the timer period
a) Check \( P \)-value
b) Start first connection if \( P = 0 \)
c) Start later connection if \( P \neq 0 \)

Step 2. Start key agreement using the first connection procedure when \( P = 0 \)
a) Start by sender and receiver having their feature vectors (i.e., \( FV_1 \) and \( FV_2 \), respectively)
b) The sender generates timer validation period \( P \) and sends \( P \) along with \( HFV_S \) to the receiver, where \( HFV_S = \text{Hashing}(FV_1) \)
c) The receiver receives \( HFV_S \) and starts to generate \( HFV_R \) by Hashing \((FV_2)\)
d) The receiver checks the authenticity of the sender by comparing \( HFV_S \) and \( HFV_R \)
e) After checking the sender’s authenticity, the key generation process starts at the receiver side by generation \( OFV_R \), where \( OFV_R = \text{Ordering algorithm}(FV_2) \)
f) Receiver side security key is generated by hashing \( OFV_R \), \( Key_R = \text{Hash}(OFV_R) \)
g) To ensure that the key is not transmitted through a medium, only the hash of the key \( HK_R \) will be sent to the sender to verify the key correction, where \( HK_R = \text{Hash}(Key_R) \)
h) The sender uses the same ordering method that was used by the receiver to generate \( OFV_S \)
i) The sender generates the security key \( Key_S \) by hashing \( OFV_S \)
j) Sender then generates \( HK_S \) by hashing its version of the security key. If \( HK_S = HK_R \), then \( Key_R \) and \( Key_S \) will be used as encryption keys, and success acknowledgment will be sent to the receiver.

Step 3. Start key agreement using the later connection procedure when \( P \neq 0 \)
a) The sender generates \( PM \) and uses it to produce a new version of its feature vector \( FV_1 \) as following: \( FV_{new\ S} = \text{Permute}(FV_1, PM) \)
b) The sender generates its new security key for this session using \( FV_{new\ S} \) as following \( Key_{new\ S} = \text{Hash}(FV_{new\ S}) \)
c) The sender generates a hash of the new generated key \( HK_{new\ S} \) and sends it along with \( PM \) to the receiver

d) The receiver uses \( PM \) to generate \( FV_{new\ R} \) as the following \( FV_{new\ R} = \text{Permute}(FV_2, PM) \)
e) The receiver generates its version of the session security key \( Key_{new\ R} \) as following: \( Key_{new\ R} = \text{Hash}(FV_{new\ R}) \)
f) To check the validity of \( Key_{new\ R} \), the receiver generates \( HK_{new\ R} \) by hashing \( Key_{new\ R} \)
g) If the \( HK_{new\ R} = HK_{new\ S} \), then \( Key_{new\ R} \) and \( Key_{new\ S} \) will be used to secure this session connection. If not, the first connection cycle will be started.
Table 1. The proposed algorithm notations identifications.

| Notation | Definition |
|----------|------------|
| HFV      | Hashed feature vector |
| OFV      | Ordered feature vector |
| HK       | Hashed key |
| HK_{new} | New hashed key |
| IDs      | Sender ID |
| IDr      | Receiver ID |
| FV_{new} | New features vector |
| P        | Period for timer validation |
| No       | Nonce (i.e., Random number for transaction refreshment) |
| MAC      | One-way hashing function |
| PM       | Permutation matrix |
| ||       | Concatenate symbol |
| Key_{new}| The new key generated based on PM |

3.2.1. First Connection Key Agreement Cycle

The main aim of the first key agreement cycle is to identify the validation timer period; by which the generated features vector can be reused for other connections. By the end of this cycle, both communicating ends keep a copy of their feature vector until the timer’s period ends. Figure 3 demonstrates the basic flow chart for the first connection cycle. This subsection demonstrates the first connection’s key agreement cycle in detail.

Figure 3. The first connection’s cycle flowchart.

(1) **Physiological signal collection and filtering**: Two sensors must collect physiological signals for a predefined period. Signal’s collection period and level of synchronization mainly depend on the features extraction method to be used. After the signal’s collection, there is a filtering step to remove any noise in the collected signal. The proposed method uses ECG signal as the main physiological signal. ECG signal feature extraction methods suffer from high noise sensitivity. Therefore, noise reduction techniques must be used as a preprocessing step before the feature’s extraction process. Many sources of ECG signal noises can affect the quality of the extracted features. The most significant sources of ECG artifacts are muscle and motion artifacts (see Figure 4).
Figure 4. The sources of ECG noises.

Muscle artifacts are high-frequency noises, while motion artifacts are low-frequency noises. ECG noises can be removed using the Pan–Tompkins algorithm [21] (see Figure 5). The Pan–Tompkins algorithm is an ECG signal filtering algorithm. It highly depends on the fact that the QRS portion consumes the most power of the ECG signal. So, it is amplifying QRS while reducing the rest of the signal portions along with noises.

![Diagram of the Pan–Tompkins algorithm for filtering ECG signal.](image_url)

**Figure 5. Pan–Tompkins algorithm for filtering ECG signal.**

**(2) Features extraction using the modified FFT version:** Features extraction methods significantly impact any physiological-based key agreement algorithm’s efficiency. The main feature extraction job is reducing unauthorized access rates while enhancing authorized access rates. This can be done by extracting the most useful features that best describe the physiological signal. The collected signals at both sensors are not entirely identical. Instead, they have large signals’ overlapped portions in common. Below, we discuss a modified version of the Fast Fourier Transform method (FFT). The same feature extraction method can be used under the same concept with different physiological signals by simple parameters modification. FFT method is the frequency-domain method that transforms the input signal from its domain (i.e., time or space) into the frequency domain. Spectral information of the collected signal is represented using sine and cosine waves. FFT has superiority over existing feature extraction methods due to its speed and lower synchronization level needed. Our modified FFT signal is applying the normal FFT method but with a higher synchronization level. This is done to eliminate the need for the feature exchange step. If two sensors collect the same physiological signal simultaneously and with high synchronization, this implies that the signal at both ends is almost identical.
Input is N points physiological signal while the output is two parts, each with N/2 samples. As stated by the well-known Nyquist theorem [38], \( f_{\text{max}} \) (i.e., the maximum frequency that can be represented by FFT) is at N/2, and only the first N/2 values are used. Implementing FFT with varying input signal length is first proposed in [15,16]. The proposed method was first implemented original FFT method by varying ECG lengths ranging from 2 to 12 s, with a low synchronization level. The proposed FFT based feature extraction method can be summarized as follows:

1) Collect ECG signal for at least 4 s with a high synchronization level.
2) Clean the collected signal with low / high pass filters.
3) Partition signal samples into two overlapped equal-size windows.
4) Apply 256-points FFT and use only the first 128 FFT coefficients.
5) Apply peak detection function to the first 128 FFT coefficients. The peak detection function output is in the form of tuple \(<\text{peak index}, \text{peak value}>\).
6) Quantize each peak index into binary number with 5-digits and each peak value into 8-digits binary number.
7) A 13-bit feature is constructed by a simple concatenation process between each quantized peak index and its corresponding quantized.
8) The final output will be a feature vector containing extracted quantized features.

By the end of feature extraction algorithm both communicating sensors has its own feature vector (i.e., \( \text{FVs} = \{fs_1 \ldots fs_N\} \) for sender and \( \text{FVr} = \{fr_1 \ldots fr_N\} \) for receiver).

(3) **Key generation and period generation:** Security key is generated by hashing feature vector. The hashing function used is a one-way hashing function (i.e., MD5 and SHA-265). The validation timer period is calculated using an equation (See Section 3.3). The validation period equation mainly depends on two factors, sensors’ power level and connection frequency rate. This means if two sensors connect frequently and have a higher power level, then a longer validation period will be used. Once the key is generated, the sender sends the following message to the receiver:

**Sender to Receiver:** \( ID_s, ID_r, \text{No}, \text{Mac (Key)}, P \)

(4) **Receiver-side key generation and acknowledgment:** Receiver regenerates security key using its feature vector using a simple hashing function. The generated key is validated by comparing the received key hash with the generated one hash. If two hashes match, then success acknowledgment is sent to the sender using the following message:

**Receiver to Sender:** \( \text{MAC (Key} || \text{ID}_r || \text{ID}_s || \text{No}) \)

If the two hashes did not match, the connection request is ended, and the new key cycle will be started. If the process of key generation failed at the receiver, the receiver retries to regenerate the key for one more time. If failed, the key agreement process will be ended, and the two communicating sensors’ authentication will be failed. Figure 6 illustrates the key generation process.

(5) **Success acknowledgments and session start permission:** After receiving the previous message, the sender sends the same message as success acknowledgment. The success acknowledgment is to permit the session and connection to start.

**Sender to Receiver:** \( \text{MAC (Key} || \text{ID}_r || \text{ID}_s || \text{No}) \)

By the end of this process, there are two subsequences. First, the key generated is used to ensure the first connection’s security. Second, the feature vector, along with the validation period for later communications security, will be stored in each communication ends.
Key generation

Success

Yes

Verify key correction

Send success acknowledgment

No

End key agreement

Retry

Yes

Fail?

End key agreement

Verify key correction

In later connections, two previously connected ends use their feature vector saved from the first connection to re-agree about a common key. This will help in reducing overhead imposed in the computation and communication step. This algorithm reduces agreement process time while preserving the key’s randomness and freshness along with resource-saving advantage. Figure 7 illustrates the basic flow chart of the later connection’s key agreement process. As we can notice from Figure 7, the main decision of approving the agreement process mainly depends on timer validation. Timer validation controls the way the algorithm will follow. If the timer is valid, then the random permutation matrix generates a new feature vector to generate a new random key. If not, then a new normal key agreement cycle as the first connection is started.

Figure 6. The key generation process at the receiver side.

3.2.2. Later Connection Key Agreement Cycle

In later connections, two previously connected ends use their feature vector saved from the first connection to re-agree about a common key. This will help in reducing overhead imposed in the computation and communication step. This algorithm reduces agreement process time while preserving the key’s randomness and freshness along with resource-saving advantage. Figure 7 illustrates the basic flow chart of the later connection’s key agreement process. As we can notice from Figure 7, the main decision of approving the agreement process mainly depends on timer validation. Timer validation controls the way the algorithm will follow. If the timer is valid, then the random permutation matrix generates a new feature vector to generate a new random key. If not, then a new normal key agreement cycle as the first connection is started.

Figure 7. The later connection’s cycle flowchart.

(1) Checking period validation: The core of later communication is the validation timer. Checking validation of the timer period is nothing but checking the ability to reuse the first connection’s feature vector. If the timer is valid, then approve later connection key
cycle. If not, this means the stored feature vectors at both ends will be deleted, and a new key agreement cycle will be started (i.e., new first connection cycle).

2) **Random permutation matrix generation and new feature vector generation:** Since the key is nothing but the hash of the feature vector, the vector’s new arrangement of features will guarantee the key’s freshness. For this reason, a random permutation matrix (PM) is generated and used to re-order features within the feature vector.

3) **Key generation:** A new random key is generated by applying a simple hashing function to the feature vector modified by PM. Example 1 illustrates the basic idea of this step. After completion of this step, the receiver sends the following message to the sender:

Receiver to Sender: *Mac (Key*$_{\text{new}}$), ID$_{\text{r}}$, ID$_{\text{s}}$, No, PM*

4) **Key recovering and acknowledgment:** Sender uses the received PM to regenerate the same new feature vector as a receiver. Then, a hashing function is applied to recover the security key. The success acknowledgment is sent as the following message:

Sender to Receiver: *Mac (Key*$_{\text{new}}$ || ID$_{\text{r}}$ || ID$_{\text{s}}$ || No)*

### Example 1: The basic idea of the proposed method

**Given:**
Feature vector with the following values:

\[1, 2, 5, 10, 12\]

1st connection key:

\[\text{Key} = \text{hash } (1 \mid 2 \mid 5 \mid 10 \mid 12)\]

2nd connection key:

\[\text{PM} = [5, 3, 1, 4, 2]\]

\[\text{Key}_{\text{new}} = \text{hash } (12 \mid 5 \mid 1 \mid 10 \mid 2)\]

**Conclusion:**

Altering the position of features will guarantee the freshness of the new session key.

### 3.3. Timer Period Calculation and Key Refreshing Rate

Timer validation period $P$ is assumed to be directly proportional to available power level $PL$ in sensors when communication starts. $P$ is also proportional to connection frequency factor $fc$ (i.e., a number that indicates how many times two sensors are connected through a predefined period) (See Equations (1) and (2)). A more extended period will be used with higher power levels, and when the sensor connects regularly.

\[P \propto PL \times fc\]  

\[P = k \times PL \times fc = k \times ((PL_S + PL_R)/2) \times fc\]

where $PL_S$ and $PL_R$ are the power levels at the sender and recipient, respectively, as shown in Equation (2), $PL$ is the average of two power levels in the two sensors. Constant $k$ is assumed to equal 1/100 for normalization purposes. Since validation period $P$ has a high impact in key refreshing (i.e., the longer the timer period, the more times the key must be refreshed), we simply assumed that key must refresh one time for every session within the period (i.e., for each session in $P$ there is a unique key).

The proposed method aims to save existing resources and prolong sensor battery life. So, if the power level (PL) is under 25%, the battery level is critical, and to help save its life, the proposed timer method is not applicable. Table 2 illustrates the timer calculation for different PL and fc.
4. Security Analysis

This section analyzes the proposed algorithm’s security in terms of the key agreement cycle in first and later connections.

- **First connection key agreement cycle:** For the first connection cycle, the only keying information to be transferred in the communication medium is the hashing of the common key. The security of legitimate features is assured because features are not transmitted in the medium since two communicating ends collect the same signal and extract the same features. This will make feature identification a very hard task for an attacker. This paper assumes that sensors are secure and connection medium may not. Secure key transmission is assured by exchanging only MAC (i.e., hashing function) instead of the plain key. Key hashing knowledge is useless for the attacker’s key guessing process, because it cannot get hands-on features. The Nonce No usage maintains the connection’s freshness; hence, avoid using the old message to break the connection.

- **Later connection key agreement cycle:** The security of a later connection depends on the fact that there is no feature transmission on the communication medium. All the legitimate features are stored securely in communicating node memories. We assume that all sensors are under supervision, and no sensor can be compromised without being detected. Hence, the attacker can try key guessing using the information transmitted in the media. The only keying information to be exchanged is the key hash; the MAC of the key will ensure the key security. Knowing key hashing will add nothing to the attacker in the key guessing process. Key refreshing, even though the timer period is still valid, will help in making the attacker task harder. Even after the timer ends, all the information stored will be erased. This means a new first connection cycle; hence, updating of data to be guessed.

5. Experimental Results and Discussion

This section discusses the proposed method’s experimental results using the original FFT method (see Table 3) and proposed a modified FFT version (see Table 4) to extract ECG features. FFT method is mainly used due to its advantages of being fast and in-dependency on the extracted features.

| ECG Length in Seconds | Sensitivity | Specificity | Efficiency | FAR | FRR | Accuracy | Error Rate |
|-----------------------|-------------|-------------|------------|-----|-----|----------|------------|
| 4                     | 0.7765      | 0.5185      | 0.7621     | 0.4815 | 0.2235 | 0.7879 | 0.2120     |
| 6                     | 0.7944      | 0.4402      | 0.7747     | 0.5598 | 0.2056 | 0.7802 | 0.2198     |
| 8                     | 0.7704      | 0.6212      | 0.7621     | 0.3788 | 0.2296 | 0.8602 | 0.1398     |
| 10                    | 0.7783      | 0.5086      | 0.7633     | 0.4914 | 0.2217 | 0.8013 | 0.1987     |
| 12                    | 0.7299      | 0.5196      | 0.7144     | 0.4804 | 0.2741 | 0.7671 | 0.2329     |
Table 4. The proposed method experimental results with the modified FFT method.

| ECG Length in Seconds | Sensitivity | Specificity | Efficiency | FAR    | FRR    | Accuracy | Error Rate |
|-----------------------|-------------|-------------|------------|--------|--------|----------|------------|
| 4                     | 0.7295      | 0.9087      | 0.7394     | 0.0913 | 0.2705 | 0.96974  | 0.0303     |
| 6                     | 0.7909      | 0.9316      | 0.7987     | 0.0684 | 0.2091 | 0.9898   | 0.0102     |
| 8                     | 0.7732      | 0.9491      | 0.7829     | 0.0509 | 0.2268 | 0.98207  | 0.0179     |
| 10                    | 0.7956      | 0.9444      | 0.8039     | 0.0556 | 0.2044 | 0.99505  | 0.0050     |
| 12                    | 0.7431      | 0.9744      | 0.7559     | 0.0256 | 0.2569 | 0.99159  | 0.0084     |

ECG-based FFT algorithm has three parameters: Sampling rate, sampling duration, and FFT points. The used sampling rate is 128 Hz, and 256-point FFT is applied. The experiments were implemented using MATLAB 2017 and MIT database [39]. This database includes 18 long-term ECG recordings of subjects. Subjects included in this database were found to have had no significant arrhythmias; they include 5 men, aged 26 to 45, and 13 women, aged 20 to 50. The original and modified FFT version’s main difference is the synchronization level used. The original FFT version uses a low synchronization level, by which only a small part of the collected signal match in the feature matching stage. The modified FFT version overcomes this issue by using a high synchronization level, by which 100% of the collected signal match.

The usage of a high synchronization method to extract ECG features was proposed in [16]. Unfortunately, the proposed method was a time-domain method and required excessive input signal to give good results and work well (i.e., the method requires about 1 to 1.5 min). The extracted features were dependent and gave no information about the input signal’s spectral values (i.e., did not characterize signal well). The proposed modified FFT method takes advantage of requiring low input signal length from the original FFT, with high synchronization just like time methods. The experiment was implemented with the same parameters as the original FFT but with higher synchronization instead of lower synchronization. This will secure features by eliminating the need for their transmission. Hence significantly reduce computation overhead needed for noisy points’ computations and common features identification. It has the advantage of reducing the collision rate to zero. Figure 8 illustrates that the proposed method can discriminate well between genuine sensor connection and imposters connections.

![Histogram for the imposter and genuine scores](image1.png)

![Histogram for the imposter and genuine scores modified FFT](image2.png)

**Figure 8.** Histogram for the imposter and genuine scores; (a) the proposed method with original FFT, (b) the proposed method with modified FFT.
This section’s experimental results are expressed in terms of sensitivity, specificity, efficiency, False Acceptance Rate (FAR), False Rejection Rate (FRR), accuracy, and error rate. Sensitivity or True Acceptance Rate (TAR) measures the portion of genuine scores that were correctly identified as genuine. Specificity or True Rejection Rate (TRR) measures the portion of imposters’ scores that were correctly identified as imposters’ scores. Accuracy measures the system’s ability to generate accurate outputs that is close to the originally expected outputs. Ideal accurate systems have TAR and TRR equal to 1 or FAR and FRR equal to 0. The error rate is also a measure of system quality and is calculated using an accuracy value. FAR measures the portion of imposters’ scores that were falsely identified as genuine scores. FRR is the genuine scores that were identified as imposters scores. Efficiency is a quality measure that mainly depends on specificity, sensitivity, and accuracy. True Positive (TP) indicates the number of genuine scores, which are correctly classified as genuine. True Negative (TN) indicates the number of impostor scores that were correctly identified as an imposter. False Negative (FN) indicates the number of genuine scores that were mistakenly identified as an imposter. False Positives (FP) indicates the number of imposters scores that were mistakenly identified as genuine ones.

\[
\text{Sensitivity} = \frac{TP}{TP + FN} = 1 - \text{FRR} \quad (3)
\]
\[
\text{Specificity} = \frac{TN}{TP + FN} = 1 - \text{FAR} \quad (4)
\]
\[
\text{Accuracy} = \frac{(TP + TN)}{(TP + TN + FP + FN)} \quad (5)
\]
\[
\text{Efficiency} = \frac{(\text{Sensitivity} + \text{Specificity} + \text{Accuracy})}{3} \quad (6)
\]

Table 3 shows the original FFT method’s experimental results with different ECG input length in seconds from 4 to 12 s. The results shown in Table 3 are the results until the cut-off of 0.60 (i.e., the hamming distance between features). The results analysis shows that the lowest error rate and highest accuracy with the original FFT method are achieved when the input ECG signal’s length is 8 s. The highest accuracy achieved by the original FFT method was 86.02%, with an error rate of 0.1398. As illustrated by Figure 8a, the original FFT method failed to distinguish genuine sensor connection and imposters connections.

In the case of the modified FFT method with a high synchronization level, the communicating ends are well synchronized. Hence, almost 100% of the collected signals at both ends matches. Table 4 shows the results of FFT with high synchronization experiment. As shown by Table 4, a huge decrease in FAR rates and massive enhancement in accuracy was achieved compared to those results in Table 3. Figure 8b shows that the FFT with high synchronization level can distinguish very well between genuine sensor connection and imposters connections. The conclusion is that high synchronization rate is an important factor in achieving the best accuracy with any ECG signal length and enhancing the authentication process.

In this experiment, we noticed that with lower input length, the number of extracted features is decreased. Hence, the number of noisy points to secure their transmission will be reduced as well. This may result in lower common feature identification time and computations. It also results in a higher collision rate, hence, lower accuracy. As shown in Figure 8a, the original FFT method is considered a good but not excellent method to discriminate between legitimate and unauthorized sensors. Table 5 compares the experimental results between our proposed method and other methods. As shown in Table 5, the proposed method achieves the lowest error rate with the highest accuracy.

The superiority of our method comes from two main factors: High synchronization and feature extraction using FFT. First, the usage of high synchronization levels to collect physiological signals. High synchronization was used to authenticate sensors and verify that two communicating sensors are in the same WBAN. Still, it is also used by our method not to transmit legitimate features in the medium. So, each communicating sensor will have its own version of the feature vector identical to the other end without transmitting features in the medium. This will increase the security and accuracy of our method over
the other key agreement method. The FFT method’s usage as the feature extraction method is advantageous in speeding the feature extraction process. Unlike time-domain feature extraction methods, the features extracted by frequency-domain methods are independent. This because time domain features are time intervals between two waves or peaks. For ECG signals, time-domain features are the interval between two successive R waves, and it is denoted as Inter-Pulse-Interval (IPI) [16].

Table 5. The proposed method experimental results compared with other methods.

| Method   | Sensitivity | Specificity | FAR    | FRR    | Accuracy | Error Rate |
|----------|-------------|-------------|--------|--------|----------|------------|
| PKA      | 0.7605      | 0.4131      | 0.2754 | 0.7807 | 0.2192   |            |
| PSKA     | 0.7861      | 0.5299      | 0.4701 | 0.2139 | 0.8047   | 0.1953     |
| OPFKA    | 0.8750      | 0.5729      | 0.4271 | 0.1250 | 0.9317   | 0.0683     |
| SGenP    | 0.8822      | 0.6724      | 0.3576 | 0.1478 | 0.9210   | 0.0790     |
| PBAKA    | 0.8695      | 0.6271      | 0.3381 | 0.1144 | 0.9407   | 0.0593     |
| Our method | 0.7956      | 0.9444      | 0.0556 | 0.2044 | 0.9950   | 0.0050     |

Another experiment was conducted to evaluate the proposed method in comparison with existing WBAN key agreement schemes; PSKA [15], OPFKA [16], PKA [34], SGenP [35], and PBAKA [36]. The evaluation process was based on the following security aspects: Key length and randomness, memory consumption, power consumption, communication and transmission cost, distinctiveness, and temporal variance. Evaluation results show the superiority of our algorithm in first and later communications.

1. **Key Length and randomness**: The generation of long and random security keys is ensured by using a one-way hashing function (i.e., MD5).
2. **Communication and feature transmission cost**: The cost of the identification number for sender and receiver (i.e., IDs and IDr) is 16 bytes each. Connection refreshment number No is 16 bytes. Index I and permutation matrix PM are at most 1 byte. The timer validation period P is 1 byte, and MAC is 16 bytes. Here, features and noisy data points are represented by 12 or 13 bit each (i.e., about 1.5 bytes). For PBAKA, transaction information T_s and T_r are 20 bytes each. Table 6 shows that our algorithm offers the lowest communication overhead among the presented schemes.

Table 6 calculates the total size of messages exchanged through the agreement process. As shown by the message size column, all the presented fuzzy vault schemes have variable length factor NFV. The average length of NFV is 1000 to 3000. So, the message size is 4.5 KB and 13.2 KB, respectively. For the SGenP algorithm, the message size is 1.33 KB, and for the PBAKA method, it is 604 bytes. The proposed method has superiority over fuzzy vault schemes since message size is fixed and there is no variable-length NFV parameter. The proposed method also has superiority over SGenP and the PBAKA method since its communication cost is 258 bytes for both the first and later communication stages combined. Figure 9 illustrates the total communication overhead in bytes for our method and other methods.

3. **Energy consumption**: The sensor consumes 28.2 mJ to receive one byte and 59.2 mJ to transmit it [40]. As shown in Table 7, our algorithm gives the lowest energy consumption. We used the message size calculated earlier by communication overhead and calculates how many bytes will be transmitted and received during the agreement cycle. After counting the bytes for each method, we calculated the energy consumed, as illustrated by Table 7. Table 7 shows that the proposed method has the lowest energy consumption compared to other methods. The values of NFV are 1000, 3000, and 1000 for PKA, PSKA, and OPFKA, respectively. The value of F_s and F_r is 100.
Table 6. Communication overhead for first/later connections.

| Method  | First Connection | Later Connection | Message Size | Cost Analysis |
|---------|------------------|------------------|--------------|---------------|
| PKA     | $2|ID_s| + 2|ID_r| + 4.5|NFV| + |No| + 2|Mac| | $2|ID_s| + 2|ID_r| + 4.5|NFV| + |No| + 2|Mac| | 112 + 4.5|NFV| bytes | In PKA analysis, NFV length is set to be 1000. So, the final cost is 4.5 KB |
| PSKA    | $2|ID_s| + 2|ID_r| + 4.5|NFV| + |No| + 2|Mac| | $2|ID_s| + 2|ID_r| + 4.5|NFV| + |No| + 2|Mac| | 112 + 4.5|NFV| bytes | PSKA set NFV length to be 1000 and 3000. So, the final cost is 4.5 KB and 13.2 KB, respectively. |
| OPFKA   | $2|ID_s| + 2|ID_r| + 2.5|NFV| + |I| + |No| + 2|Mac| | $2|ID_s| + 2|ID_r| + 2.5|NFV| + |I| + |No| + 2|Mac| | 113 + 2.5|NFV| bytes | If NFV is 1000, then total cost is 2.5 KB. |
| SGenP   | $2|ID_s| + 2|ID_r| + |No| + 2|Mac| + |HMac| + 2|String| | $2|ID_s| + 2|ID_r| + |No| + 2|Mac| + |HMac| + 2|String| | 1.33 KB | HMAC is 600 bytes and random string is 20 bytes length. |
| PBAKA   | $2|ID_s| + 2|ID_r| + 2.5|Fs| + 2.5|F_r| + T_s + T_r | $2|ID_s| + 2|ID_r| + 2.5|Fs| + 2.5|F_r| + T_s + T_r | 104 + 2.5|Fs| + 2.5|F_r| bytes | In PBAKA analysis, $F_s$ and $F_r$ lengths are 100. As a result, the final cost will be 604 bytes. |

The proposed method

| Method | First connection: | Later connection: |
|--------|-------------------|-------------------|
|        | 129 bytes         | 129 bytes         |

Message size is fixed.
The proposed method:

\[ 2|ID_s| + 2|ID_r| + 1.5|F| + 3|Mac| + |P| + |PM| \]

The energy consumption for first/later connections.

| Algorithm   | First Connection | Later Connections | Total Energy Consumed |
|-------------|------------------|-------------------|-----------------------|
| PKA         | 112 + 4.5|NFV| \times (28.2 + 59.2) | 112 + 4.5|NFV| \times (28.2 + 59.2) | 403.088 mJ |
| PSKA        | 112 + 4.5|NFV| \times (28.2 + 59.2) | 112 + 4.5|NFV| \times (28.2 + 59.2) | 1189.688 mJ |
| OPFKA       | 113 + 2.5|NFV| \times (28.2 + 59.2) | 113 + 2.5|NFV| \times (28.2 + 59.2) | 228.367 mJ |
| SGenP       | 1368 \times (28.2 + 59.2) | 1368 \times (28.2 + 59.2) | 1361.92 mJ |
| PBAKA       | 104 + 2.5|F_s| + 2.5|F_r| \times (28.2 + 59.2) | 104 + 2.5|F_s| + 2.5|F_r| \times (28.2 + 59.2) | 52.789 mJ |
| The proposed method | 129 \times (28.2 + 59.2) | 129 \times (28.2 + 59.2) | 11.274 mJ |

Figure 9 illustrates the total communication overhead in bytes for the proposed method and other methods.

Table 7. The energy consumption for first/later connections.

Figure 10 illustrates the total energy consumption of the proposed method along with other methods.

4. **Memory storage:** Memory storage means the amount of memory consumed during the key agreement process. As we can see from the results in Table 8, our algorithm shows better memory storage results.

Figure 10. Total energy consumption in mJ for the proposed method and other methods.
This mainly because the proposed method has a fixed message size in both first and later connections. The only part of the proposed method stores the feature vector for the first connection and the feature vector. The timer validation period for the later connections.

The fuzzy vault methods such as PKA, PSKA, and OPFKA; need to store variable-length parameter NFV. NFV vector has an average length of 1000 to 3000 data points. Each point is represented by 1.5 bytes. The memory cost for IDs and IDR is 16 bytes each. No is 16 bytes, I and permutation matrix PM are at most 1 byte., P is 1 byte, and MAC is 16 bytes. The value of NFV is 1000 for PKA and OPFKA, and its value is 3000 with PSKA. Each NFV point is represented by 1.5 bytes. For SGenP, HMAC is 60 bytes, and the random string is 20 bytes in length. In PBKA analysis, Fs and F lengths are 100, and T, T, r, s are 20 bytes each. The total memory overhead per connection in bytes is 6862, 20362, 3863, 3900, and 644 for PKA, PSKA, OPFKA, SGenP, and PBKA, respectively. For the proposed method, communicating sensors will save their feature vector. We will denote it as F; F is much smaller than NFV (i.e., F << NFV), and its size is about 100 features. The first connection’s total memory cost is 311 bytes and is 312 bytes for the later connections. Figure 11 illustrates the memory overhead in bytes for our method and the other methods for the first connection.

5. **Distinctiveness**: Distinctiveness means the ability of an algorithm to best discriminate between authorized sensors from unauthorized ones (i.e., distinguish sensors in the same WBAN from those in another WBAN). This can be achieved by using a modified version of FFT with a high synchronization level. High synchronization level ensures that only sensors that are willing to communicate in the same WBAN can connect securely.

6. **Temporal variance**: Higher temporal variance implies that signal’s better randomness. The higher the randomness, the harder it is getting to comprise network security. Signals collected at different times are generally unique. However, if the time difference between two successive signal readings is so close, the collected signal values will be

---

### Table 8. Memory cost for first/later connections.

| Algorithm       | First Connection                                      | Later Connection                                      |
|-----------------|-------------------------------------------------------|-------------------------------------------------------|
| PKA             | \[2|ID| + 2|ID| + 4.5|NFV| + |No| + 2|Mac|\] bytes | \[2|ID| + 2|ID| + 4.5|NFV| + |No| + 2|Mac|\] bytes |
| PSKA            | \[2|ID| + 2|ID| + 2.5|NFV| + |I| + |No| + 2.5|Mac|\] bytes | \[2|ID| + 2|ID| + 2.5|NFV| + |I| + |No| + 2.5|Mac|\] bytes |
| OPFKA           | \[2|ID| + 2|ID| + 2|NFV| + |No| + 2|Mac|\] bytes | \[2|ID| + 2|ID| + 2|NFV| + |No| + 2|Mac|\] bytes |
| SGenP           | \[2|ID| + 2|ID| + 4|NFV| + |No| + 2|Mac|\] bytes | \[2|ID| + 2|ID| + 4|NFV| + |No| + 2|Mac|\] bytes |
| PBKA            | \[2|ID| + 2|ID| + 2.5|F| + 2.5|F| + |T| + |T| + |r| + |s|\] bytes | \[2|ID| + 2|ID| + 2.5|F| + 2.5|F| + |T| + |T| + |r| + |s|\] bytes |
| The proposed method | \[2|ID| + 2|ID| + 1.5|F| + 3|Mac| + |P|\] bytes | \[2|ID| + 2|ID| + 1.5|F| + 3|Mac| + |P|\] bytes |

---

**Figure 11.** Memory overhead in bytes for the proposed method and other methods.
similar [16]. The proposed method solves close readings/similar values problem and achieves better temporal variance than the other schemes. This is mainly by using period $P$.

7. **Low latency:** Sampling duration needed for secure key agreement highly depends on the physiological signal used [16]. As illustrated in the discussion section, when FFT is used to extract ECG signal, at least 4 s is needed with 128 Hz sampling rate. PBAKA needs at least 12.6 s.

6. **Conclusions and Future Work**

This paper proposed a secure, fast, and resource-efficient WBAN key agreement algorithm. The proposed method allows two sensors to use previous connection information to agree upon a new and random key. Existing key agreement algorithms assumed that the two communicating sensors must go through the new key agreement cycle for every connection; even the two sensors were connected and agreed upon a previous key. For previously connected sensors that agreed upon a key in the previous session, going through a new cycle for a new random key generation will waste some resources that can be saved. Saving WBAN resources can be achieved by saving the previous session common feature vector for a predefined period to be used for later connections’ key agreement between those two sensors. The proposed method’s performance was analyzed in terms of overhead imposed by communication and computational processes and the amount of memory needed. The results indicate the applicability, efficiency, and reliability of the proposed method. Keys generated had the properties of randomness and efficiency.

In the future, we plan to enhance the first connection by using an adaptive chaff points generator. Adaptive chaff points generator generates an appropriate amount of chaff points to the security level estimated by the sensors. This will help in reducing the collision rate between legitimate features and noisy data. In addition, we intend to reshape the first connection in a way that improves memory and energy consumption. We also plan to estimate lengths for new feature extraction methods such as wavelet with new physiological signals such as Photoplethysmogram (PPG).

**Author Contributions:** Conceptualization, Y.A.-S., E.E., A.A. and O.O.; methodology, Y.A.-S., E.E., A.A., M.E. and O.O.; software, Y.A.-S.; validation, E.E. M.E. and O.O.; formal analysis, Y.A.-S., M.E. and O.O.; investigation, A.A.; resources, E.E., A.A. and O.O.; data curation, Y.A.-S., E.E. and A.A.; writing—original draft preparation, Y.A.-S., M.E. and O.O.; writing—review and editing, Y.A.-S., M.E. and O.O.; visualization, Y.A.-S., M.E. and O.O.; supervision, E.E., A.A. and O.O.; project administration, M.E. and O.O.; funding acquisition, M.E. and O.O. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Data Availability Statement:** The used dataset is a benchmark dataset from MIT ECG database and it is available online for download from the following link: https://physionet.org/.

**Conflicts of Interest:** The authors declare no conflict of interest.

**References**

1. Venkatasubramanian, K.K.; Gupta, S.K.S. Security for Pervasive Health Monitoring Sensor Applications. In Proceedings of the 2006 Fourth International Conference on Intelligent Sensing and Information Processing, Bangalore, India, 15 October–18 December 2006; pp. 197–202.

2. Tobón, D.P.; Falk, T.H.; Maier, M. Context awareness in WWBNAs: A survey on medical and non-medical applications. *IEEE Wirel. Commun.* **2013**, *20*, 30–37. [CrossRef]

3. O’Donoghue, J.; Herbert, J.; Sammon, D. Patient Sensors: A Data Quality Perspective. In Proceedings of the International Conference on Smart Homes and Health Telematics (iCOST 2008), Ames, IA, USA, 28 June–2 July 2008; pp. 54–61.

4. O’Donoghue, J.; Herbert, J. Data Management within mHealth Environments. *J. Data Inf. Qual.* **2012**, *4*, 1–20. [CrossRef]

5. Lai, D.T.H.; Begg, R.K.; Palaniswami, M. *Healthcare Sensor Networks: Challenges towards practical implementation*; CRC Press: Boca Raton, FL, USA, 2011.

6. O’Donoghue, J.; Herbert, J.; Fensli, R.; Dineen, S. Sensor Validation within a Pervasive Medical Environment. In Proceedings of the 2006 5th IEEE Conference on Sensors, Daegu, Korea, 22–25 October 2006. [CrossRef]
7. Boyd, C. On key agreement and conference key agreement. In Proceedings of the Australasian Conference on Information Security and Privacy (ACISP 1997), Sydney, Australia, 7–9 July 1997; pp. 294–302.
8. Kumar, P.; Lee, S.-G.; Lee, H.-J. E-SAP: Efficient-Strong Authentication Protocol for Healthcare Applications Using Wireless Medical Sensor Networks. IEEE Sens. J. 2012, 12, 1625–1647. [CrossRef] [PubMed]
9. Jana, S.; Premnath, S.N.; Clark, M.; Kasera, S.K.; Patwari, N.; Krishnamurthy, S.V. On the effectiveness of secret key extraction from wireless signal strength in real environments. In Proceedings of the 15th Annual International Conference on Mobile Computing and Networking (MobiCom 09), Beijing, China, 20–25 September 2009; pp. 321–332.
10. Diffie, W.; Hellman, M. New directions in cryptography. IEEE Trans. Inf. Theory 1976, 22, 644–654. [CrossRef]
11. Du, W.; Deng, J.; Han, Y.S.; Varshney, P.K.; Katz, J.; Khalili, A. A pairwise key pre-distribution scheme for wireless sensor networks. ACM Trans. Inf. Syst. Secur. 2005, 8, 228–258. [CrossRef]
12. Wilhelm, M.; Martinovic, I.; Schmitt, J. Secure Key Generation in Sensor Networks Based on Frequency-Selective Channels. IEEE J. Sel. Areas Commun. 2013, 31, 1779–1790. [CrossRef]
13. Chen, Y.; Ge, Y.; Wang, W.; Yang, F. A Biometric-based User Authentication and Key Agreement Scheme for Heterogeneous Wireless Sensor Networks. KSII Trans. Internet Inf. Syst. 2018, 12, 1779–1798.
14. Hei, X.; Du, X. Biometric-based two-level secure access control for Implantable Medical Devices under emergencies. In Proceedings of the IEEE Annual Joint Conference: INFOCOM, IEEE Computer and Communications Societies, Shanghai, China, 10–15 April 2011; pp. 346–350.
15. Venkatapurubamanian, K.K.; Banerjee, A.; Gupta, S.K.S. PSKA: Usable and Secure Key Agreement Scheme for Body Area Networks. IEEE Trans. Inf. Technol. Biomed. 2009, 14, 60–68. [CrossRef] [PubMed]
16. Hu, C.; Cheng, X.; Zhang, F.; Wu, D.; Liao, X.; Chen, D. OPPKA: Secure and efficient Ordered-Physiological-Feature-based key agreement for wireless Body Area Networks. In Proceedings of the IEEE Annual Joint Conference: INFOCOM, IEEE Computer and Communications Societies, Turin, Italy, 14–19 April 2013; pp. 2274–2282.
17. Venkatapurubamanian, K.K.; Banerjee, A.; Gupta, S.K. EKG-based key agreement in Body Sensor Networks. In Proceedings of the IEEE Conference on Computer Communications Workshops, INFOCOM Wksp, Phoenix, AZ, USA, 13–18 April 2008; pp. 1–6.
18. Available online: https://en.wikipedia.org/wiki/Electrocardiography (accessed on 4 February 2021).
19. Karimian, N.; Guo, Z.; Tehranipoor, M.; Forte, D. Highly Reliable Key Generation from Electrocardiogram (ECG). IEEE Trans. Biomed. Eng. 2016, 64, 1400–1411. [CrossRef]
20. Arefin, T.; Ali, M.H.; Haque, A.K.M.F. Wireless Body Area Network: An Overview and Various Applications. J. Comput. Commun. 2017, 5, 53–64. [CrossRef]
21. Pan, J.; Tompkins, W.J. A Real-Time QRS Detection Algorithm. IEEE Trans. Biomed. Eng. 1985, BME-32, 230–236. [CrossRef] [PubMed]
22. Hu, R.; Duan, X.; Jiang, H.; Zeng, P.; Jiang, Y. Pair-Wise Key Pre-Distribution Scheme for Wireless Sensor Networks. In Proceedings of the 2012 8th International Conference on Wireless Communications, Networking and Mobile Computing, Shanghai, China, 21–23 September 2012. [CrossRef]
23. Rasheed, A.; Mahapatra, R.N. Key Predistribution Schemes for Establishing Pairwise Keys with a Mobile Sink in Sensor Networks. IEEE Trans. Parallel Distrib. Syst. 2010, 22, 176–184. [CrossRef]
24. Fu, J.; Li, Q.; Li, S.; Ssanyu, L. A modified q-composite random key pre-distribution scheme based on kryptograph. In Proceedings of the 2010 International Conference on Computer Application and System Modeling (ICCASM 2010), Taiyuan, China, 22–24 October 2010. [CrossRef]
25. Di Mauro, A.; Dragoni, N. Adaptive Multipath Key Reinforcement for Energy Harvesting Wireless Sensor Networks. Procedia Comput. Sci. 2015, 63, 48–55. [CrossRef]
26. Liu, H.; Yang, J.; Wang, Y.; Chen, Y. Collaborative secret key extraction leveraging Received Signal Strength in mobile wireless networks. In Proceedings of the IEEE Annual Joint Conference: INFOCOM, IEEE Computer and Communications Societies, Orlando, FL, USA, 25–30 March 2012. [CrossRef]
27. Van Torre, P. Channel-Based Key Generation for Encrypted Body-Worn Wireless Sensor Networks. Sensors 2016, 16, 1453. [CrossRef] [PubMed]
28. Zhang, Z.; Wang, H.; Vasilakos, A.; Fang, H. Channel information based Cryptography and Authentication in Wireless Body Area Networks. In Proceedings of the 8th International Conference on Body Area Networks (BodyNets 13), Brussels, Belgium, 30 September–2 October 2013. [CrossRef]
29. Mathur, S.; Trappe, W.; Mandayam, N.; Ye, C.; Reznik, A. Radio-telepathy: Extracting a Secret Key from an Unauthenticated Wireless Channel. In Proceedings of the 14th ACM International Conference on Mobile Computing and Networking (MobiCom 08), San Francisco, CA, USA, 14–19 September 2008; pp. 128–139.
30. Sudarsono, A.; Yuliana, M.; Kristalina, P. A Reciprocity Approach for Shared Secret Key Generation Extracted from Received Signal Strength in The Wireless Networks. In Proceedings of the 2018 International Electronics Symposium on Engineering Technology and Applications (IES-ETA), Bali, Indonesia, 29–30 October 2018; pp. 170–175.
31. Croft, J.; Patwari, N.; Kasera, S.K. Robust uncorrelated bit extraction methodologies for wireless sensors. In Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN 10), Stockholm, Sweden, 12–16 April 2010. [CrossRef]
32. Patwari, N.; Croft, J.; Jana, S.; Kasera, S.K. High-Rate Uncorrelated Bit Extraction for Shared Secret Key Generation from Channel Measurements. *IEEE Trans. Mob. Comput.* 2009, 9, 17–30. [CrossRef]
33. Brassard, G.; Salvail, L. Secret-Key Reconciliation by Public Discussion. In Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques (EUROCRYPT 1993), Lofthus, Norway, 23–27 May 1993; pp. 410–423.
34. Venkatasubramanian, K.K.; Banerjee, A.; Gupta, S.K.S. Plethysmogram-based secure inter-sensor communication in Body Area Networks. In Proceedings of the 2008 IEEE Military Communications Conference (MILCOM 2008), San Diego, CA, USA, 16–19 November 2008. [CrossRef]
35. Kumari, P.; Anjali, T. Symmetric-Key Generation Protocol (SGenP) for Body Sensor Network. In Proceeding of the 2018 IEEE International Conference on Communications Workshops (ICC Workshops), Kansas City, MO, USA, 20–24 May 2018; pp. 1–6.
36. Tang, W.; Zhang, K.; Ren, J.; Zhang, Y.; Shen, X.S. Flexible and Efficient Authenticated Key Agreement Scheme for BANs Based on Physiological Features. *IEEE Trans. Mob. Comput.* 2018, 18, 845–856. [CrossRef]
37. Juels, A.; Sudan, M. A fuzzy vault scheme. *Des. Codes Cryptogr.* 2006, 38, 237–257. [CrossRef]
38. Nilsson, J.; Panizza, M.; Hallett, M. Principles of digital sampling of a physiologic signal. *Electroencephalogr. Clin. Neurophysiol. Evoked Potentials Sect.* 1993, 89, 349–358. [CrossRef]
39. Goldberger, A.; Amaral, L.; Glass, L.; Hausdorff, J.; Ivanov, P.C.; Mark, R.; Stanley, H.E. PhysioBank, PhysioToolkit, and PhysioNet: Components of a new research resource for complex physiologic signals. *Circulation* 2000, 101, 215–220. [CrossRef] [PubMed]
40. Ren, K.; Lou, W.; Zeng, K.; Moran, P.J. On Broadcast Authentication in Wireless Sensor Networks. *IEEE Trans. Wirel. Commun.* 2007, 6, 4136–4144. [CrossRef]