International Journal of Scientific Research and Innovation ISSN 2455-0140
Volume 12, Issue 3, March 2024, IJSRI1003

WIRELESS BODY AREA NETWORKS USING REUSABLE ECG-BASED FEATURES

R. ROBERT

Assistant Professor,

Dept. of Electronics and Communication Engineering,

Annai Velankanni College of Engineering,

Kanyakumari .

Email id: rrobertraj@gmail.com

Dr. V.V. VINOTH., M.E, Ph.D

Associate Professor,

Dept. of Electronics and Communication Engineering,

Annai Velankanni College of Engineering,

Kanyakumari.

Email id: vinfo.vv@gmail.com

Abstract--With the advancement in electronics and embedded systems Wireless Body Area Networks (WBANs) are employed in different medical applications, such as early detection of medical conditions ,remote health monitoring, , and computer-assisted rehabilitation. A WBAN use a number of sensor nodes in-built or fixed on the human body for monitoring physiological characteristics. Advancement of WBAN technology, in sensor nodes novel key-agreement protocol is used for secure communications. This paper analyzes the distinct key agreement schemes under specific attacks, security threats and corresponding counter measures in WBAN environment. The proposed protocol is based on measuring and verifying common physiological features with secure communication in a specific period of time and communicating with both sender and recipient sensors. Compared with other existing key agreement protocols, the proposed protocols have high efficient and accuracy.

Keywords-- Wireless Body Area Network (WBAN), Inter-Sensor Communication, Electrical Cardio Graph), pattern recognition

I. INTRODUCTION

Wireless Body Area Networks (WBANs) are mostly used in medical applications with monitoring node with some processing and computing abilities. Wireless Sensor Network (WSN) and Wireless Body Area Network (WBAN) differentiated with distances. WBAN is used human body within a range of few centimeters/meters whereas WSN extended up to few kilometers. WBAN nodes can be divided into two types first one is sensing and monitoring nodes, which are used to collect physiological and contextual data [1]and the second one is personal server (PS), which is used in terms of processing, power, and storage. WBAN enables sensor communication using wireless technology. The mostly used wireless standard is IEEE 802.15.6. The connection in WBAN between two nodes or between nodes and PS is called intra-WBAN communication. Then the connection between PS and remote server using the internet is called inter-WBAN communication. Figure 1 explains a WBAN consists of two types of nodes, PS and physiological signal sensors. The sensors can send any data to a Personal Server not through remote server.

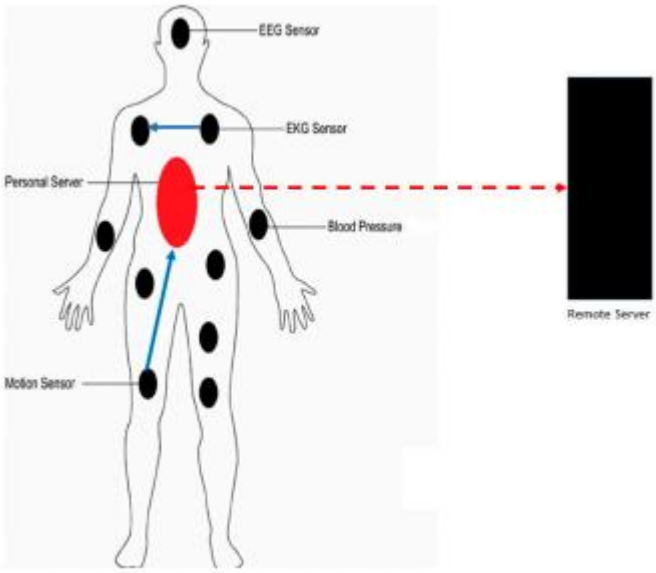


Fig.1 A Wireless Body Area Network (WBAN) contains two types of nodes, personal server (PS) and physiological signal sensors

WBAN applications used in Medical and non-medical applications [2–6].In medical applications are mainly associated with disease detection and healthcare systems for patient tele-monitoring .Medical applications wearable WBAN, implanted WBA are used. Non-medical applications include WBAN applications, which are used for entertainment and gaming purposes. Information transmitted among WBAN sensors are encrypted before transmission using a symmetric or asymmetric key. A symmetric key is a single key used for both ciphering and deciphering operations. Asymmetric key are two different keys that is public and private keys. The public key not secret key while the private key is kept a secret. The key generation based on biometric data, such as iris and fingerprint have the advantage of removing the need for key predistribution , it requires less memory consumption. The proposed method is a biometric-based key generation algorithm. The proposed method algorithm enables two sensors that regularly connect to use some information from their previous connection.

II.RELATED WORK

Electrocardiogram (ECG) signal as the physiological 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.

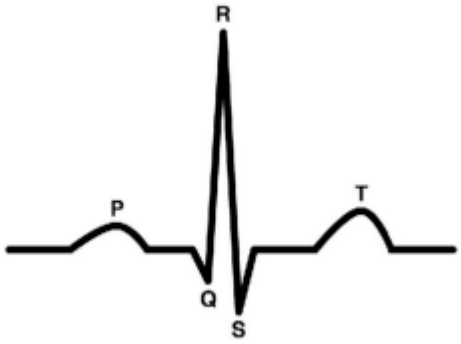


Fig. 2 Electrocardiogram (ECG) signal

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 [7,8]. 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 predistribution 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 [9], composite random key pre-distribution scheme [10], and the multipath reinforcement scheme [11] are examples of key pre-distribution algorithms.

Security Requirements of WBAN

There are certain expectations from WBAN from the security perspective without which the crucial medical data would not be secure. Based upon the literature review, following are the expectations of WBAN from security perspective.

1. Data confidentiality : Medical data is private and crucial in nature which needs to be protected from unauthorized access. Data confidentiality in transmission as well as in storage requires being secured by means of cryptographic techniques.
2. Node authenticity : Node authentication is a major concern in WBAN. Spoofed nodes may ruin the entire network authenticity. Lightweight cryptographic methods are required as traditional techniques are not suitable for energy constraint resources.
3. Data integrity: Personal health related data may be modified in transit in absence of any mechanism to ensure the data integrity. It could be dangerous in life critical situations. System must ensure to detect any modification in data. To check the data integrity, lightweight cryptographic hash functions are required which can authenticate inter BAN communication.
4. Mutual authentication: The nodes of WBAN participating in the system must authenticate one another to thwart Man-In-The-Middle (MITM) attack.

5. Unforgeability: A secure WBAN must ensure that the personal server cannot be forged. A compromised server may divert all the medical data towards the attacker which can play disastrous to the system.
6. Unlinkability: Unlinkability is ensured if the system is able to hide the identity of sender and the corresponding receiver. The identity of the sender and receiver must be hidden during communication.
7. Forward secrecy and backward secrecy : In backward secrecy, when a node joins a network after it was established, system must not provide the access of those messages exchanged earlier before it joined the network. In forward secrecy, a node which has left the network is not allowed to access the messages exchanged after its departure.
8. Scalability : System must ensure the implementation of security schemes keeping in view of the scalability of the system. It must support the inclusion of more nodes without causing any security flaw.
9. Freshness: To maintain the freshness of data packets, time-stamping on the data packets is done. It will identify the new and old data packets. It will help the system to thwart the replay attack.
10. Prevention of DoS attack: Denial of Service attack is meant to forbid the accessibility of any service or resource to its intended users. It is accomplished by flooding the target resource that triggers a crash.
11. Prevention of Node Capture attack: An adversary can capture the node and install malicious software. It is redeployed to launch various attacks.

III.PROPOSED METHOD

WBAN Topology is a short-range network, and its range is the human body around 3 to 6 m. So, limited range of communication star topology is used. Two communicating sensors communicate through PS to proceed with their connection. The proposed method has two communicating sensors can connect directly without PS help with the use of mesh topology. Due to the short range the most used standard is IEEE 802.15.6, which is a low-power wireless technology for WBANs, with around 10 Mbps of data rates.

The Proposed Key Agreement Method

The proposed method uses symmetric key for communicating sensors to some previous connection features. The initial key agreement process between two sensors collect the same physiological signal e for a given period, t, simultaneously. Both sensors extract the collected signal and store them in two independent feature vectors with the size typically in the range of 12 to 24 features. The only constraint on the communicating ends is they should collect the same type of phycological signal with a high synchronization level. The feature extraction stage using different physiological signals will make no difference at as long as it is frequency domain with FFT. FFT features measures the peaks of the frequency transformed signal. This paper construct feature vectors used in the key agreement process uses physiological ECG signal.

Algorithm

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 ≠ 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., FV1 and FV2, respectively)
b) The sender generates timer validation period P and sends P along with HFVS to the receiver, where HFVS = Hashing (FV1)
c) The receiver receives HFVS and starts to generate HFVR by Hashing (FV2).
d) The receiver checks the authenticity of the sender by comparing HFVS and HFVR
e) After checking the sender's authenticity, the key generation process starts at the receiver side by generation OFVR, where OFVR= Ordering algorithm (FV2)
f) Receiver side security key is generated by hashing OFVR, Key R = Hash (OFVR)
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= Hash (Key R)
h) The sender uses the same ordering method that was used by the receiver to generate OFVS
i) The sender generates the security key Key S by hashing OFVS
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 ≠ 0
a) The sender generates PM and uses it to produce a new version of its feature vector FV1 as following: FV new S =Permute (FV1, PM)
b) The sender generates its new security key for this session using FV new S as following Key new S = 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 =Permute (FV2, PM)
e) The receiver generates its version of the session security key Key new R as following: Key new R = 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.

First Connection Key Agreement Cycle

The first key agreement cycle identifies the validation timer period and the generated features vector can be reused for other connections. Figure 3 explains the flow chart for the first connection key agreement cycle..

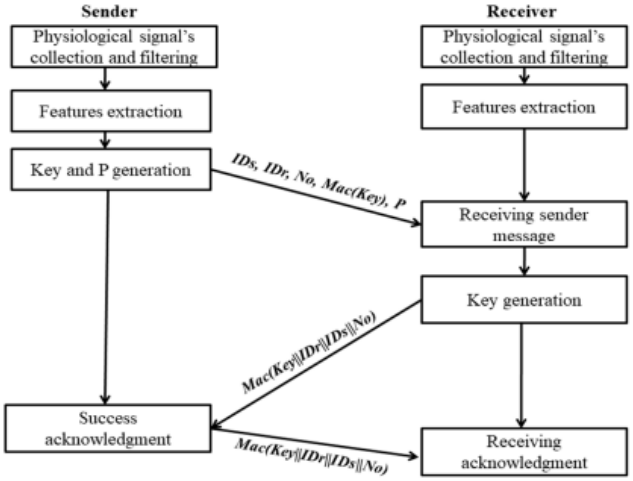


Fig.3 The first connection's cycle flowchart

Physiological signal collection and filtering:

Physiological signals collected by two sensors for a given period. Features extraction methods mainly focus on the signal's collection and level of synchronization. Filtering step removes any unwanted noise in the collected signal using Pan–Tompkins algorithm. ECG signal feature extraction methods affected by high noise sensitivity, therefore, noise reduction must be used as a preprocessing step before the feature's extraction process.

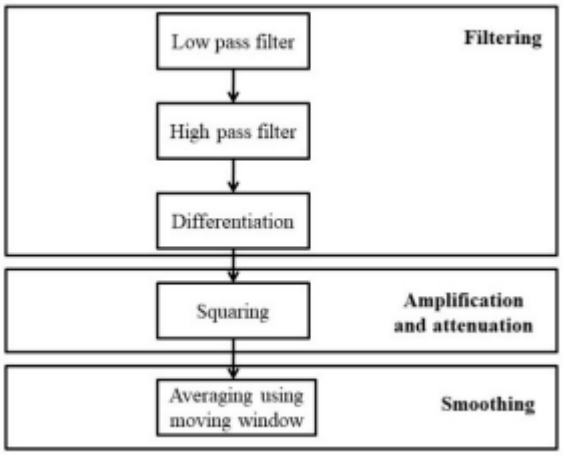


Fig.4 Pan–Tompkins algorithm for filtering ECG signal.

Features extraction using the modified FFT version:

Physiological-based key agreement algorithm's increased efficiency, reducing unauthorized access rates. This can be done by extracting the most useful features that best describe the physiological signal. Modified version of the Fast Fourier Transform method (FFT) is the frequency-domain method that transforms the input signal from its domain (i.e., time or space) into the frequency domain. The proposed method implemented with original FFT method with a low synchronization level by varying ECG lengths ranging from 2 to 12 s,.

Key generation and period generation:

In this proposed method using hashing feature vector the security key is generated. The hashing function used is a MD5 and SHA265. Once the key is generated, the sender sends the message to the receiver and receiver sends acknowledgement to the sender as follows

Sender to Receiver: IDs, IDr, No, Mac (Key), P

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

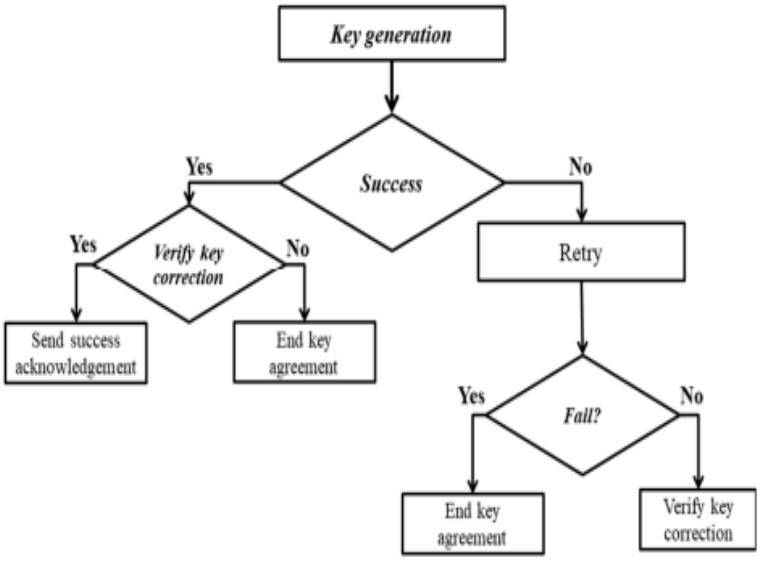
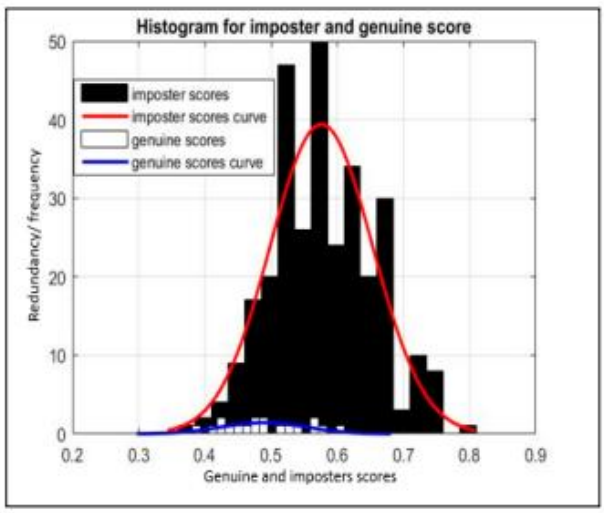


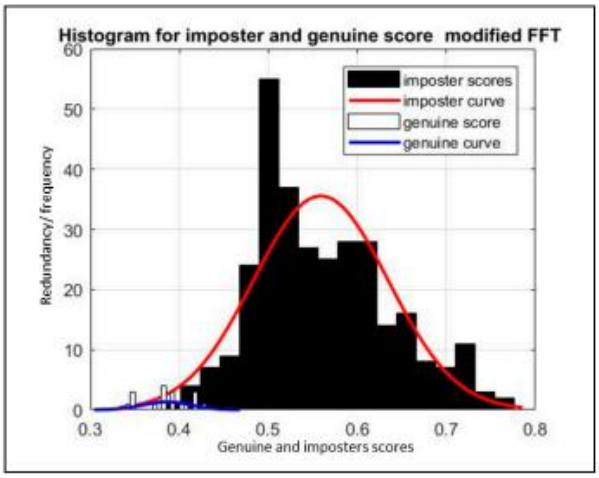
Fig.5 The key generation process at the receiver side

IV. EXPERIMENTAL RESULTS AND DISCUSSION

This proposed method's experimental results using the original FFT method and proposed a modified FFT version to extract ECG features. FFT method is fast and in-dependency on the extracted features. Figure.8 shows the histogram for the original FFT and the proposed method with modified FFT.



(a)



(b)

Fig.6 Histogram for the imposter and genuine scores; (a) the proposed method with original FFT, (b) the proposed method with modified FFT

V.CONCLUSION

WBAN key agreement algorithm is a secure, fast, and resource-efficient, it allows two sensors to use previous connection data to agree upon a new and random key. WBAN resources can be achieved by feature vector for a predefined period and saving the previous session common to be used for later connections' key agreement. Advancement of WBAN technology, in sensor nodes novel key-agreement protocol is used for secure communications.

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] obón, D.P.; Falk, T.H.; Maier, M. Context awareness in WWBANs: A survey on medical and non-medical applications. IEEE Wirel. Commun. 2013, 20, 30–37.

[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

[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; doi:10.1109/icsens.2007.355786.

[7] Pan, J.; Tompkins, W.J. A Real-Time QRS Detection Algorithm. IEEE Trans. Biomed. Eng. 1985, BME-32, 230–236.

[8] 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; doi:10.1109/wicom.2012.647860.

[9] Rasheed, A.; Mahapatra, RN Key Predistribution Schemes for Establishing Pairwise Keys with a Mobile Sink in Sensor Networks. IEEE Trans. Parallel Distrib. Syst. 2010, 22, 176–184; doi:10.1109/tpds.2010.57.

[10] 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; doi:10.1109/iccasm.2010.5622602.

[11] Di Mauro, A.; Dragoni, N. Adaptive Multipath Key Reinforcement for Energy Harvesting Wireless Sensor Networks. Procedia Comput. Sci. 2015, 63, 48–55; doi:10.1016/j.procs.2015.08.311.

[12] Van Torre, P. Channel-Based Key Generation for Encrypted Body-Worn Wireless Sensor Networks. Sensors 2016, 16, 1453; doi:10.3390/s16091453

[13] 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; doi:10.4108/icst.bodynets.2013.253689.

[14] 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.

[15] Ren, K.; Lou, W.; Zeng, K.; Moran, P.J. On Broadcast Authentication in Wireless Sensor Networks. IEEE Trans. Wirel. Commun. 2007, 6, 4136–4144