Mansoura Journal of Computers and Information Sciences

FREKA: Fast Resource Efficient Key Agreement Algorithm within Body Area Network

Yasmeen Al-Saeed Eman Eldaydamony Osama Ouda Ahmed Atwan

Department of Information Technology, Faculty of Computer and Information Sciences, Mansoura University, Mansoura 35516, Egypt

Yasmeensaeed1654@gmail.com eman.8.2000@gmail.com oudaosama@yahoo.com atwan_2@yahoo.com

Abstract

Body area network (BAN) considered a hot research topic and attracted many researchers due to its increasing applications. Providing light, fast and efficient key agreement algorithm to secure inters-sensor communications is critical challenge. In this paper, we present an enhanced algorithm that enables two sensors to use previous connection's pre-knowledge to fast the later connections key agreement process. Our algorithm saves sensor's resources, key agreement cycle's time and preserves randomness of the key. Results imply the efficiency, applicability and security of FREKA. Compared with OPFKA algorithm, our algorithm achieves better power and memory consumption. In addition, it requires lower computational operations.

General Terms

Security, Pattern Recognition, Algorithms.

Keywords

Key Agreement; Wireless Body Area Network (WBAN); Inter- sensor communication; Physiological feature based key agreement.

1. Introduction

Body area network (BAN) is a wireless sensors network that is used to monitor physiological and environmental data [1]. BANs had attracted many biomedical engineering researchers due to its several applications [2-6]. One of the most common applications is providing medical real time monitoring for patients [1]. BAN applications had been built on the same concept; that sensors collect and exchange data between them. BAN''s sensors usually collect data from human body (i.e. physiological signals) such as: blood pressure, heart rate and body temperature; as well as data about surrounding environment such as: humidity. BAN has been considered as a very attractive target for attackers, due to the sensitivity of collected data and the usage of wireless technology for sensors' communications. Thus, enabling security algorithms to secure BAN communications is highly desired. BAN's communication security means to preserve confidentiality, integrity and authenticity for each network sensor's communication. Those security services can be ensured by using encryption keys. Security keys used in BAN can be generally classified into two main approaches: symmetric keys and asymmetric keys. Symmetric key approach uses single unique key which kept as secret for both ciphering and deciphering operations. Because of this, securing key distribution among communicating nodes is required. On the other hand, asymmetric security key schemes use two complementary and mathematically related keys, public and private keys. Public key is assumed to be available (i.e. not kept as secret). On the other hand, private key is kept as a secret. Symmetric keys schemes are considered much faster and more efficient in terms of key generation complexity when compared to asymmetric schemes. Asymmetric schemes have the advantages of eliminating the need for key distribution and considered more secure; but it is computationally complex in terms of public/private keys generation. Due to the limited capabilities of BAN's sensors, symmetric key schemes are used to secure sensors communication. To overcome symmetric algorithms limitations, key distribution algorithms are used.

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. First type is pre-deployed key where keying information pre-distributed over the network sensors. This type has the benefit of eliminating key generation computations overhead, with limitation of losing efficiency as new sensors added to network [7]. Second type is key generation based on wireless channel characteristics. This method is complex and costly in terms of computations overhead needed for key establishment process [8]. On other hand, it has the advantage of avoiding processing overhead, imposed during key generation in dynamic key generation schemes. 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 [9-10]. Biometric based key agreement algorithms have the advantage of removing the need of key pre-distribution (i.e. plug and play) along with noticed

less memory consumption when compared to second type. Our work will be concerned with biometric based key generation algorithms.

Existing biometric physiological key agreement algorithms such as Physiological-Signal-Based Key Agreement (PSKA) [11] and Ordered-Physiological-Feature-Based Key Agreement (OPFKA) [12] assumed that for every connection the two communicating sensors must go through new key agreement cycle (even the two sensors were connected and agreed upon a key, previously). The basic idea of key agreement cycle was built on the top of same concept in all about excising algorithms as follows: 1) the two sensors that are willing to communicate should collect same type of physiological signals with some form of synchronization; 2) each sensor generates its feature vector and exchange it other communication partner to identify common features; 3) common features are used to generate a key used to secure communication.

For previously connected sensors that agreed upon a key in previous session; going through new cycle for the sake of new random key generation will waste some resources that can be saved. This can be done using previous session's feature vector. This paper proposes an enhanced algorithm termed *Fast Resource Efficient Key Agreement (FREKA)* that will help in saving resources for sensors that previously connected and agreed upon a common key. This can be achieved by saving previous session common feature vector for predefined period to be used for later connections' key agreement between those two sensors. FREKA algorithm is meant to be fastening key agreement process. Since FREKA uses some pre-knowledge from previous session, this will help in reducing processing overhead, as well as time needed for key agreement. The effect of FREKA is supposed to last for specific period of time specified by validation time. Validation time for FREKA's later connection can be identified by adaptive timer. Timer is mainly affected by sensor's power level. FREKA is working as following: 1) features generated by each sensor are ordered and saved in feature vector; 2) the sender sends features along with number that indicates the validation period for later connections to the receiver; 3) the receiver used the received feature vector to remark the common features along with its indices; 4) a key is generated by using one way hashing function on the common features; 5) for any later connection within timer validation period, new random key will be generated using hashing of a random permutation of the saved feature vector. FREKA is meant to be meeting the design goals stated by [13] for biometrical- physiological based key agreement algorithms. FREKA ensures to preserve randomness, long length and efficiency of the generated keys. The main contribution of this paper is proposal of FREKA, a fast and light algorithm for saving recourses used for key agreement process between two previously connected sensors. Keys generated had the properties of randomness and efficiency.

This paper (i) compares FREKA to OPFKA [12], the comparison showed that FREKA algorithm demonstrates superiority over OPFKA for later communications, (ii) analyzes the performance of FREKA in terms of overhead imposed by communication and computational processes and amount of memory needed, the results indicate applicability, efficiency and reliability of FREKA, (iii) discusses feature extraction algorithm and implements an experiment to estimate best input signal time needed for each method; to enhance accuracy and reduce key agreement process time.

The rest of this paper is organized as follows. Section 2 reviews the related work. System model of our algorithm is discussed in Section 3. The basic idea of FREKA is presented in Section 4. Security analysis is presented in Section 5 and performance analysis in Section 6. Finally, conclusion is discussed in Section 7.

2. Related Work

Previous researches in BAN security were concerned with how to (i) generate and agree upon key [14-17], (ii) encrypt data [18-20], (iii) ensure authorized access control [18, 21, 22].

Usage of physiological signal-based key agreement algorithms to secure sensors' communications was first introduced in [23-24]. They stated some basic assumptions. First, sensors that are willing to communicate should collect same type of physiological signal simultaneously. Second, features extracted from collected signals form the basis for the key generation process. Finally, to agree upon common key, sensors should have a common set of features. Because of dynamic nature of human body, physiological signals collected by sensors at different location of the body will tend to have similar trends rather than identical values. To deal with this fact fuzzy vault-based schemes were proposed [25-27]. The basic idea of fuzzy vault is to conceal legitimate features that form the basis of the key by adding some sort of noisy data to construct vault. Based on the idea of fuzzy vault, many key agreement algorithms had been raised such as: PSKA [11] and Plethysmogram [25]. Both algorithms used the same fuzzy vault scheme unless PSKA [11] uses ECG signal as the main physiological signal while Plethysmogram [25] uses PPG signal. Fuzzy vault algorithms security level mainly depends on the vault size. Vault size can be defined as the amount of noisy data added to legitimate features to make it harder for adversary to recognize them. As vault size increases security increases as well. Unfortunately, vault size imposes more complexity in terms of computation and communication overheads. To deal with fuzzy vault limitations, authors in [12] proposed OPFKA. OPFKA uses the idea of features ordering. OPFKA assumes that sensors use ordering mechanism that is known only by the sensors generating features. OPFKA uses noisy data addition technique to ensure features security. Thus, it has the same drawback as PSKA [11]. Authors in [28] proposed a symmetric key agreement protocol with a fixed communication message length. This gives them superiority over OPFKA [12] with large coffer size.

Authors in [29] proposed the use of control unit to launch authentication process. This can be done by the usage of pre-deployed master key at control unit. A new unique session key can be generated based on physiological signal and some random numbers. This method highly depends on hardness of the hash function.

All algorithms mentioned above assume that two sensors must go through a new key agreement cycle every time they are willing to communicate. This assumption possess overhead that can be avoided between the two sensors that

Table 1. Summary of related work for key agreement schemes in WBAN

Paper title	Author	Year	Brief description	Evolution aspects	Results	FRR	FAR	EER
Biosec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body [23]	S Cherukuri et al.	2003	Proposal of usage of physiological signals to secure WBAN communications.	-	-	-	-	-
Plethysmogram-based secure inter-sensor communication in Body Area Networks [25]	KK Venkatasubramanian et al.	2008	PKA is a fuzzy vault key agreement scheme that uses PPG signal as the main physiological signal.	Performance evaluation was based on two security aspects: (i) distinctiveness and (ii) temporal variance.	(i) PKA is distinctive among subjects, (ii) security level is function of vault size, (iii) features at given time are unique, (iv) for higher security 9^{th} polynomial order is used.	FFR= 0; If polynomial order (i.e. threshold) is $\leq$ 4; hence, number of features is $\leq$ 5	FAR=0; If threshold is $\geq$ 10; hence, number of features is $\geq$11	At threshold =7
physiological-signal-based key agreement (PSKA) [11]	KK Venkatasubramanian et al.	2010	PSKA is a fuzzy vault-key agreement scheme. PSKA enables two sensors to agree upon symmetric key using Electrocardiogram (ECG) signal.	Performance evaluation was based on two security aspects: (i) distinctiveness and (ii) temporal variance.	(i)PSKA is distinctive and preserve temporal variance; (ii) best polynomial order is 12.	FRR $\approx$ 0; If threshold < 5; hence, number of features is $\leq$ 5.	FAR is min; If threshold $\geq$ 14; hence, number of features is $\geq$15.	At threshold= 14
Ordered-Physiological-Feature-based Key Agreement (OPFKA) [12]	C Hu et al.	2013	OPFKA is an algorithm proposed to reduce false rejection resulted when larger vault size is used; by ordering the features.	Performance evaluation was based on several security aspects: (i) distinctiveness, (ii) temporal variance, (iii) key length, (iv)overhead imposed by communication and processing and (v) energy consumption.	Compared to PSKA; OPFKA achieves higher security level with much lower computations.	FFR= 0; If number of common features (i.e. threshold) is < 12.	FAR=0; if threshold > 5.	At threshold =8.
Secret- key Generation Protocol (SGenP) [28]	P Kumari et al.	2018	SGenP is a symmetric key agreement scheme that uses HMAC feature exchange (HMAC-FE) and secret key construction (SKC) to establish a secure communication.	Performance was mainly evaluated by energy consumption analysis for different key agreement stages.	(i)The resulted key is 128-bit length, (ii) SGenP offers some essential properties like plug-n-play, replaceability, scalability, flexibility and easy refreshment of keys	FFR= 0; If number of common features (i.e. threshold) is $\leq$ 10.	FAR=0; if threshold $\geq$5.	At threshold =8.
Flexible and Efficient Authenticated Key Agreement Scheme for BANs Based on Physiological Features (PBAKA) [29]	W Tang et al.	2018	PBAKA uses control unit to launch authentication rather than sensors; based on physiological signals.	Performance evaluation was based on several security aspects: (i) recognition rate, (ii)overhead imposed by communication and processing and (iii) energy consumption.	PBAKA is secure under decisional bilinear Diffie-Hellman (DBDL) assumption.	FRR = 0.15	FAR=0.01	-

connected and agreed upon a key for a while. We use the assumption that previous session's common feature vector can be used to generate new random key; thus, saving sensors' recourses. Our analysis shows the feasibility and efficiency of FREKA and proves that it is meeting design goals stated in [13] for physiological based key agreement algorithms.

3. System Model

A BAN consists of environmental and physiological sensors which form a network using wireless communication. In medical field applications, collected signals are forwarded to a sink node that processes them and send them to medical servers (i.e. hospital computers) for administrative tasks, storage in hospitals databases or further processing such as: calculation of some parameters needed for patient surgery [30]. We assume that all sensors' communications can be classified into two categories: first time communication and later fast communications. For the first-time communication, all sensors which are willing to communicate must measure the same physiological signal for predefined period with some sort of synchronization. Level of synchronization required mainly depends on signal's feature extraction method used. For later fast communications, we use first communication's feature vector to ensure data security and generate new key for a period specified by the sensors in the first connection. Also, we assume that communication medium is not secure. Hence, attackers can eavesdrop on BAN's connections, replay old messages or inject messages. This paper is focusing on the designing of a fast and high-performance algorithm to secure inter-sensors communications while maintain randomness and length of the key and saving resources. This paper, did not consider sink to server communication security, jamming attacks or electromagnetic interference.

4. Key Agreement

The purpose of FREKA is to enable two sensors previously connected to agree upon new symmetric key using previous connection's features; in such a way that saves both: time and resources without compromising security and key aspects. The key agreement process between two sensors for the first time works as follows. First, both sensors collect same type of physiological signal for specified period, simultaneously. Then, both sensors independently extract features from collected signal and store them in what called *feature vectors*. The size of feature vector is usually in the range of 12 to 24 features [25]. Extracted features at both sensors are dynamic (extracted in real time) and ordered using ordering algorithm known by the two sensors. After that, the sender sensor sends validation time value along with its own feature vector random permutated with some noisy data to ensure its security in the medium. Validation time refers to the time at which first connection's features will be valid for later communications security. Since two sensors collect the same signal type, receiver identifies common features with simple set interaction process between two feature vectors (i.e. the received noisy feature vector and receiver's feature vector). The outputs of intersection process are common features' values along with their indices in receiver's feature vector. Receiver uses the hash of identified common features as a key. Receiver sensor sends indices of identified features to the sender. Sender uses received indices to identify common features then hashing them to generate the key. At this case both sensors save the common features along with their indices for timer validation period. In the case of later communications between sensors that connected before, sender sensor must check for timer validation first. If the timer is valid then sender sends random permutation of common features' indices along with hash of new key generated. The new key is simply the output of hashing of features belong to indices permutation. Receiver simply uses the received indices and identifies the features and then re-generates the key. Algorithm1 demonstrates basic idea of FREKA scheme, whose steps are discussed in detail later. This paper uses ECG signal [31] as example physiological signal. FREKA algorithm can be used with any physiological signal.

Algorithm 1. FREKA key agreement

```
Input: Physiological signal
Output: Symmetric Key

While P ≠ 0 do;
   FREKA;
 else
   New key agreement cycle;
End

function FREKA (FV1, FV2)

 //For sender
  Generate C        // random noisy data
  Generate P
   NFV=Permute (C, FV1)
   Send NFV, P

 //For receiver
   Receive NFV
   [Co indices, Co values] = (NFV ∩ FV2) //Common features
   Key R= Hash (Co values)
   HK R= Hash (Key R)
   Send HK, Co indices

 //For sender
   Co s = FV1(Co indices)
   Key s= Hash (Co s)
   HK s= Hash (Key s)
   If HK s == HK R
      Use Key R and Key s
   else
      New Cycle
   End

 // Later communications
     // Receiver
     I new = Permute (Co indices)
     Key new R = Hash (FV2 (I new))
     NHK R = Hash (Key new R)
     Send NHK R , I new

     // Sender
     Key new S = Hash (FV1(I new))
     NHK s = Hash (Key new S)
     If NHK s == NHK R
        Use Key new R and Key new s
     else
        New Cycle
     End

END
```

4.1 First Connection Key Agreement Cycle

In the first connection key agreement cycle, two sensors will agree upon a common key and identify the period at which common features vector generated can be reused. After common features identification, both sensors store common features vector until timer's period ends. Figure1 demonstrates the basic flow chart for first connection cycle. Table 2 demonstrates the basic notations in FREKA scheme first/later connection. This subsection demonstrates first connection's key agreement cycle in some detail.

Table 2. FREKA algorithm notations identification

Notation	Definition
C	Chaff points
NFV	Noisy feature vector
Co	Common features
HK	Hashed key
NHK	New hashed key
IDs	Sender ID
IDr	Receiver ID
NFV	Noisy features vector
P	Period for timer validation
No	Nonce (i.e. Random number for transaction refreshment)
MAC	One-way hashing function
I	Indices of common features
I_{new}	New indices vector after random permutation
||	Concatenate symbol
Key_{new}	New key generated based on I_{new}

1) Physiological signal collection and filtering: Two sensors must collect physiological signal for predefined period. Signal's collection period and level of synchronization needed mainly depend on features extraction method to be used. After signal's collection, there is filtering step to remove any kind of noises in the collected signal. The most common sources of noises are baseline and muscles noises, which can be easily, removed using low and high pass filters, respectively. Electrocardiogram (ECG) signal is descriptive signal for heart's electrical activity (see Figure1). Normal ECG signal consists of three parts. First part is P wave which represents heart's atria depolarization. Second part is QRS complex which represents ventricle depolarization. Last part is T wave which represents the relaxation of the heart at ventricle repolarization. ECG signal's noises are usually high and low frequency noises. ECG noises can be removed using Pan-Tompkins algorithm [32]. Pan – Tompkins algorithm is ECG signal filtering algorithm. It highly depends on the fact that most power of ECG signal is consumed by QRS portion. So, it is amplifying QRS while reducing rest of the signal portions along with noises.

2) Features extraction: Features extraction methods have significant impact on efficiency of any physiological based key agreement algorithm. This can be referred to that fact that, collected signals at both sensors are not perfectly identical. Instead, they have large signals' overlapped portions in common. So, feature extraction job is extracting the most effective common features that are highly reducing unauthorized access rates while enhancing authorized access rates. Below, we discuss two features extraction methods: Fast Fourier Transform method (FFT) and Inter Pulse Interval (IPI) method. Note that, same features extraction method can be used under the same concept with different physiological signals by simple parameters modification.

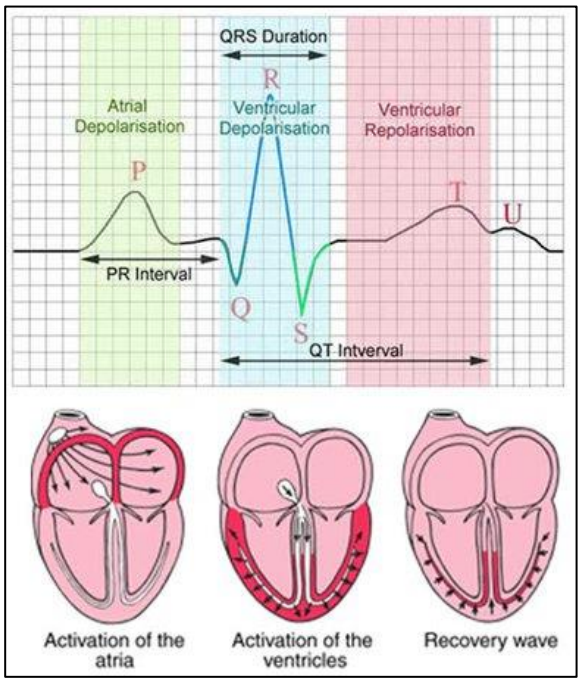

Figure1. ECG signal waves [31]

The FFT method: FFT method is frequency domain method that transforms input signal from its domain (i.e. time or space) into frequency domain. Spectral information of collected signal is represented using 'sin' and 'cos' waves. FFT has superiority over existing features extraction methods due to its speed and lower synchronization level needed. FFT input is N points physiological signal while the output is two parts each with N/2 samples. The Cos FFT coefficients can be referred as FFT real part while Sin coefficients can be referred as imaginary part. The only useful part is the first part (i.e. the real one). This is due the Nyquist theorem that stated: f_{max} (i.e. the maximum frequency that can be represented by FFT) is at N/2. Specialized FFT version for ECG features extraction is implemented as follow:

1) Partition signal samples into two overlapped windows.
2) Perform N-points FFT and take only first N/2 points from resulted FFT coefficients.
3) Pass FFT coefficients to peak detection method.
4) Represent detected peaks in the form of tuple <peak index, peak value>.
5) Quantize each index into binary number with 5-digits and each value into 8 –digits binary number.
6) Concatenation is done on each quantized peak index and its corresponding quantized value to form 13-bit feature.
7) The final output will be a feature vector containing extracted quantized features.

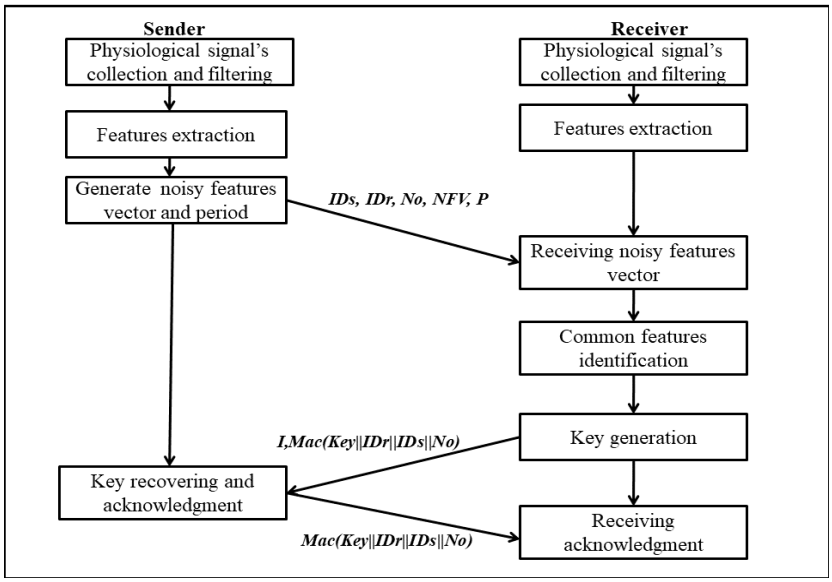

Figure 2. First connection's flowchart

Inter Pulse Interval Method (IPI): IPI method [33] is considered time domain feature extraction method. This method uses time intervals between physiological signal waves as features. This method requires noiseless and synchronized signals to give reliable results. For ECG signal, IPI commonly uses the time interval between two successive R waves as feature. In normal heart status, IPI varies from cycle to cycle. At some conditions such as exercises and some diseases, IPI may be constant among hearts' cycles. Experimental study [10] shows that 4-bit random digits can be extracted from each IPI. Technically, IPI implementation using ECG signal is quite simple and need no complex operations like FFT. The only drawback of this method is the need for longer signal collection duration than FFT. Because IPI represents the time interval between two successive signal cycles, the first step for IPI usage is reference peak identification and detection. Reference peak commonly is the peak that easy to detect or the cycle discriminative peak. For ECG signal, the reference peak R peak. R peak is detected using Pan-Tompkins algorithm [32]. By the end of feature extraction algorithm both communicating sensors has its own features vector (i.e. $FV_s = \{f_{s1} \ldots f_{sN}\}$ for sender and $FV_r = \{f_{r1} \ldots f_{rN}\}$ for receiver). IPI method is working as follow:

1) Apply Pan-Tompkins algorithm to detect QRS complex.
2) Identify R peak as reference peak.
3) Calculate time difference between every R peak in two consecutive cycle in signal.
4) Quantize calculated time differences into 4-bit binary number.
5) Concatenate each three successive quantized peaks to generate 12-bit number (i.e. IPI feature).
6) Every generated feature is saved to feature vector.

3) Noisy features vector receiving and common features identification: common values are identified using simple intersection function between received noisy feature vector and receiver features vector. The output is simply common features values and their corresponding indices. Number of common features must be greater than specified threshold to approve key generation process. If not, then no key will be generated, and connection will be ended.

4) Key generation and acknowledgments: keys are generated by hashing common values using one-way hashing function. The most common hashing functions used are MD5 and SHA-265. Once the key is generated, receiver sends the following message to sender:

Receiver to Sender: ***I, MAC (Key|| IDr|| IDs||No)***

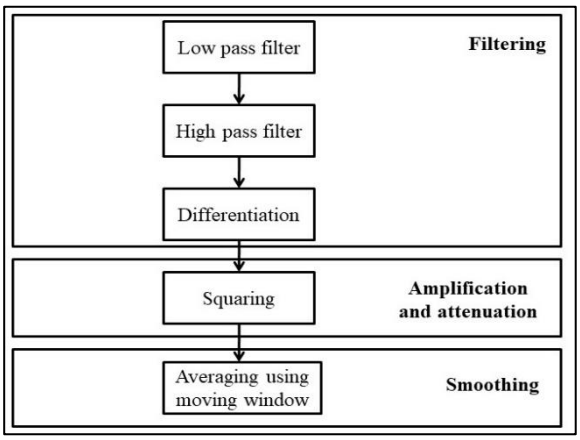

Figure 3. Pan -Tompkins QRS extraction method block diagram

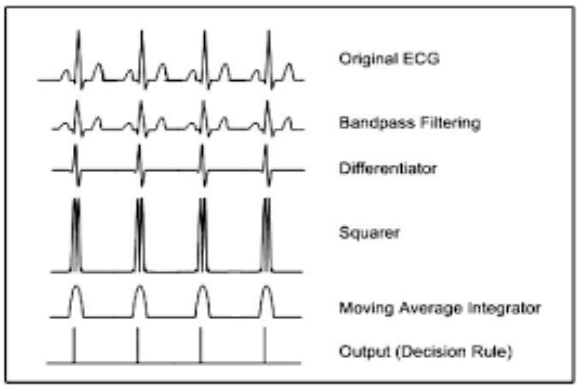

Figure 4: Pan-Tompkins implementation results [32]

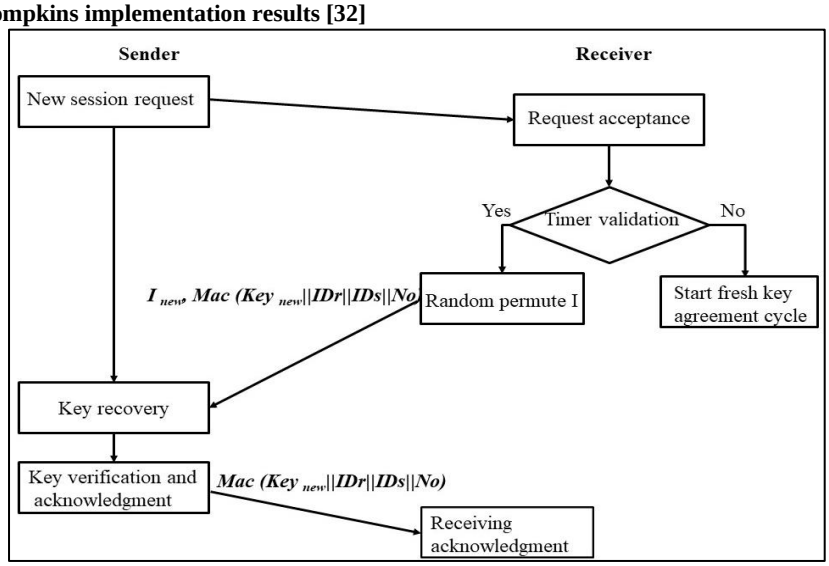

Figure 5. Later connections' flowchart

5) Key recovering and acknowledgments: After receiving the previous message, sender starts its key recovering process. Key recovering process at sender side will be implemented in two steps. First, identify features belong to received indices; then, hashing them to generate the key. To validate the correctness of generated key, sender will compare MAC of the generated key with the MAC received. If two MAC codes are identical, then, success acknowledgment will be sent to the receiver as the following:

Sender to Receiver: ***MAC (Key|| ID_r|| ID_s||No)***

By the end of this process, there are two subsequences. First, the key generated is used to ensure first connection's security. Second, common features along with their indices are stored for later communications security within timer validation period.

4.2 Later Connections Key Agreement Cycle

In later connections, two previously connected sensors can re-use saved common features vector to agree upon new random common key. This process is meant to be reducing computational overhead needed for agreement process, hence, reducing the time while maintain randomness and freshness of the key. Figure 5 illustrates the basic flow chart of later connection's key agreement process. As we can notice from Figure 5, later communications are highly depending on: timer validation and indices vector. Timer validation controls the way algorithm will follow. If timer is valid, then random permutation of the indices of previously stored common features is used; to generate new random key. If not, then a new normal key agreement cycle as first connection is started. This subsection demonstrates later connections' key agreement cycle in some detail.

1) Timer validation: timer is one of the most important aspects of FREKA algorithm. For later communications, checking timer validation is just checking the ability of using previous first connection's common features. If timer is valid; then, approve later connection key cycle. If not, which means the common features stored are deleted; then, start new cycle as the first one previously illustrated to construct new common features vector.

2) New indices vector generation: since new indices vector generation implies the freshness of the key, indices vector assumed to be the basic building block of generation process. New indices vector I_{new} is generated using simple random permutation process on first connection's indices vector *I.*

I_{new} = **Random Permutation (*I*)**

3) Key generation: to generate new key, common features are ordered with the same arrangement stated by I_{new} and then hashing them to get the key. Example 1 illustrates the basic idea of this step. After completion of this step, receiver sends the following message to sender:

Receiver to Sender: ***I new, Mac (Key new||IDr||IDs||No)***

4) Key recovering and acknowledgment: at the sender side, key recovering is done by using new indices vector received to re-order features saved and then hashing them to get the key. The success acknowledgment is sent as the following message:

Sender to Receiver: ***Mac (Key new||IDr||IDs||No)***

Example1:
Given:

Original index vector *'I'* with the following values [1, 2, 5, 10, 12]

1st connection key:
Key= hash (*f (1) ||f (2) ||f (5) ||f (10) ||f (12))*

2ndconnection key:
I_{new} = Random Permutation (*I*) = [2, 5, 12, 1, 10]

Key new= hash (*f (2) ||f (5) ||f (12) ||f (1) ||f (10))*

Conclusion:
Altering the position of features resulted in new different key.

Example1. FREKA basic idea example

5. Security Analysis

This section analyzes the security of FREKA algorithm; for both, first and later connections key agreement cycles.

5.1 First connection's key agreement cycle

The most important pieces of information transferred through the medium in the first connection are: indices vector (*I)* along with legitimate features and the key. The security of legitimate features is assured due to the noisy data added to features vector before transmission. The number of noisy data points is much more than the number of legitimate features points. This will make features identification a very hard task for an attacker. Key security is assured by: using MAC (i.e. hashing function) of the key instead of key transmission. Indices vector (*I)* knowledge is useless for attacker's key guessing process; because attacker is unable to get hands on features. The Nonce *No* usage maintains the freshness of the connection; hence, avoid usage of old message to break the connection.

5.2 Later connections' key agreement cycles

The security of later connection is highly depending on the fact that there are no features transmitted on the media and all the common features are stored securely in sensors memories. We assume that all sensors are under supervision and there is no sensor that can be compromised without being detected; and what the attacker can do is key guessing using the information transmitted in the media. For an attacker, knowledge of new indices vectors I_{new} and comparing to previous *I* will help with nothing in key guessing process. As before, MAC of the key will ensure the key security. The brief period of the timer will help in making attacker task harder. This because after the timer ends, all the information stored will be erased. This means new first connection cycle; hence, updating of data to be guessing.

5.3 Timer validation period and key refreshing

Timer validation period *P* is assumed to be directly proportional to sensor's power level *PL* connection frequency factor f_c (i.e. a number that indicates how many times two sensors connected through predefined period). Longer period will be used with higher power levels; and when sensor connects regularly.

$$P \propto PL * fc \quad (1)$$

$$P = k * PL * fc \quad (2)$$

Constant *k* is assumed to equal 1/100 for normalization purpose. Since, validation period *P* has high impact in key refreshing (i.e. the longer the timer period, the more times key must be refreshed), we simply assumed that key must refreshed one time for every period minute (i.e. for each minute in P there is a unique key).

$$\forall n \; \exists_1 \, m \quad (3)$$

Where n is number of minutes in P and m is number of keys for each minute**.** *P* was limited to be 5 minutes in maximum, to maintain higher level of security, which cannot be reached if longer period is used (i.e. if $P \geq 5$; then set P=5). Also, if the power level *(PL)* is under 25% our algorithm is not applicable.

Table 3. Timer period for different *PL* and f_c

PL	f_c	*P*	*P*
100	15	(15*100)/100= 15	5
100	10	(10*100)/100=10	5
100	5	(5*100)/100=10	5
100	3	(3*100)/100=3	3
50	15	(15*50)/100=7.5	5
50	10	(10*50)/100=5	5
50	5	(5*50)/100=2.5	3
50	3	(3*50)/100=1.5	2
25	15	(15*25)/100=3.7	4
25	10	(10*25)/100=2.5	3
25	5	(5*25)/100=1.25	1
25	3	(3*25)/100=0.75	1

6. Evaluation and Discussion

In [11-12], authors proposed different schemes to hide secret features as well as key agreement process. For those schemes, the computational cost for key agreement process between two previously connected sensors is high (i.e. the cost for later connections is the same as first connection cost). This excessive cost is due to the assumption that two sensors must start new agreement process from scratch every time they are willing to communicate even, they were in connection before. This problem is addressed by using pre-knowledge saved from previous connection (i.e. the features generated from the first connection) to generate new random key. This method will help in fasten key agreement process, as well as saving sensors resources and prolong sensor's life.

In this section, we discuss some features extraction methods notes and how these methods can be used to fast key agreement process and save memory used for later connections. Then, the performance of FREKA algorithm is evaluated in comparison with OPFKA algorithm. The following security algorithm evaluation aspects will be discussed: randomness and length of the key, memory storage, communication overhead, energy consumption and distinctiveness.

6.1 Discussion

This subsection discusses features extraction methods usage, benefits and drawbacks along with best signal length for every method. Signal length must be sufficient; so, it raises the accuracy while giving enough features for further usage. ECG signal was used as an example of physiological signal. ECG signal length needed was estimated using experimental results. Experiment was implemented using Mat- lab 2017 and MIT Database [34].

6.1.1FFT method

Papers [11-12] proposed to implement FFT using different ECG signal length as input. FFT algorithm was implanted using different ECG lengths ranging from 2 to 12 seconds. Table 5 conclude FFT method and its implementation notes. Even number of seconds were

used to be able to divide input samples into two equal windows. Experimental results show that the best accuracy of this algorithm can be reached when 8 seconds ECG signal is used. Figure 6 shows the ROC curves for FFT implantation using different input signal lengths. From experimental results stated at Table 4; the following points can be concluded: (i) FFT minimum time needed of ECG signal as input to be applicable is 4 seconds. Two seconds ECG signal gives no results because of the lake of minimum samples required, (ii) minimum number of samples required for 256-point FFT algorithm is 512 samples, (iii) usage of integer number of seconds (each second represent one ECG cycle) since FFT works with integer number of cycles only, (iv) usage of even number of seconds to be able to divide input samples into two equal windows, (v) ECG based FFT algorithm has three parameters: sampling rate, sampling duration, FFT points. Sampling rate was set to 128 Hz and FFT points to 256 with varying sampling duration, (vi) FFT is recursive operation that decomposes input signal into sum of its frequency components. The accuracy of FFT depends on root of unity used for decomposition process.

In this experiment, the better accuracy resulted is just a consequence of two things: First, when input shorter signal to FFT, number of extracted features at both sides will be decreased. Therefore, feature matching time and collusion will be reduced to minimum. Second, when shorten the length of input signal; the number of noisy data generated to conceal the legitimate features should be decreased.

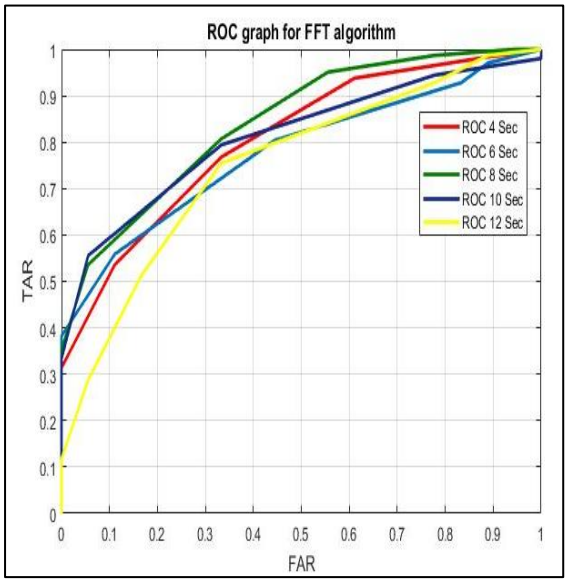

Figure 6. ROC Curves for FFT algorithm with different ECG lengths

Table4. FFT results with different ECG lengths

ECG Length in seconds	Efficiency	Recognition Accuracy	Error Rate
2 sec.	NAN	NAN	NAN
4 sec.	0.9444	0.78799	0.2120
6 sec.	0.9414	0.78021	0.2198
8 sec.	0.9506	0.86025	0.1398
10 sec.	0.9321	0.80133	0.1987
12 sec.	0.9475	0.76711	0.2329

Table 5. FFT features extraction method

General overview	
Domain	Frequency domain method.
Best usage	Stationary and periodic signal (i.e. normal signal).
Advantages	1-Best speed over all existing real-time methods. 2-Extracted features are independent. 3- Minimum level of synchronization is required.
Disadvantages	1-It has poor spectral estimation when used with very short signals (e.g. 2sec.). 2-It cannot reveal localized peaks among input signal.
Implementation steps notes	
Step	**Note/Reason**
Windowing	To give some time resolution beside frequency resolution.
***Overlapping* windows signal division**	To reduce the artifacts effect at the boundaries of each window (i.e. signal cycles within the window should end at zero). If signal beginning and ending not the same, then FFT will give wrong and inefficient results.
Output only N/2 samples of the resulted N-points FFT	Because that the maximum frequency 'f_{max}' that can be represented by n-point FFT is equal to n/2(i.e. Nyquist Theorem).
Use FFT peaks as features	Because of their ability to characterize original signal very well.

6.1.2 IPI method

Authors in [12] proposed IPI method for feature extraction. They claimed that this method requires about 1 to 1.5-minute ECG signal as input; to implement and get satisfactory results. IPI algorithm was implemented different ECG lengths ranging from 10 to 60 seconds. Experimental results show that the best accuracy of this algorithm can be reached when 10 seconds ECG signal is used. Figure 7 illustrates the ROC curves for our experiment. Table 6 illustrates our experimental results and Table 7 conclude IPI method with some implantation notes. From results showed at Table 6; the following point can be concluded: this method requires highly synchronized input signal to work and give reliable results. FFT is considered the fastest features extraction method due to its reasonable accuracy with much less input signal length than IPI and other methods.

Table 6. IPI results with different ECG lengths

ECG Length in Seconds	Efficiency	Recognition Accuracy	Error Rate
10 sec.	0.9691	0.97223	0.0278
20 sec.	0.9691	0.95609	0.0439

30 sec.	0.9630	0.95503	0.0450
40 sec.	0.9660	0.94648	0.0535
50 sec.	0.9599	0.90943	0.0906
60 sec.	0.9568	0.93174	0.0683

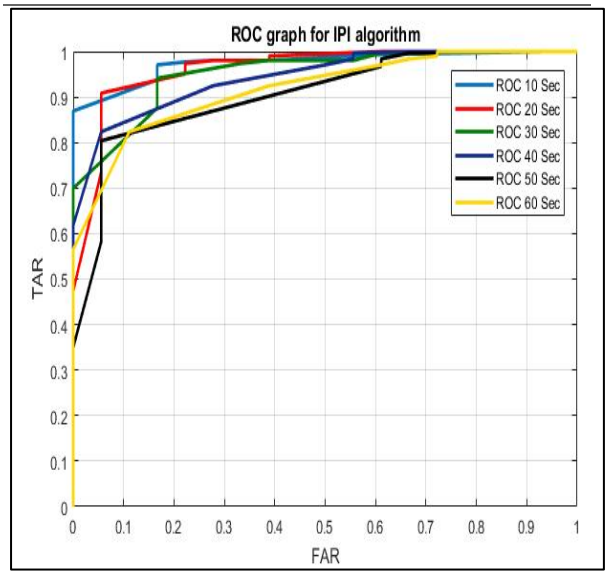

Figure 7. ROC Curves for IPI algorithm with different ECG lengths

Table 7. IPI features extraction method

General overview	
Domain	Time domain method.
Best usage	Stationary and periodic signal (i.e. normal signal).
Advantages	1-Good results with noiseless, synchronized signal than FFT method. 2-IPI method consumes less computation power when compared to FFT due its simple operations.
Disadvantages	1-Slow when compared to FFT, due to time required for collecting input signal (i.e. 10 seconds or 1 minute). 2-Extracted Features are dependent. 3-Require prominent level of synchronization to give reliable results.
Implementation Steps notes	
Step	**Note/Reason**
Synchronization	Since IPI uses time interval as features, synchronization is needed to get some features in common.
Filtering	IPI uses time interval between prominent peaks as features. Noises may distort dominant peaks, which makes prominent peaks detection a challenging task. To overcome this problem, filtering methods are used.

6.2 Evaluation

In this subsection, FREKA algorithm was evaluated in comparison with several popular key agreement schemes; PKA [25], PSKA [11], OPFKA [12], SGenP [28] and PBAKA [29]. Evaluation aspects are key length and randomness, storage cost, energy consumed, overhead imposed by communication, distinctiveness and temporal variance. Our results show superiority of our algorithm in later communications.

1- Length and randomness of the key: The usage of one-way hashing function ensures that resulting key every time is random and long. Hash function used here is MD5.

2-Communication overhead: *IDs* and *IDr* are represented by 16 bytes each, *No* is 16 bytes, index *I* is at most 1 byte, *P* is 1 byte and *MAC* is 16 bytes. Here features and noisy data points represented by 12 or 13 bit each (about 1.5 byte). For PBAKA, transaction information T_s and T_r are 20 bytes each. Table 8 shows that our algorithm offers the lowest communication overhead among presented schemes.

3-Energy consumption: In [35] authors assumed that sensor consumes 28.2 mJ to receive one byte and 59.2 mJ to transmit it. As shown in Table 9, our algorithm gives the lowest energy consumption.

4-Memory storage: As we can see from results in Table10, the main difference between first connection in our algorithm and other schemes is number of bytes used for R representation. Our algorithm shows better results. Note that, Memory storage here means the amount of memory consumed during key agreement process. In first connection, sensors must save *NFV* until success of agreement process. In later communication sensors will save common feature vector we will denote it as F; F is much lighter than NFV (i.e. F<<NFV). Because of that FREKA gives better results.

5- Distinctiveness: Distinctiveness means the ability of scheme to distinguish the sensors in the same WBAN from those in another WBAN. This can be achieved by maintaining sufficient number of common features between sensors in the same network. Common features threshold is set to be great than or equal 12. FRR is the minimum when common features are less than 12. On the other hand, FAR is minimum when common features are greater than 5.

6- Temporal variance: Higher temporal variance implies that the signal has better randomness. The more randomness; the harder for attacker to comprise network security. Signals collected at different time are generally unique. However, if time difference between two successive signal reading is so close, the collected signal values will tend to be similar [11]. FREKA solves close readings/similar values problem and achieves better

temporal variance than the other schemes. This mainly due the usage of period P.

7- Low latency: Sampling duration needed for secure key agreement highly depends on physiological signal used [11]. As illustrated in discussion section; when FFT is used to extract ECG signal, at least 4 second signal is needed with 128 Hz sampling rate. PBAKA [29] needs at least 12.6 seconds.

Table 8. Communication overhead for first/later connections

Algorithm	First connection communication overhead	Later connection communication over head	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	$2\|ID_s\|+2\|ID_r\|+No\|+2\|Mac\|+$ $2\|HMac\|+2\|String\|$	$2\|ID_s\|+2\|ID_r\|+No\|+2\|Mac\|+$ $2\|HMac\|+2\|String\|$	1.33 KB	HMAC is 600 bytes and random string is 20 bytes length.
PBAKA	$2\|ID_s\|+2\|ID_r\|+2.5\|F_s\|+ 2.5\|F_r\|+ T_s + T_r$	$2\|ID_s\|+2\|ID_r\|+2.5\|F_s\|+ 2.5\|F_r\|+ T_s + T_r$	104+2.5|F_s|+ 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.
FREKA	$2\|ID_s\|+2\|ID_r\|+1.5\|NFV\|+\|I\|+\|No\|+2\|Mac\|+$ $\|P\|$	$2\|ID_s\|+2\|ID_r\|+\|I_{new}\|+\|No\|+2\|Mac\|$	First connection: 114+1.5|NFV| bytes. Later connection: 113 bytes.	If NFV length is 100; then final cost is 264 bytes.

Table 9. Energy consumption for first/later connections

Algorithm	First connection energy consumption	Later connections energy consumption	Analysis
PKA	112+4.5|NFV|*(28.2+59.2)	112+4.5|NFV|*(28.2+59.2)	9.788+3.146|NFV| *mJ*
PSKA	112+4.5|NFV|*(28.2+59.2)	112+4.5|NFV|*(28.2+59.2)	9.788+3.146|NFV| *mJ*
OPFKA	113+2.5|NFV|*(28.2+59.2)	113+2.5|NFV|*(28.2+59.2)	9.876+1.748|NFV| *mJ*
SGenP	1368*(28.2+59.2)	1368*(28.2+59.2)	119.5 *mJ*
PBAKA	104+2.5|F_s|+2.5|F_r|*(28.2+59.2)	104+2.5|F_s|+2.5|F_r|*(28.2+59.2)	9.089+1.748|F_s|+1.748 F_r| *mJ*
FREKA	114+1.5|NFV|*(28.2+59.2)	113*(28.2+59.2)	First connection: 9.963+1.048|NFV| *mJ* Later connection: 9.876 *mJ*

Table 10. Memory cost for first/later connections

Algorithm	First connection memory cost	Later connection memory cost
PKA	$2\|ID_s\|+2\|ID_r\|+4.5\|NFV\|+\|No\|+2\|Mac\|+Key_s + Key_r$	$2\|ID_s\|+2\|ID_r\|+4.5\|NFV\|+\|No\|+2\|Mac\|+Key_s + Key_r$
PSKA	$2\|ID_s\|+2\|ID_r\|+4.5\|NFV\|+\|No\|+2\|Mac\|+Key_s + Key_r$	$2\|ID_s\|+2\|ID_r\|+4.5\|NFV\|+\|No\|+2\|Mac\|+Key_s + Key_r$
OPFKA	$2\|ID_s\|+2\|ID_r\|+2.5\|NFV\|+\|I\|+\|No\|+2\|Mac\| +Key_s + Key_r$	$2\|ID_s\|+2\|ID_r\|+2.5\|NFV\|+\|I\|+\|No\|+2\|Mac\| +Key_s + Key_r$
SGenP	$2\|ID_s\|+2\|ID_r\|+No\|+2\|Mac\|+ 2\|HMac\|+2\|String\| Key_s + Key_r$	$2\|ID_s\|+2\|ID_r\|+No\|+2\|Mac\|+ 2\|HMac\|+2\|String\| Key_s + Key_r$
PBAKA	$2\|ID_s\|+2\|ID_r\|+2.5\|F_s\|+ 2.5\|F_r\|+ T_s + T_r + r +s + Key_s + Key_r$	$2\|ID_s\|+2\|ID_r\|+2.5\|F_s\|+ 2.5\|F_r\|+ T_s + T_r + r +s + Key_s + Key_r$
FREKA	$2\|ID_s\|+2\|ID_r\|+1.5\|NFV\|+\|I\|+\|No\|+2\|Mac\|+\|P\|+ Key_s + Key_r$	$2\|ID_s\|+2\|ID_r\|+\|I_{new}\|+\|No\|+2\|Mac\|+ Key_s + Key_r$

7. Conclusion

In this paper, we propose a secure, fast and resource efficient algorithm, namely Fast-Resource-Efficient-Key-Agreement (FREKA). FREKA allows two sensors to use previous connection information to agree upon new and random key. Performances analysis shows that our algorithm achieves better communication, memory and energy costs when compared with OPFKA. Thus, our algorithm is applicable approach to secure inter-sensor communication within BANs and prolong sensors' life.

8. Acknowledgments

Our sincere appreciation to the 'Information Technology Department' experts who have contributed towards development of this research.

9. References

[1] Venkatasubramanian, K. K., & Gupta, S. K. (2006). Security for Pervasive Health Monitoring Sensor Applications. *2006 Fourth International Conference on Intelligent Sensing and Information Processing*.

[2] Venkatasubramanian, K. K., Gupta, S. K., Jetley, R. P., & Jones, P. L. (2010). Interoperable Medical Devices. *IEEE Pulse, 1*(2), 16-27.

[3] Schwiebert, L., Gupta, S. K., &Weinmann, J. (2001). Research challenges in wireless networks of biomedical sensors. *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking - MobiCom 01*.

[4] Chen, M., Gonzalez, S., Vasilakos, A., Cao, H., & Leung, V. C. (2010). Body Area Networks: A Survey. *Mobile Networks and Applications, 16*(2), 171-193.

[5] Penders, J., Molengraft, J. V., Brown, L., Grundlehner, B., Gyselinckx, B., & Hoof, C. V. (2009). Potential and challenges of body area networks for personal health. *2009 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*.

[6] Schmidt, R., Norgall, T., Mörsdorf, J., Bernhard, J., &Grün, T. V. (2002). Body Area Network BAN – a Key Infrastructure Element for Patient-Centered Medical Applications. *Biomedizinische Technik /Biomedical Engineering, 47*(S1a), 365-368.

[7] Kumar, P., Lee, S., & Lee, H. (2012). E-SAP: Efficient-Strong Authentication Protocol for Healthcare Applications Using Wireless Medical Sensor Networks. *Sensors, 12*(2), 1625-1647.

[8] Jana, S., Premnath, S. N., Clark, M., Kasera, S. K., Patwari, N., & Krishnamurthy, S. V. (2009). On the effectiveness of secret key extraction from wireless signal strength in real environments. *Proceedings of the 15th Annual International Conference on Mobile Computing and Networking - MobiCom 09*.

[9] Hei, X., & Du, X. (2011). Biometric-based two-level secure access control for Implantable Medical Devices during emergencies. *2011 Proceedings IEEE INFOCOM*.

[10] M.Mana, M.Feham and B.A.Bensaber(2009). Secure and Efficient Key Exchange for wireless Body Area Network. *International Journal of Advanced Science and Technology*.

[11] Venkatasubramanian, K., Banerjee, A., & Gupta, S. (2010). PSKA: Usable and Secure Key Agreement Scheme for Body Area Networks. *IEEE Transactions on Information Technology in Biomedicine, 14*(1), 60-68.

[12] Hu, C., Cheng, X., Zhang, F., Wu, D., Liao, X., & Chen, D. (2013). OPFKA: Secure and efficient Ordered-Physiological-Feature-based key agreement for wireless Body Area Networks. *2013 Proceedings IEEE INFOCOM*.

[13]Venkatasubramanian, K. K., Banerjee, A., & Gupta, S. K. (2008). EKG-based key agreement inBody Sensor Networks. *IEEE INFOCOM 2008 - IEEE Conference on Computer Communications Workshops*.

[14] Keoh, S. L., Lupu, E., &Sloman, M. (2009). Securing body sensor networks: Sensor association and key management. *2009 IEEE International Conference on Pervasive Computing and Communications*.

[15] Li, M., Yu, S., Lou, W., & Ren, K. (2010). Group Device Pairing based Secure Sensor Association and Key Management for Body Area Networks. *2010 Proceedings IEEE INFOCOM*.

[16] Law, Y. W., Moniava, G., Gong, Z., Hartel, P., &Palaniswami, M. (2010). KALwEN: A new practical and interoperable key management scheme for body sensor networks. *Security and Communication Networks, 4*(11), 1309-1329.

[17] Li, M., Yu, S., Guttman, J. D., Lou, W., & Ren, K. (2013). Secure ad hoc trust initialization and key management in wireless body area networks. *ACM Transactions on Sensor Networks, 9*(2), 1-35.

[18] Tan, C. C., Wang, H., Zhong, S., & Li, Q. (2008). Body sensor network security. *Proceedings of the First ACM Conference on Wireless Network Security - WiSec 08*.

[19] Malan, D., Welsh, M., & Smith, M. (n.d.). A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography. *2004 First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON 2004.*

[20] Tan, C., Wang, H., Zhong, S., & Li, Q. (2009). IBE-Lite: A Lightweight Identity-Based Cryptography for Body Sensor Networks. *IEEE Transactions on Information Technology in Biomedicine, 13*(6), 926-932.

[21] Xu, F., Qin, Z., Tan, C. C., Wang, B., & Li, Q. (2011). IMDGuard: Securing implantable medical devices with the external wearable guardian. *2011 Proceedings IEEE INFOCOM*.

[22] Hu, C., Liao, X., & Cheng, X. (2012). Verifiable multi-secret sharing based on LFSR sequences. *Theoretical Computer Science, 445*, 52-62.

[23] Cherukuri, S., Venkatasubramanian, K., & Gupta, S. (n.d.). Biosec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body. *2003*

International Conference on Parallel Processing Workshops, 2003. Proceedings

[24] Venkatasubramanian, K. K., & Gupta, S. K. (2006). Security for Pervasive Health Monitoring Sensor Applications. *2006 Fourth International Conference on Intelligent Sensing and Information Processing*. .

[25] Juels, A., & Sudan, M. (2006). A fuzzy vault scheme. *Proceedings IEEE International Symposium on Information Theory.*

[26] Venkatasubramanian, K. K., Banerjee, A., & Gupta, S. K. (2008). Plethysmogram-based secure inter-sensor communication in Body Area Networks. *MILCOM 2008 - 2008 IEEE Military Communications Conference*.

[27] Jammali, N., &Fourati, L. C. (2015). PFKA: A physiological feature based key agreement for wireless body area network. *2015 International Conference on Wireless Networks and Mobile Communications (WINCOM)*.

[28] Kumari, P., & Anjali, T. (2018). Symmetric-Key Generation Protocol (SGenP) for Body Sensor Network. *2018 IEEE International Conference on Communications Workshops (ICC Workshops)*. doi:10.1109/iccw.2018.8403548

[29] Tang, W., Zhang, K., Ren, J., Zhang, Y., & Shen, X. S. (2018). Flexible and Efficient Authenticated Key Agreement Scheme for BANs Based on Physiological Features. *IEEE Transactions on Mobile Computing*, 1-1. doi:10.1109/tmc.2018.2848644.

[30] Silva, C. A., & Junior, G. S. (2018). Fog Computing in Healthcare: A Review. *2018 IEEE Symposium on Computers and Communications (ISCC)*. doi:10.1109/iscc.2018.8538671

[31]https://en.wikipedia.org/wiki/Electrocardiograpy.

[32]Pan, J., & Tompkins, W. J. (1985). A Real-Time QRS Detection Algorithm. *IEEE Transactions on Biomedical Engineering, BME-32*(3), 230-236.

[33] Poon, C., Zhang, Y., & Bao, S. (2006). A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. *IEEE Communications Magazine*, *44*(4), 73-81.

[34] http://physionet.org/physiobank/database

[35] Ren, K., Lou, W., Zeng, K., & Moran, P. (2007). On Broadcast Authentication in Wireless Sensor Networks. *IEEE Transactions on Wireless Communications, 6*(11),4136-4144.

[36] Diffie, W., & Hellman, M. (1976). New directions in cryptography. IEEE Transactions on Information Theory, 22(6), 644-654. doi:10.1109/tit.1976.1055638.

[37] Kumari, P., & Anjali, T. (2017). Securing a body sensor network. *2017 9th International Conference on Communication Systems and Networks (COMSNETS)*. doi:10.1109/comsnets.2017.7945445

[38] Sun, Y., Wong, C., Yang, G., & Lo, B. (2017). Secure key generation using gait features for Body Sensor Networks. *2017 IEEE 14th International Conference on Wearable and Implantable Body Sensor Networks (BSN)*. doi:10.1109/bsn.2017.7936042

[39] Li, P., Wang, Y., He, J., Wang, L., Tian, Y., Zhou, T., Li, J. (2017). High-Performance Personalized Heartbeat Classification Model for Long-Term ECG Signal. *IEEE Transactions on Biomedical Engineering*, *64*(1), 78-86.

[40] Karimian, N., Guo, Z., Tehranipoor, M., & Forte, D. (2017). Highly Reliable Key Generation From Electrocardiogram (ECG). *IEEE Transactions on Biomedical Engineering*, *64*(6), 1400-1411.

[41] Altop, D. K., Levi, A., & Tuzcu, V. (2017). Feature-level fusion of physiological parameters to be used as cryptographic keys. *2017 IEEE International Conference on Communications (ICC)*. doi:10.1109/icc.2017.7996338