A Biometric based Anonymous User Authentication Technique in Wireless Body Area Networks

Gitanjali Behera, Saroj Kumar Panigrahy, and Ashok Kumar Turuk
Department of Computer Science and Engineering
National Institute of Technology Rourkela, Odisha - 769008, India
gitanjalibehera1108@gmail.com, skp.nitrkl@gmail.com, akturuk@nitrkl.ac.in

***Abstract*—The sensor nodes used in wireless body area networks are resource constrained, having limited battery power and memory capacity. Hence, they are not capable of running more complex algorithm to ensure the security. Therefore, designing a light-weight protocol for wireless body area networks which aims to provide maximum security with resource-constrained devices is a tough challenge. In this paper, we propose a light weight biometric-based anonymous authentication technique between the user and the application server in WBAN which preserves the patient's privacy as well as achieves mutual authentication. In addition, we have given an informal cryptanalysis which ensures that the proposed technique resists different well known attacks.**

***Index Terms*—WBAN, Wireless Body Area Network, Anonymity, Authentication, Biometric**

I. Introduction

Wireless body area network (WBAN) is very much effective in the field of health-care industry by enabling patients in real time health monitoring and receiving medical care remotely by using a number of tiny wireless sensor nodes. Because of the wide spread applications, WBAN has gained more attention from the heath-care industries as well as from the research industries. In 2012, IEEE has published a standard IEEE 802.15.6 for WBANs [1], which is basically a multi-hop centralized architecture, where a central node called hub node or local server is involved. The sensors used in WBANs are responsible for monitoring and collecting various information regarding the patient's vital signs like body temperature, heartbeat, pulse rate, blood pressure and many other crucial environmental factors like room temperature and humidity etc. The collected data are transmitted to the local server or hub node. According to [2], it is always recommended that there should be some intermediate nodes between the sensor nodes and local server. An extended three tier architecture for WBANs is shown in Fig. 1. In WBANs, the leakage of privacy of the potential users and security of data should be the major concern and must be taken into account as the data are transmitted through insecure wireless channel. In this paper, we propose a biometric based anonymous authentication protocol between the user and the application server in a WBAN.

The rest of the paper is organized as follows. In Section II, we discuss the related works. We describe our proposed authentication scheme in Section III. In Section IV, We perform an informal security analysis of the proposed authentication scheme. In Section V, we describe performance analysis in terms of storage requirements, computation cost and communication overheads of the proposed protocol and finally, Section VI gives the concluding remarks.

II. Related Works

Authentication plays an essential and vital role for secure communication in WBANs which allows the application server to confirm user's identity when the user is trying to access the system. Many user authentication schemes have been proposed by various researchers to guarantee secure communication in WBANs. Previously, to provide secure communication in WBANs, many non-cryptographic authentication and key agreement schemes like channel-based schemes, proximity-based schemes, physiological signal based schemes have been proposed. Physiological schemes cannot be implemented in WBANs, because the physiological signals are different for the same patient if they are measured by different sensor nodes used in patient which results in denial-of-service (DoS) attacks [3]. Channel based authentication schemes, however, fail to provide user anonymity as well as require special hardware and software which limits further research [4]. Proximity-based authentication schemes are more restrictive than the other schemes requiring the constraint that, the devices must be nearer to each other, which cannot be achieved in case of WBAN [5].

In view of WBAN, many authentication schemes have been presented based on public key cryptography (PKC), identity-based cryptosystem (IBC), and elliptic curve cryptography (ECC) techniques to guarantee secure communication. Li et al. [6], [7] proposed a public key cryptography (PKC) based key management scheme in order to guarantee mutual authentication. However, these schemes require complex modular exponentiation operations which are not suitable for WBANs containing resource constrained nodes limited with computing capability and battery capacity. In order to reduce heavy modular exponentiation operations, several ECC based authentication schemes have been proposed where requirement of computation is less. In the IBC, identity of the user plays the role of the public key and the key generation centre (KGC) uses his/her secret key in order to calculate the user's private key based on his/her identity. Therefore, the complex management of public key certificates is relieved that arises

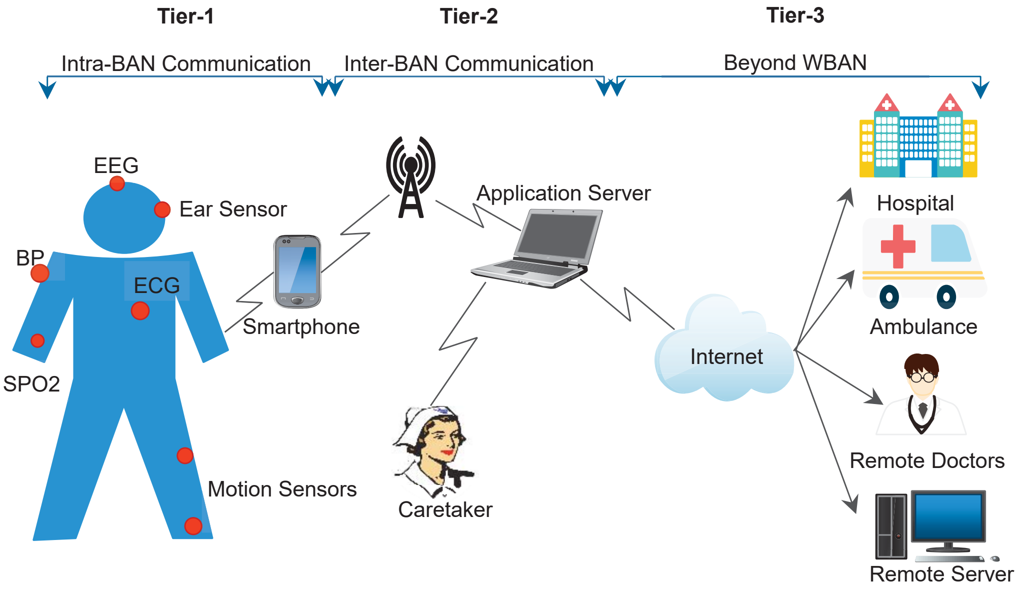

Fig. 1. Extended three tier architecture of WBAN.

in traditional public key infrastructure. However, it bears key escrow issues related to KGC.

Considering the above identified problems, many certificate less public key cryptography (CL-PKC) based protocols were presented. A bilinear pairing based certificate-less signature scheme has been proposed by Liu et al. [8] to guarantee secure communication in WBANs. However, their scheme is vulnerable to insider impersonation attacks and not suitable for practical application as insider attack is more dangerous than the outsider attack. Again, in such protocols, either no revocation procedure was presented for revoking the user's privilege of getting the services, or the protocols were lacking anonymity. He et al. [9] proposed a protocol based on [8] in order to prevent impersonation attack. For this purpose, they stored all the data in network-manager's database instead of application server's database. As the application server is generally at the hospital location, it is more prone to physical attacks by the attackers. Hence, they placed the network-manager in a secure place and the server was operated by a trusted third party.

Liu et al. [10] proposed an efficient and anonymous 1-round authentication protocol based on bilinear pairing for WBAN to thwart attackers from bullying legitimate users. Their protocol achieves anonymity, mutual authentication, non-repudiation and session key verification property and claim that, their protocol is more secure than existing protocol. However, their protocol suffers from DoS attack, key-compromise impersonation attack (KCI), and session key guessing attacks. Xiong Li et al. [11] proposed an improved single-round authentication protocol to remove the flaws in protocol proposed by Liu et al. [10]. They proved that, their protocol resists against the DoS attack, key-compromise impersonation attack, and stolen-verifier attack keeping the same computation and communication cost. Amin et al. [12] proposed an anonymous patient monitoring system using hash and XOR function to reduce the computation cost, communication overheads and storage overheads. However, their protocol was not resistant to stolen mobile device attack, desynchronization attack and sensor key exposure attack.

III. Proposed Authentication Scheme

To make secure communication, authentication with session key agreement protocols are widely used. In such protocols, after sharing a common session key between two parties, information can be easily transmitted through open channel by encrypting the message with the session key. Here, session key verification is the major security aspects to get assurance about the establishment of the common and secret session key between different participants. The proposed scheme achieves authentication by establishing session key between users and application server.

The proposed scheme has three phases— initialization phase, registration phase, and login and authentication phase. The initialization phase is performed by the system administrator where as the registration phase is performed by the users and finally after the login phase, authentication is performed between the user and the application server.

A. Initialization Phase

The system administrator SA initializes the application server AS by choosing a secret key ASK for AS.

B. Registration Phase

In order to receive health-care services, an i^{th} user U_i ($i \in \{1, 2, ..., n\}$, where n is the number of users) must register himself through the SA. Here, when the user U_i is registering for the first time, the SA provides the ID_i for the user. After receiving the ID_i from the SA for the first time, user U_i can perform steps given in Fig. 2. In this phase, ID_i, PW_i and BM_i represent identity, password and biometric of the user U_i respectively, whereas r_i is a random number and h is a one-way hash function represented by $h : \{0,1\}^* \to \{0,1\}^l$, where l is the output length. Here, it is assumed that all the information are transmitted using a secure protocol (such as the TLS protocol).

C. Login and Authentication Phase

In this phase, session key SSK is exchanged between the U_i and the AS by achieving mutual authentication. The details of this phase are presented in Fig. 3. In this phase, r_i and rn_j are the random numbers, whereas T_j represents timestamp and $j \in \{1,2\}$. Here, the timestamp T_j is validated by verifying the predicate($T^* - T_j \overset{?}{<} \delta T$), where T^* is the received time of the message and δT is the maximum transmission delay allowed. If the predicate condition is not valid, aborts the connection.

IV. Security Analysis

For secure communication, the authentication schemes should be immune to various security attacks, as the data are transmitted through wireless channel. In this section, we analyze different well known security attacks/security requirements and how our scheme withstands against these attacks are described.

A. Resists Replay Attack

In the proposed protocol, at every session of login and authentication, we are using a random nonce and a time stamp in order to verify weather that message value is fresh or not. If the message is received after the specified transmission delay (δT), simply the authentication party discards the message and abort the connection. Therefore, replay attack is not possible by the adversary in our protocol.

B. Resists Mobile Device Stolen Attack

In our protocol even if the adversary has got the mobile device, he/she can only extract the information $\langle HID_i, W_i, Y_i, h(.) \rangle$ and from these information, he cannot extract the ID_i, PW_i or BM_i, as HID_i is the hashed value of the all three $\langle ID_i, PW_i, BM_i \rangle$ and hash is a one-way function and cannot be reversible. Therefore, the adversary can not launch user impersonation attack using mobile device information.

C. Resists Forgery Attack

In the proposed protocol, at every session of the login and authentication phase, we are checking the validity of the transmitted message as described below.

- After reception of the tuple $\langle HID_i, TID_i, V_1, V_2, T_1 \rangle$ by the AS from user, AS validates the time stamp as well as the value of V_1 by calculating V_1'. If the condition $V_1 = V_1'$ is not valid, AS simply aborts the connection.
- Similarly, after reception of the tuple $\langle V_3, V_4, T_2 \rangle$ by the user(U_i) from the AS, U_i validates the time stamp T_2 as well as the value of V_3 by calculating the value V_3'. If $V_3 \neq V_3'$, U_i simply aborts the connection.

D. Preserves Anonymity of the User (U_i)

In the proposed protocol, the user sends ID_i in a secure channel by using TLS protocol in registration phase, so in no way, the adversary can get the user's identity. In the login and authentication phase also, there is no way of getting the user's identity as described below.

- From the intercepted message $\langle HID_i, TID_i, V_1, V_2, T_1 \rangle$, the adversary cannot get the user's identity. As HID_i is calculated as $HID_i = h(ID_i||r_i||HPB_i)$ and $h(.)$ is a one-way hash function, there is no way of getting identity of the user. From TID_i also, there is no way of getting the identity of the user even if the adversary has HID_i, TID_i, T_1, he/she does not know the hash function and the value rn_1. Similarly, from V_1 and V_2 also the adversary cannot get the identity of the user.
- From the intercepted message $\langle V_3, V_4, T_2 \rangle$, the adversary cannot get the identity of the user as he/she does not know the value of rn_2 and hash function.

E. Achieves Mutual Authentication

In the proposed protocol,both of legal parties user(U_i) and application server AS authenticate each other mutually. Since at every session of the login and authentication phase, we are checking the validity of the received message by calculating $V_1 = V_1'$ and $V_3 = V_3'$ at the application server side and user side respectively, our protocol achieves mutual authentication.

F. Achieves Session Key Verification Property

In the proposed protocol, the calculated session key will be always same for both the parties, as both parties ensures the exactness of the session key by calculating whether $V_1 \overset{?}{=} V_1'$ and $V_3 \overset{?}{=} V_3'$.

G. Achieves Perfect Forward Secrecy

In the proposed protocol, session key is calculated as $SSK = h(V_3||V_4||rn_2)$ in which all the sensitive parameters V_3, V_4 and rn_2 are protected by one-way hash function and these values are dynamically changing in every session because of the use of the random nonce and time stamp. Therefore, the proposed scheme achieves forward and backward secrecy.

H. Fully Protection to Random Numbers

In the proposed protocol, the random numbers r_i, rn_1 and rn_2 are fully protected, i.e from the intercepted messages, the adversary cannot get the random number values. From the intercepted messages $\langle HID_i, TID_i, V_1, V_2, T_1 \rangle$ and $\langle V_3, V_4, T_2 \rangle$, there is no way of getting the random numbers because of the one-way function.

V. Performance Evaluation

In this section, we analyze the performance of the proposed scheme by means of storage requirements, computation cost and communication overheads.

User(U_i)/ Mobile device		**Application server(AS)**
Provides ID_i, PW_i, BM_i		
Computes $HPB_i = h(ID_i\|\|PW_i\|\|BM_i)$		
	$\xrightarrow[\text{(Via a secure channel)}]{\langle ID_i, HPB_i, BM_i \rangle}$	
		Computes $h(BM_i)$
		Checks whether $h(BM_i)$ already exist or not, if not
		Generates a random number r_i
		Computes $HID_i = h(ID_i\|\|r_i\|\|HPB_i)$
		$W_i = r_i \oplus HPB_i$
		$X_i = h(ID_i\|\|r_i\|\|ASK)$
		$Y_i = X_i \oplus h(ID_i\|\|r_i\|\|HPB_i)$
		$Z_i = r_i \oplus h(HID_i\|\|ASK)$
		Stores $\langle h(BM_i), HID_i, Z_i \rangle$
	$\xleftarrow[\text{Via a secure channel}]{\langle HID_i, W_i, Y_i, h(.) \rangle}$	
Stores $\langle HID_i, W_i, Y_i, h(.) \rangle$ in the mobile device		

Fig. 2. Steps involved in the registration phase

User(U_i)/ Mobile device		**Application server(AS)**
Provides ID_i, PW_i, BM_i		
Computes $HPB'_i = h(ID_i\|\|PW_i\|\|BM_i)$		
$r'_i = HPB'_i \oplus W_i$		
$HID'_i = h(ID_i\|\|r'_i\|\|HPB'_i)$		
If $(HID'_i \neq HID_i)$ abort connection Else		
Generates a random number rn_1		
Generates a timestamp T_1		
Computes $X_i = Y_i \oplus h(ID_i\|\|r'_i\|\|HPB'_i)$		
$TID_i = ID_i \oplus h(HID'_i\|\|r'_i\|\|T_1)$		
$V_1 = X_i \oplus h(ID_i\|\|rn_1\|\|T_1)$		
$V_2 = rn_1 \oplus h(r'_i\|\|T_1)$		
	$\xrightarrow[\text{(Via an insecure channel)}]{\langle HID_i, TID_i, V_1, V_2, T_1 \rangle}$	
		Checks the validity of timestamp T_1
		Computes $r'_i = Z_i \oplus h(HID_i\|\|ASK)$
		$ID'_i = TID_i \oplus h(HID_i\|\|r'_i\|\|T_1)$
		$rn'_1 = V_2 \oplus h(r'_i\|\|T_1)$
		$V'_1 = h(ID'_i\|\|r'_i\|\|ASK) \oplus h(ID'_i\|\|rn'_1\|\|T_1)$
		If $(V'_1 \neq V_1)$ aborts connection Else
		Generates a random number rn_2
		Generates a timestamp T_2
		Computes $V_3 = h(ID'_i\|\|rn_2\|\|T_2)$
		$V_4 = rn_2 \oplus h(V_3\|\|T_2)$
		$SSK = h(V_3\|\|V_4\|\|rn_2)$
		Stores SSK.
	$\xleftarrow[\text{Via an insecure channel}]{\langle V_3, V_4, T_2 \rangle}$	
Checks the validity of timestamp T_2		
Computes $rn'_2 = V_4 \oplus h(V_3\|\|T_2)$		
$V'_3 = h(ID_i\|\|rn'_2\|\|T_2)$		
If $(V'_3 \neq V_3)$ abort connection Else		
Computes $SSK = h(V'_3\|\|V_4\|\|rn'_2)$		
Stores Session key SSK		

Fig. 3. Steps involved in the login and authentication phase

A. Storage Requirements

Storage requirements of the propose protocol is calculated as described below.

- The application server is required to store $\langle h(BM_i), HID_i, Z_i \rangle$ as well as the session key. Here, we are using SHA-1 as the one-way hash function and its message digest size is 160 bits. So, for storage of $h(BM_i)$, HID_i and Z_i require 160 bits each. As, session key is calculated as $SSK = h(V_3||V_4||rn_2)$, it also requires 160 bits. Therefore, in our protocol, application server (AS) requires $|h(BM_i)| + |HID_i| + |Z_i| + |SSK| = 160 + 160 + 160 + 160 = 640$ bits $= 80$ Bytes for storage.
- The user (U_i) is required to store $\langle HID_i, W_i, Y_i \rangle$ as well as the session key. So, for storage of HID_i, W_i and Y_i require 160 bits each and for session key also it requires 160 bits. Therefore, in our protocol, user (U_i) requires $|HID_i|+|W_i|+|Y_i|+|SSK| = 160+160+160+160 = 640$ bits $= 80$ Bytes for storage.

Therefore, total storage cost for the proposed protocol is 80+80=160 Bytes.

B. Computation Cost

In the proposed protocol, we use two operations: XOR operation and hash function. Here, we consider T_x and T_h are the computation time of one XOR operation and one hash operations respectively. As, XOR operator is a bit-wise operator, the computation time of XOR operation can be neglected i.e. $T_x \approx 0$. The computation cost of the proposed protocol is calculated as described below.

- In the login and authentication phase, User (U_i) performs 6 XOR operations and 9 hash operations. So, in total user (U_i) performs $6T_x + 9T_h \approx 9T_h$ operations.
- Similarly, in the login and authentication phase, application server (AS) performs 5 XOR operations and 8 hash operations. So, in total application server (AS) performs $5T_x + 8T_h \approx 8T_h$ operations.

C. Communication Overhead

The communication overheads of the scheme is calculated as described below.

- In the transmission of the tuple $\langle HID_i, TID_i, V_1, V_2, T_1 \rangle$ from user (U_i) to application server (AS), we are assuming that the time stamp $|T_1|$=32 bits, therefore, size of this tuple is 4*(160)+32=672 bits.
- In the transmission of the tuple $\langle V_3, V_4, T_2 \rangle$ from application server (AS) to user (U_i), the size of the time stamp $|T_2|$=32 bits. So, the total size of this tuple is 2*(160)+32=352 bits.

VI. Conclusion

To guarantee secure communication in WBANs, we proposed a biometric based light weight authentication protocol which achieves user anonymity as well as mutual authentication. The computation cost of the proposed protocol is very less, as our proposed technique only needs to calculate the XOR operations and hash functions. In aspects of storage overhead also, our scheme is efficient, as only 80 bytes is required for both user (U_i) and the application server AS. In addition, informal proof shows that, our scheme withstands against well known security attacks and best suitable for WBAN architectures. In our future work, we will try to find more security threats for WBANs and design authentication schemes accordingly, which will be more suitable for WBANs.

Acknowledgment

This research work is partially supported by Information Security Education and Awareness Project, Phase-II (ISEA-II) funded by Ministry of Electronics and Information Technology (MeitY), Government of India.

References

[1] "IEEE std 802.15.6-2012. IEEE standard for local and metropolitan area networks - part 15.6: Wireless body area networks," pp. 1–271, Feb 2012.

[2] X. Li, M. H. Ibrahim, S. Kumari, A. K. Sangaiah, V. Gupta, and K.-K. R. Choo, "Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks," *Computer Networks*, 2017.

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

[4] L. Shi, M. Li, S. Yu, and J. Yuan, "BANA: body area network authentication exploiting channel characteristics," *IEEE Journal on selected Areas in Communications*, vol. 31, no. 9, pp. 1803–1816, 2013.

[5] S. Mathur, R. Miller, A. Varshavsky, W. Trappe, and N. Mandayam, "Proximate: proximity-based secure pairing using ambient wireless signals," in *Proceedings of the 9th international conference on Mobile systems, applications, and services*. ACM, 2011, pp. 211–224.

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

[7] M. Li, S. Yu, J. D. Guttman, W. Lou, and K. Ren, "Secure ad hoc trust initialization and key management in wireless body area networks," *ACM Transactions on sensor Networks (TOSN)*, vol. 9, no. 2, p. 18, 2013.

[8] J. Liu, Z. Zhang, X. Chen, and K. S. Kwak, "Certificateless remote anonymous authentication schemes for wirelessbody area networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 332–342, 2014.

[9] D. He, S. Zeadally, N. Kumar, and J.-H. Lee, "Anonymous authentication for wireless body area networks with provable security," *IEEE Systems Journal*, 2016.

[10] J. Liu, L. Zhang, and R. Sun, "1-RAAP: An efficient 1-round anonymous authentication protocol for wireless body area networks," *Sensors*, vol. 16, no. 5, p. 728, 2016.

[11] X. Li, J. Peng, S. Kumari, F. Wu, M. Karuppiah, and K.-K. R. Choo, "An enhanced 1-round authentication protocol for wireless body area networks with user anonymity," *Computers & Electrical Engineering*, 2017.

[12] R. Amin, S. H. Islam, G. Biswas, M. K. Khan, and N. Kumar, "A robust and anonymous patient monitoring system using wireless medical sensor networks," *Future Generation Computer Systems*, vol. 80, pp. 483 – 495, 2018.