COMPUTERS & SECURITY 83 (2019) 300–312

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Efficient privacy preserving device authentication in WBANs for industrial e-health applications

Vanga Odelu[a,*], Sourav Saha[b], Rajendra Prasath[b], Lakshminarayana Sadineni[c], Mauro Conti[d], Minho Jo[e,*]

[a] Department of Computer Science and Information Systems, Birla Institute of Technology & Science, Pilani, Hyderabad Campus, 500 078, India

[b] Department of Computer Science and Engineering, Indian Institute of Information Technology, Sri City, Chittoor 517646, India

[c] Department of Computer Science and Engineering, Malaviya National Institute of Technology, Jaipur 302017, India

[d] Department of Mathematics, University of Padua, Padua 35122, Italy

[e] Department of Computer Convergence Software, Korea University, Sejong Metropolitan 30019, South Korea

ARTICLE INFO

Article history:
Received 20 July 2018
Revised 4 December 2018
Accepted 1 March 2019
Available online 6 March 2019

Keywords:
Internet-of-Things
Security
Credential privacy
Mutual authentication
WBANs
CK-adversary model
Industrial e-health systems

ABSTRACT

Leakage of sensitive e-health data would severely cause threats leading to tampering of health and person related information. So preserving the privacy of the patient information is an essential feature in e-health systems. In this paper, we first explore the security limitations of the existing authentication schemes. Most of the schemes fail to provide privacy of the credentials of users when session ephemeral secrets are revealed to an adversary. To address the drawbacks found in the existing schemes, we propose a privacy preserving device authentication scheme for wireless body area networks. This proposed scheme provides robust security even if ephemeral secrets are revealed to the adversary. Additionally the proposed scheme avoids the management of large number of public-keys of application providers by the client device. Using Java Pairing-Based Cryptography Library (JPBC), we performed simulations to show that our proposed scheme provides reduced computational overhead for both the client device and the application provider.

1. Introduction

The Internet of Things (IoT) based technologies using medical sensors and actuators are revolutionizing the next generation e-health systems to provide high-quality patient care (Hossain and Muhammad, 2016). In recent times, an aging population and sedentary lifestyles are fueling the prevalence of chronic diseases such as cardiovascular diseases, hypertension, and diabetes (Patel and Wang, 2010). Most diseases could be prevented through automatic/early detection systems and based on the observed data, e-health centers could give advices to the patients to improve their health. Wireless Body Area Networks (WBANs) Technology is a promising wireless sensor technology to build such devices that could provide efficient e-health services, particularly during medical emergency

* Corresponding authors.
E-mail addresses: odelu.vanga@hyderabad.bits-pilani.ac.in (V. Odelu), minhojo@korea.ac.kr (M. Jo).
https://doi.org/10.1016/j.cose.2019.03.002
0167-4048/

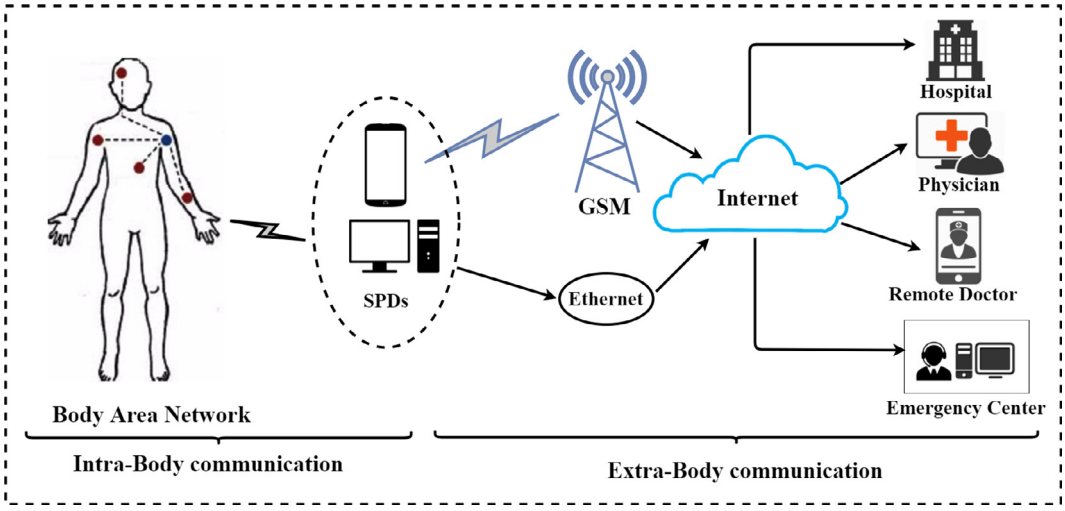

Fig. 1 – An e-health application using WBANs: an example.

(Chen et al., 2011; Li et al., 2013; Movassaghi et al., 2014). This opens up huge possibilities for building industrial applications in e-health domains.

The WBAN formed with many lightweight intelligent sensors placed in or around the human body to monitor real-time health data. In a typical healthcare application, WBAN collects real-time biomedical data such as heart rate, blood pressure, and pulse, and then sends the data to a remote medical server through mobile devices such as a personal digital assistant or a smart phone. Based on the collected data, doctors and other medical practitioners will get the patient's status and provide appropriate clinical diagnostics. We have illustrated a typical scenario of e-health application using WBANs in Fig. 1. We can observe that the WBANs mainly consist of wearable medical sensor nodes which are implanted inside and/or worn on human body and Smart Portable Device (SPD) held by the patient, called WBANs client. A self-organized WBANs can be formed to monitor the health status and the surrounding environments of human bodies. The WBAN has two communication modes, namely Intra-Body Communications (IBCs) and Extra-Body Communications (EBCs). IBCs allow sensors to communicate with each other and to the SPD, and EBCs enable SPD to communicate with the remote Application Providers (APs) such as hospitals, physicians, remote doctors or emergency centers (Li et al., 2017a; 2017b; Liu et al., 2014). Since the health information is sensitive and leakage of it may cause death, it is an important security challenge to protect EBCs against any polynomial time adversary. In addition, it is also necessary to preserve the credential's privacy as the activities of a patient may reveal his health information to the adversary.

The considered system model consists of three entities namely, Network Manager (NM), WBAN client (C), and the Application Provider (AP). In this system model, NM is a trusted third party organization and responsible for secure key distribution to the WBAN clients and APs. All WBAN clients and APs register with NM and receive their respective authentication credentials. Finally, after the successful registration, C and AP mutually authenticate each other and establish a secure session between them whenever required.

Assume that $\mathcal{A}$ is a probabilistic polynomial-time (PPT) adversary and has full control over the communications between two parties, and thus, he/she can read, modify or delete the transmitted messages. In addition, $\mathcal{A}$ may get the parties secret information stored in the parties' memory with the explicit attacks. According to the Canetti-Krawczyk (CK) adversary model, defined in Canetti and Krawczyk (2001), an adversary $\mathcal{A}$ is allowed to ask the queries such as *session-state reveal* (current internal state information of incomplete session, but not related to the long-term private key), *session-key* (the session-key of a completed session) and *party-corruption* (the long-term private key). To achieve the security under the above assumptions, an authentication scheme should satisfy the following security features (Odelu et al., 2015; 2016):

- *Session-Key security (SK-security):* An authentication scheme ensures the security in the following two cases:
  (i). Even if a session key or session-state information is revealed to an adversary, other sessions should not be affected.
  (ii). Even if the long-term private keys of client and/or application provider is revealed to an adversary, the past sessions should not be compromised, which is known as the perfect forward secrecy.
- *Privacy of user credential:* In this case, even if the session ephemeral secrets revealed to an adversary from the *session-state reveal* query, an authentication scheme should guarantee the privacy of user credentials such as identity and the long-term private keys issued by the trusted key distribution center.

The rest of the paper is organized as follows: In Section 2, we summarize the related works. In Section 3, we briefly discuss the required mathematical definitions. In Section 4, we analyze security limitations of the existing authentication schemes. We then propose an efficient and secure authentication scheme for WBANs in Section 5. In Section 6, we prove that the proposed scheme is secure under the CK-adversary model. In Section 7, we present the simulations to show

the performance of the proposed scheme with the existing related schemes. Finally, we conclude the paper in Section 8.

2. Related work

The concept of WBAN was first introduced by Zimmerman (1996). Later, several variations of WBANs were presented in the literature. Due to the wireless nature of WBANs and sensitiveness of health data, security and privacy of patients is a major concern in WBANs. Thus, authentication in these scenarios plays an important role in identifying the legitimate users and prevent the unauthorized accesses. The authentication systems for WBANs can be classified into four categories (He et al., 2016): (a) physiological value based (Poon et al., 2006), (b) channel based (Zeng et al., 2010), (c) proximity based (Varshavsky et al., 2007) and (d) cryptographic based (Li et al., 2010). Among these categories, the cryptography based authentication schemes are becoming more popular than the other non-cryptographic methods. In recent years, several solutions are proposed using the traditional public-key cryptography (TPKC). Li et al. (2013, 2010) proposed authentication schemes that require large key sizes as they use modular field operations in their implementation. In order to avoid this drawback, many elliptic curve cryptography (ECC) based authentication schemes are presented (Das et al., 2015; Omala et al., 2017; Shen et al., 2018; 2015). However, these traditional authentication schemes are Public-Key Infrastructure (PKI)-based schemes. In PKI-based schemes, user's identity is bound with a certificate which contains the corresponding public key. Thus, management of a huge number of public-keys would be a challenge. In the context of security issues in EBCs, Liu et al. (2014) presented two certificateless authentication schemes by combining the idea of certificateless cryptography (Al-Riyami and Paterson, 2003; Zhang et al., 2006) and Identity-based authentication scheme (Cao et al., 2009). In Liu et al.'s (2014) scheme, a WBANs client and corresponding AP can mutually authenticate each other and share a secure session key. The proposed authentication schemes in Liu et al. (2014) combine the merits of the authentication schemes based-on traditional public key infrastructure (PKI) and Identity-based public key cryptography (ID-PKC) Cao et al. (2009). Additionally they provide security against inborn key escrow problem in ID-PKC (Shamir, 1984) and the overhead of heavy certificate management in conventional PKI.

In recent years, several Identity-based (ID-based) authentication schemes are presented (He et al., 2018; Xiong and Qin, 2015). In ID-PKC, the user identity is used as the public-key and therefore storing the public-key of the corresponding party may not be required. Zhao (2014) proved that both the preliminary and security-enhanced versions of the authentication scheme proposed by Liu et al. (2014) are insecure, and then Zhao (2014) presented an enhancement to withstand those weaknesses. Xiong (2014) also commented on the security and scalability of Liu et al.'s both preliminary and security-enhanced versions, and then presented a new authentication scheme. However, Xiong (2014) proposed authentication scheme fails to avoid the management of huge amount of public key of APs by WBAN clients. Wang and Zhang (2015) has shown that the enhanced Zhao's (2014) scheme still fails to provide the required security features, and suggested further enhancement. However, Wu et al. (2016) proved that the enhanced Wang et al.'s scheme is again insecure. Recently, He et al. (2016) again analyzed Liu et al.'s security-enhanced authentication scheme (Liu et al., 2014) and showed that it is not secure for practical applications by presenting an impersonation attack. He et al. (2016) then proposed an efficient scheme for WBANs. However, He et al.'s scheme is still has security limitations and also fails to avoid the management of large number of public-keys of APs by WBAN's clients.

Table 1 – A comparative summary of recent related authentication schemes for WBANs.

Scheme	F1	F2	F3	F4	F5
Liu et al. (2014)	N	N	N	N	N
Zhao (2014)	Y	N	N	N	Y
Wang and Zhang (2015)	Y	Y	N	N	N
Wu et al. (2016)	Y	Y	N	N	Y
He et al. (2016)	Y	Y	N	N	Y
Ours	Y	Y	Y	Y	Y

Note: F1: Mutual authentication; F2: Non-Traceability; F3: Whether user credentials are temporal; F4: Whether provides credential's privacy and protects the session-key when session-ephemeral secrets are unexpectedly revealed to an adversary; F5: Resistant Impersonation Attack; Y : Provides the security feature; N : Does not provide the security feature.

In this paper (Section 4), we discuss the limitations of the recent authentication scheme proposed by He et al. (2016) and Wu et al. (2016) in which the session ephemeral secrets are revealed to the adversary (Canetti and Krawczyk, 2001). We prove that the scheme fails to protect the credentials privacy as well as session key when the ephemeral secrets are revealed to the adversary. According to this analysis, most of the existing authentication schemes fail to protect the credential's privacy as well as session key when session ephemeral are unexpectedly revealed to the adversary. To overcome these drawbacks, we propose a new authentication scheme for WBANs. In our scheme, we use the lifetime-based pseudo-identity to reduce more vulnerability of the system when the long-term user credentials are unexpectedly revealed to an adversary. In addition, the management of huge amount of public-keys of APs by WBAN's client is not required in our scheme. The comparative summary of security features of the related authentication schemes is shown in Table 1.

3. Mathematical definitions

In this section, we briefly discuss the required mathematical definitions. Assume that two groups G_1 and G_2 are additive and multiplicative cyclic group of a prime order q, respectively. Let P be a generator of G_1. A map e: $G_1 \times G_1 \rightarrow G_2$, known as bilinear pairing, satisfies the following properties (Zhang et al., 2004):

- $e(xP, yP) = e(P, P)^{xy}$, $\forall P \in G_1$ and $\forall a, b \in Z_q^*$.
- $e(P, P) \neq 1$, where $1 \in G_2$ is the identity element.
- Computing the pairing e is efficient.

Then we call the groups $\{G_1, G_2\}$ are pairing groups.

Definition 1. Suppose G is a multiplicative cyclic group with a generator g of prime order q, and l a security parameter. The following are the computationally infeasible problem (Bao et al., 2003).

- Finding an exponent $x \in Z_q^*$ for given g and g^x is known as discrete logarithm problem (DLP).
- Computing g^{xy} for given g, g^x, and g^y, where $x, y \in Z_q^*$, is known as computational Diffie–Helman problem (CDHP). We define the advantage of an adversary $\mathcal{A}$ in solving CDHP as

$$Adv_{\mathcal{A}}^{CDH}(l) = Pr[\mathcal{A}(g, g^x, g^y) = g^{xy} \in G]$$

We say that a CDH assumption holds in G if for any polynomial-time adversary $\mathcal{A}$, the advantage $Adv_{\mathcal{A}}(l)$ is a negligible function of the security parameter l.

4. Limitations of recent works

In this section, we briefly review the limitations of He et al.'s (2016) scheme when session-specific ephemeral secrets are unexpectedly revealed to adversary $\mathcal{A}$. In the following, we show that He et al.'s (2016) scheme fails to provide the session-key security as well as user credentials' privacy. Note that the similar analysis is applicable to Liu et al. (2014), Zhao (2014), Wang and Zhang (2015), and Wu et al. (2016) schemes when session-ephemeral secrets are revealed to the adversary. Authentication scheme in EBCs consists of three roles, namely Network Manager (NM), Application Provider (AP), and WBAN's client (C). To get the authentication credentials, AP and C register with NM by sending their chosen identities. Using the received authentication credentials both AP and C mutually authenticate and establish a secure session. In the following subsections, we list the transmitted messages of authentication schemes presented in the He et al. and Wu et al.'s authentication schemes in order to discuss their limitations.

4.1. Limitations of He et al.'s (2016) scheme

When a session ephemeral secrets are revealed to the adversary $\mathcal{A}$, He et al.'s proposed scheme has many drawbacks. In Table 2, we briefly review the transmitted messages of He et al.'s authentication scheme.

Assume that an ephemeral secret x is unexpectedly revealed to the adversary $\mathcal{A}$ and $\mathcal{A}$ also captures the transmitted messages $m_1 = \{W, X, t_c\}$. Then $\mathcal{A}$ can compute the long-term private key S_{id} of C as follows:

- Compute $X'' = xP$, and search X in m_1 until match with X''. If match is found, follow the next step.
- Compute $X' = xQ_{ap}$, $k = h(X, X', t_c)$, and decrypt W using k as $(ID_c, right, U) = D_k(W)$, and then compute the secret credentials as $S_{id} = U - xvQ_{id}$, where $Q_{id} = h(ID_c, right)$ and $v = h(ID_c, right, Q_{id}, Q_{nm}, X, X', t_c)$.

In addition, $\mathcal{A}$ can also compute $K = xY = xyP$ and then the session key sk as $sk = h(X, X', Y, K)$. Thus, He et al. proposed authentication scheme fails to protect the user credentials' privacy as well as the session-key.

4.2. Limitations of Wu et al.'s (2016) scheme

In this section, we show that Wu et al.'s scheme also fails to protect the session-key and credentials' privacy when session ephemerals are revealed to the adversary. In Table 3, we briefly review the transmitted messages of Wu et al.'s authentication scheme.

Assume that the session ephemeral secret r_c is revealed to the adversary $\mathcal{A}$ and $\mathcal{A}$ also captures the communicated messages $m_1 = \{V_c, Auth_c, t_c\}$ from C to AP. Then $\mathcal{A}$ can derive the long-term secret key α_c of C as follows.

- Compute $R_c = g^{r_c}$, $V_c' = r_c(Q_{nm} + h(ID_{ap})P)$, and then search V_c in m_1 until match with V_c'. If match is found, follow the next step.
- Compute $(ID_c, t_c, \sigma_c, K_c, W_c) = D_{R_c}(Auth_c)$, $h_a = h_1(ID_c, W_c, R_c, V_c)$, and then secret credential as $\alpha_c = \frac{1}{h_a}(\sigma_c - r_c)$.

Further, $\mathcal{A}$ also computes $L_c = (R_{ap})^{r_c}$ and then the corresponding session key $sk = sk_c = h_4(t_c, R_c, R_{ap}, L_c, t_{ap})$. This shows that Wu et al.'s scheme also fails to protect the long-term secret credentials of C as well as session key.

5. Proposed authentication scheme

In this section, we propose an efficient provably secure anonymous authentication scheme. Our scheme consists of three roles such as Network Manager NM, Application Provider AP, and WBAN Client C. First, NM sets up its parameters during the initialization phase; secondly, C and AP register with NM and receive their corresponding authentication credentials to establish a secure session between them in the authentication phase. Hereafter, we use the notation provided in Table 4. The summary of all the phases of our scheme is shown in Table 5.

5.1. Initialization phase

The NM initializes with the following parameters:

1. NM chooses bilinear pairing groups $\{G_1, G_2\}$ of order q, with generators $P \in G_1$ and $g = e(P, P) \in G_2$, where e is a bilinear pairing operation defined as e: $G_1 \times G_1 \rightarrow G_2$. It also chooses the symmetric-key cryptography Ω (In our scheme, we consider AES-128 for the performance evaluation) and two cryptographic one-way hash functions $h_1 : \{0, 1\}^* \rightarrow Z_q^*$ and $h_2 : \{0, 1\}^* \rightarrow Z_q^*$. Note that we choose two different hash functions, one for generating one-time keys and another for message authentication code.
2. NM then generates its master private key $s_{nm} \xleftarrow{R} Z_q^*$ and computes public keys $Q_{nm} = s_{nm}P \in G_1$ and $g_{nm} = g^{s_{nm}} \in G_2$.
3. Finally, NM declares the public parameters $\{G_1, G_2, q, e, P, Q_{nm}, g_{nm}\ g, h_1, h_2, \Omega\}$.

Table 2 – Brief review of transmitted messages in He et al.'s scheme.

C	AP
$x \leftarrow_R Z_q^*$ Compute: $X = xP$, $X' = xQ_{ap}$, $Q_{id} = H(ID_c, right)$, $v = h(ID_c, right, Q_{id}, Q_{nm}, X, X', t_c)$, $k = h(X, X', t_c)$, $U = S_{id} + xvQ_{id}$, $W = E_k(ID_c, right, U)$ $\xrightarrow{m_1=\{W,X,t_c\}}$	
	Check t_c. Accept/Reject. Compute: $X' = s_{ap}X$, $k = h(X, X', t_c)$ Decrypt W using k Compute: $Q_{id} = H(ID_c \| right_c)$, $v = h(ID_c, right, Q_{id}, Q_{nm}, X, X', t_c)$ Check: $e(U, P) =^? e(Q_{id}, Q_{nm} + vX)$. Accept/Reject. $y \leftarrow_R Z_q^*$; Compute: $Y = yP$, $K = yX = yxP$, $sk = h(X, X', Y, K)$, $Auth = h(W, t_c, X, X', Y, K)$ $\xleftarrow{m_2=\{Y,Auth\}}$
Compute: $K = xY = xyP$, $sk = h(X, X', Y, K)$ Check: $Auth =^? h(W, t_c, X, X', Y, K)$. Accept/Reject.	

Note: H: $\{0,1\}^* \times G_1 \rightarrow G_1$ and h are secure hash functions; ID_c is identity of C; Q_{ap} is public-key of AP; Q_{nm} is public key of NM; S_{id} is long-term private key of C issued by NM; t_c: current timestamp; $x \leftarrow_R S$ means x is randomly picked from a set S.

Table 3 – Brief review of transmitted messages in Wu et al.'s scheme.

C	AP
$r_c \leftarrow_R Z_q^*$; Compute: $R_c = g^{r_c}$, $K_c = r_cP$, $V_c = r_c(Q_{nm} + h(ID_{ap})P)$, $h_a = h_1(ID_c, W_c, R_c, V_c)$, $\sigma_c = r_c + \alpha_c h_a$, $Auth_c = E_{R_c}(ID_c, t_c, \sigma_c, K_c, W_c)$. $\xrightarrow{m_1=\{V_c, Auth_c, t_c\}}$	
	Check t_c. Accept/Reject. Compute: $R'_c = e(S_{ap}, V_c)$, $D_{R'_c}(Auth_c)$, $h_b = h_2(ID_c, W_c)$ Check $\sigma_c P =^? K_c + h'_a(W_c + h_b Q_{nm})$. Accept/Reject. $r_{ap} \leftarrow_R Z_q^*$; Compute: $R_{ap} = g^{r_{ap}}$, $L_{ap} = (R_c)^{r_{ap}}$, $Auth_{ap} = h_3(t_c, R_c, R_{ap}, L_{ap}, t_{ap}, \sigma_c)$, $sk_{ap} = h_4(t_c, R_c, R_{ap}, L_{ap}, t_{ap})$, $\xleftarrow{m_2=\{t_{ap}, Auth_{ap}, R_{ap}\}}$
Check: t_{ap}. Accept/Reject. Compute: $L_c = (R_{ap})^{r_c}$ Check: $Auth_{ap} =^? h_3(t_c, R_c, R_{ap}, L_c, t_{ap}, \sigma_c)$. Accept/Reject. Compute: $sk_c = h_4(t_c, R_c, R_{ap}, L_c, t_{ap})$	

Note: $h_i : \{0,1\}^* \rightarrow Z_q^*$ are secure hash functions, $i = 1, 2, 3, 4$; Q_{nm} is public key of NM; (α_c, W_c) is long-term secret key pair of C provided by NM; $x \leftarrow_R S$ means x is randomly picked from a set S.

Table 4 – Notations used in the proposed scheme.

Symbol	Description
NM	Network Manager
G_1, G_2	Bilinear groups
P	Generator of G_1
g	Generator of G_2; $g = e(P, P)$
q	Prime order of G_1 and G_2
h_1, h_2	Secure hash functions, where $h_1, h_2 : \{0,1\}^* \rightarrow Z_q^*$
(s_{nm}, Q_{nm})	Private and public key pairs of NM; $Q_{nm} = s_{nm}P$
AP, ID_{ap}	Application provider, and its identity
(s_{ap}, K_{ap})	Private key pair of AP; $s_{ap} = h_1(K_{ap} \| ID_{ap})$
C, ID_c	WBAN client, and its identity
(s_c, g_c)	Key pair of C, where s_c is kept secret
$x \leftarrow_R S$	x is randomly picked from a set S

5.2. *Registration phase*

In this phase, WBAN's client C and the application provider AP register with NM and get the authentication credentials as follows:

5.2.1. *Client registration*

- C sends its chosen unique identity ID_c to NM via a secure channel.
- Upon receiving a request from C, NM checks its validity and then defines its access right as $Right_c = [EID_c \| right \| Lifetime]$, where $EID_c = E_{s_{nm}}(ID_c \| Lifetime)$. Next, NM chooses $r_c \overset{R}{\leftarrow} Z_q^*$ and computes $g_c = g^{r_c}$ and s_c with the condition $s_c = r_c + s_{nm}h_c$, where $h_c = h_1(g_c, Right_c, Q_{nm})$ (El-Gammal type digital signature, ElGamal, 1985). Note that, the credential $Right_c$ contains temporal identity, access right and its lifetime (it may be current day, month or year). Finally, NM sends $\{Right_c, s_c, g_c\}$ to C via a secure channel.
- C keeps secret the received credentials $\{Right_c, s_c, g_c\}$.

Remark 1. When it requires, for example the malicious activities found, NM can track the original identity of the client C from the given temporal identity $EID_c = E_{s_{nm}}(ID_c \| Lifetime)$ using its master secret key s_{nm}.

5.2.2. *AP registration*

- AP sends its chosen unique identity ID_{ap} to NM via a secure channel.

Table 5 – Summary of the proposed scheme.

Client registration phase	
Client C	NM
Choose ID_c $\xrightarrow{\{ID_c\}}$	
	Checks validity of ID_c Defines access right $Right_c = [EID_c \| \| right \| \| Lifetime]$ where $EID_c = E_{s_{nm}}(ID_c \| \| Lifetime)$. Chooses $r_c \xleftarrow{R} Z_q^*$ Computes $g_c = g^{r_c}$ and s_c with $s_c = r_c + s_{nm}h_c$ where $h_c = h_1(g_c, Right_c, Q_{nm})$ $\xleftarrow{\{Right_c, s_c, g_c\}}$.
Stores $\{Right_c, s_c, g_c\}$.	
AP registration phase	
Application Provider AP	NM
Choose ID_{ap} $\xrightarrow{\{ID_{ap}\}}$	
	Checks validity of ID_{ap} Computes $K_{ap} = \frac{1}{h_1(ID_{ap})+s_{nm}}P$. $\xleftarrow{\{K_{ap}\}}$.
Computes $s_{ap} = h_1(K_{ap} \| \| ID_{ap})$. Stores the pair (K_{ap}, s_{ap}) Publicly declares ID_{ap}	
Authentication phase	
Client C	Application Provider AP
Chooses $x_c \xleftarrow{R} Z_q^*$ and ID_{ap} of AP Computes $T_1 = x_c(h_1(ID_{ap})P + Q_{nm})$, $k_1 = g^{x_c}$, $C_1 = E_{k_1}[g_c, Right_c, t_1]$, $Auth_1 = h_2(T_1, g_c, Right_c, t_1, k_1)$. $\xrightarrow{m_1=\{T_1, C_1, Auth_1\}}$	
	Computes $k_2 = e(T_1, K_{ap})$ Retrieves $[g_c', Right_c', t_1'] = D_{k_2}(C_1)$ Checks the validity of t_1' and $Right_c'$. Accept/Reject. Checks $Auth_1 =^? h_2(T_1, g_c', Right_c', t_1', k_2)$. Accept/Reject. Generates $y_{ap} \xleftarrow{R} Z_q^*$ Computes $h_c = h_1(g_c, Right_c, Q_{nm})$ $y_1 = g_c \times g_{nm}^{h_c} = g^{s_c}$ $y_2 = y_1^{y_{ap}+s_{ap}} = g^{s_c(y_{ap}+s_{ap})}$ $sk_{ap} = (y_1 \times k_2)^{y_{ap}+s_{ap}}$ $Auth_2 = h_2(y_2, sk_{ap}, g_c, ID_c, T_1, k_2, t_2)$ $\xleftarrow{m_2=\{y_2, Auth_2, t_2\}}$
Checks the validity of t_2. Computes $sk_c = y_2^{(x_c+s_c)/s_c}$ Verifies $Auth_2 =^? h_2(y_2, sk_c, g_c, ID_c, T_1, k_1, t_2)$. Accept/Reject. Computes $Auth_3 = h_2(sk_c, k_1, y_2, t_1, t_2)$ $\xrightarrow{m_3=\{Auth_3\}}$	
	Checks $Auth_3 =^? h_2(sk_{ap}, k_2, y_2, t_1, t_2)$. Accept/Reject.

- After receiving a request from AP, NM checks its validity and then computes $K_{ap} = \frac{1}{h_1(ID_{ap})+s_{nm}}P$. Finally, NM sends K_{ap} to AP via a secure channel.
- Upon receiving credential K_{ap}, AP computes $s_{ap} = h_1(K_{ap} \| \| ID_{ap})$. Finally, AP keeps secret the pair (K_{ap}, s_{ap}) and publicly declares its identity ID_{ap}.

Remark 2. We can also replace the identity ID_{ap} of AP with temporal identity as $TID_{ap} = [ID_{ap} \| \| Lifetime]$, where $Lifetime$ may be the current month, or current year, when it is required for the system to distribute the time-dependent credentials that would strengthen the system.

5.3. *Authentication and key establishment phase*

In this phase, using the received credentials, C and AP mutually authenticate each other and establish a secure session

key. Note that the NM does not involve in the authentication process. The detailed steps are as follows:

- C chooses $x_c \xleftarrow{R} Z_q^*$ and publicly available identity ID_{ap} of AP. Then, C computes $T_1 = x_c(h_1(ID_{ap})P + Q_{nm})$, $k_1 = g^{x_c}$, $C_1 = E_{k_1}[g_c, Right_c, t_1]$, and $Auth_1 = h_2(T_1, g_c, Right_c, t_1, k_1)$, where t_1 is the current time stamp. Finally, C sends $m_1 = \{T_1, C_1, Auth_1\}$ to AP.
- After receiving m_1, AP computes $k_2 = e(T_1, K_{ap})$, and retrieves $[g_c', Right_c', t_1']$ by decrypting C_1 using computed k_2. AP then checks the validity of t_1' and $Right_c'$. If these are valid, AP further checks whether $Auth_1 = h_2(T_1, g_c', Right_c', t_1', k_2)$ holds or not. If the received message m_1 is valid, AP next generates $y_{ap} \xleftarrow{R} Z_q^*$ and computes

$$\begin{aligned} h_c &= h_1(g_c, Right_c, Q_{nm}) \\ y_1 &= g_c \times g_{nm}^{h_c} = g^{s_c} \\ y_2 &= y_1^{y_{ap}+s_{ap}} = g^{s_c(y_{ap}+s_{ap})} \\ sk_{ap} &= (y_1 \times k_2)^{y_{ap}+s_{ap}} \\ Auth_2 &= h_2(y_2, sk_{ap}, g_c, ID_c, T_1, k_2, t_2) \end{aligned}$$

  where t_2 is the current timestamp. Finally, AP sends the challenge message $m_2 = \{y_2, Auth_2, t_2\}$ to C.
- Upon receiving m_2, C checks the validity of t_2. Then C computes $sk_c = y_2^{(x_c+s_c)/s_c}$, and verifies the validity of the condition $Auth_2 = h_2(y_2, sk_c, g_c, ID_c, T_1, k_1, t_2)$. If it is valid, C authenticates AP and confirms that the shared session key is sk_c. Finally, C computes the confirmation message $Auth_3 = h_2(sk_c, k_1, y_2, t_1, t_2)$, and sends $m_3 = \{Auth_3\}$ to AP.
- After receiving m_3, AP checks the validity of the condition $Auth_3 = h_2(sk_{ap}, k_2, y_2, t_1, t_2)$. If it is valid, AP confirms that the C is legitimate and agrees on the session key sk_{ap}.

Correctness proof: The correctness of the proposed scheme is presented below:

$$\begin{aligned} sk_{ap} &= (y_1 \times k_2)^{y_{ap}+s_{ap}} \\ &= (g^{s_c} \times g^{x_c})^{y_{ap}+s_{ap}} \\ &= g^{(s_c+x_c)(y_{ap}+s_{ap})} \end{aligned} \qquad \begin{aligned} sk_c &= y_2^{(x_c+s_c)/s_c} \\ &= (g^{s_c(y+s_{ap})})^{(x+s_c)/s_c} \\ &= g^{(y_{ap}+s_{ap})(x_c+s_c)} \end{aligned}$$

Therefore, the session key computed by both the parties C and AP are same.

6. Security analysis

The rigorous formal security analysis is presented in this section, and it shows that the proposed scheme provides SK-Security under the CK-adversary model (Canetti and Krawczyk, 2001). In this model, an adversary $\mathcal{A}$ can have the ability to intercept, read and modify the transmitted messages between the communicating parties. $\mathcal{A}$ does not have direct access to the secret information, however, $\mathcal{A}$ can be allowed to obtain the secret information using the following queries.

6.1. Security proof under the CK-adversary model

Let U be a participant representing one of the three roles in the proposed protocol $\mathcal{P}$: client C, application provider AP, and network manager NM. Note that the only two parties C and AP involve in the authentication process. Assume that C_i represents ith instance of C and AP_j represents jth instance of AP. In this adversary model, an instance is considered as an oracle and employ a simulator to answer the input message.

- *Execute*(C_i, AP_j) query simulates passive attacks and allows $\mathcal{A}$ to get access to the simulated messages transmitted between the instances C_i and AP_j.
- *Send*(*M, U*) query simulates active attacks. In this query, $\mathcal{A}$ can have ability to modify messages transmitted between C_i and AP_j. If $\mathcal{A}$ sends a modified message M to the oracle U, U then answers by returning the corresponding message.
- *SSReveal*(*U*) query allows $\mathcal{A}$ to get access on the session-state information held by U, but the output of this query does not include the long-term private key of U.
- *SKReveal*(*U*) query allows $\mathcal{A}$ to get access the session key held by U.
- *Corrupt*(*U*) query simulates and captures the perfect forward secrecy. This query allows $\mathcal{A}$ to get access to the long-term private key of U.
- *Expire*(*U*) query erases the session key of a completed session held by U.
- *Test*(*U*) query returns either a session key or a random key. This query can be issued only to a session where the queries *SSReveal*, *SKReveal* and *Corrupt* have not been requested.

Semantic security: If C_i and AP_j mutually authenticate each other and share a common session key, then they are called partners. For a session, say s, held by U, if adversary $\mathcal{A}$ asks the query *SSReveal*(*U*) or *SKReveal*(*U*) or *Corrupt*(*U*) before the query *Expire*(*U*), including the case where U is corrupted even before s is created, the session s is called locally exposed. If neither s nor its matching session are locally exposed, the session s is said to be fresh. The $\mathcal{A}$'s goal in this security setting is to distinguish a fresh session key from a random key.

Adversary $\mathcal{A}$ is allowed to ask several *Test* queries to either instances of client C or application provider AP. In this query, U flips a coin b and $\mathcal{A}$ guess a bit b'. Then the advantage, say $Adv_{\mathcal{P}}^{AKE}(\mathcal{A})$, of $\mathcal{A}$ in guessing the correct bit b' is defined as follows

$$Adv_{\mathcal{P}}^{AKE}(\mathcal{A}) = |2Pr[b = b'] - 1|$$

The scheme $\mathcal{P}$ is secure against the CK-adversary under the random oracles if

$$Adv_{\mathcal{P}}^{AKE}(\mathcal{A}) \leq \epsilon,$$

for any sufficiently small $\epsilon > 0$.

Let $E_k(M)/D_k(M)$ be an XOR operation to encrypt/decrypt a message M with the key k. The *Hash*, *Send*, *Execute*, *SSReveal*, *SKReveal*, *Corrupt*, and *Test* are used to simulate real attacks.

Lemma 1 (Difference Lemma, Shoup, 2004). *Let R_1, R_2 and R_3 represent the events defined in some probability distribution. If $R_1 \wedge \neg R_3 \Leftrightarrow R_2 \wedge \neg R_3$, we have, $|Pr[R_1] - Pr[R_2]| \leq Pr[R_3]$.*

Theorem 1. *In the proposed scheme $\mathcal{P}$, G_1 and G_2 are the two sufficiently large prime order, say q, bilinear groups. Let $\mathcal{A}$ be a t-polynomial time adversary and can make at most q_s, q_e, and q_h times*

Send, Execution and *Hash queries, respectively. Let* T_{exp} *denote the cost of group exponentiation operation in* G_1 *and* G_2, *and* l *denote the security parameter. Then the advantage of* $\mathcal{A}$ *is given by*

$$Adv_{\mathcal{P}}^{AKE}(\mathcal{A}) \leq \frac{O((q_s+q_e)^2)}{q} + \frac{O(q_h^2)}{2^l} + \frac{O(q_s)}{2^{l-1}} + O(2.q_h Adv_{\mathcal{A}}^{CDHP}(t'))$$

where $t' = O(t + (q_s + q_e)\, T_{exp})$.

Proof. Using the sequence of games GM_0 to GM_4, we prove that the proposed scheme $\mathcal{P}$ is security against t-polynomial time adversary $\mathcal{A}$. Let $Succ_i$ be an event that $\mathcal{A}$ guesses correctly the bit b in *test session* in GM_i.

Game GM_0: This game simulates real attacks with random oracles. If any of the following things happen, a random bit b' is selected instead of the answer of *Test*.

- $\mathcal{A}$ does not guess b' when the game is terminated.
- $\mathcal{A}$ uses more queries/time than the pre-determined ones.

Then from definition, we have

$$Adv_{\mathcal{P}}^{AKE}(\mathcal{A}) = |2Pr[Succ_0] - 1|. \quad (1)$$

Game GM_1: This game simulates all oracles and stores answers to the oracles in three lists, namely, L_H, $L_{\mathcal{A}}$, and L_{trans}. Where L_H stores the answers of queries to the random oracles h_1 and h_2; $L_{\mathcal{A}}$ stores the answers of the random oracle queries asked by $\mathcal{A}$; and L_{trans} stores the transcripts transmitted messages. $\mathcal{A}$ can do queries using the oracles to break the privacy of authentication process and the session keys. So, the transcript distribution of the games GM_0 and GM_1 are indistinguishable, and therefore, we have

$$Pr[Succ_1] = Pr[Succ_0]. \quad (2)$$

Game GM_2: This game considers all oracles simulated in the game GM_1, and additionally performs the simulations of the Send and Hash oracles, which represents an active attack. The objective of $\mathcal{A}$ is to fool a participant to accept a modified message. In this case, adversary $\mathcal{A}$ is allowed to make different Hash queries to examine the existence of hash collisions. The following two cases causes the collisions in transcripts, which we obtain from the birthday paradox (Boyko et al., 2000):

- The upper bound of the probability of collisions in hash values is $\frac{O(q_h^2)}{2^{l+1}}$.
- The upper bound of the probability of collisions in random numbers $x, y \in \{1, q-1\}$ in different sessions is $\frac{O((q_s+q_e)^2)}{2q}$.

GM_1 and GM_2 are indistinguishable unless the collisions happen in the transcripts. Therefore, we have

$$|Pr[Succ_2] - Pr[Succ_1]| \leq \frac{O((q_s+q_e)^2)}{2q} + \frac{O(q_h^2)}{2^{l+1}}. \quad (3)$$

Game GM_3: This game simulates forging of transmitted messages without using random oracles. Consider the steps simulated under the send queries $m_1 \leftarrow Send(Start, C_i)$, $m_2 \leftarrow Send(m_1, AP_j)$ and $m_3 \leftarrow Send(m_2, C_i)$. Simulator checks if m_1, m_2 and m_3 are in L_{trans}, and $((T_1, *, *, *, *), H_2)$, $((y_2, *, *, ID_c, T_1, *, t_2), H_2)$, $((*, *, y_2, *, t_2), H_2)$ are in $L_{\mathcal{A}}$, where $*$ represents an unknown value. The adversary $\mathcal{A}$ looses the game if the submitted message, with a hash, was not previously queried. Games GM_2 and GM_3 are perfectly indistinguishable unless the Application Provider rejects $Auth_1$ or $Auth_3$, or client rejects $Auth_2$. Hence, the probability to forge the transcripts without calling random oracles is bounded by $\frac{O(q_s)}{2^l}$.

$$|Pr[Succ_3] - Pr[Succ_2]| \leq \frac{O(q_s)}{2^l}. \quad (4)$$

Game GM_4: This game considers the simulate of SK-security under the CDH assumption. The game GM_3 is same as game GM_4 except the simulator S output a random bit if *Forge* event happens where $\mathcal{A}$ made a send query in the form of $\{g^{*s_0}, h_2(g^{*s_0}, g^{*(x_i+s_0)}, g^{s_0}, ID_c, T_1, g^{x_i}, t_2), t_2\}$ and h_2 query for valid forgery $\sigma = g^{*(x_i+s_0)} = g^{*(x_i+r_0+s_{nm}h_0)}$ for challenge g^*, such that user i is not corrupted when the hash query is made. Then we have

$$|Pr[Succ_4] - Pr[Succ_3]| \leq Pr[Forge] \quad (5)$$

Lemma 2. *The Forge event happens only with a negligible probability when the CDH assumption is hold in* G_2.

Proof. Let S denote the CDH problem solver, who is given g^a, g^b, and aims to compute h^{ab}. The S simulates the game for $\mathcal{A}$ as follows:

Suppose $\mathcal{F}$ sets up the game for $\mathcal{A}$ by creating n users (set $\mathcal{U}$) with the corresponding key pairs $\{s_i, g^{r_i}\}$. $\mathcal{F}$ randomly selects an index i and guesses that the *Forge* event will happen with regard to user i and session i. S then sets the master secret key as $g^{s_{nm}} = g^a$ and generates the key pairs for other users honestly. In addition, S sets the challenge as $g^* = g^b$ in the guessed session i. If a *Forge* event with respect i does not occurs, S aborts the game. Otherwise, given a valid forgery $\sigma = g^{*(x_i+s_0)} == g^{*(x_i+r_0+s_{nm}h_0)}$ such that $Auth_2 = h_2(g^{*s_0}, \sigma, g^{s_0}, ID_c, T_1, g^{x_i}, t_2)$ holds. Note that $\mathcal{A}$ may ask *SSReveal*(U) to get session state secret x_i. According to the Forking Lemma (Bellare and Neven, 2006), by rewinding the adversary $\mathcal{A}$, S would obtain two forgeries $\sigma_1 = g^{b(r_0+s_{nm}h_0)}$ and $\sigma_2 = g^{b(r_0+s_{nm}h'_0)}$ from h_2. Therefore, S can obtain a solution to CDH as

$$h^{ab} = \left(\frac{\sigma_1}{\sigma_2}\right)^{1/(h_0-h'_0)}$$

□

We can obtain sk in the list $L_{\mathcal{A}}$ with the probability $\frac{1}{q_h}$. Let t' be the running time in all, and it is easy to obtain $t' = O(t + (q_s + q_e)T_{exp})$. Hence, we have

$$Pr[Forge] \leq O(q_h Adv_{\mathcal{P}}^{CDH}(t')). \quad (6)$$

After the game GM_4, $\mathcal{A}$ has no advantage, and therefore $Pr[Succ_4] = 1/2$. As a conclusion, from the games GM_0 to GM_4, and using Lemma 1, Eqs. (1)–(6) and triangle inequality, we obtain the result as follows:

$$\frac{1}{2}Adv_{\mathcal{P}}^{AKE}(\mathcal{A}) = Pr[succ_0] - 1/2|$$

$$|Pr[Succ_1] - Pr[succ_4]| \leq |Pr[Succ_1] - Pr[succ_2]| + |Pr[Succ_2] - Pr[succ_3]| + |Pr[Succ_3] - Pr[succ_4]|$$

$$|Pr[Succ_0] - 1/2| \leq \frac{O((q_s+q_e)^2)}{2q} + \frac{O(q_h^2)}{2^{l+1}} + \frac{O(q_s)}{2^l} + O(q_h Adv_{\mathcal{A}}^{CDHP}(t'))$$

$$\frac{1}{2}Adv_{\mathcal{P}}^{AKE}(\mathcal{A}) \leq \frac{O((q_s+q_e)^2)}{2q} + \frac{O(q_h^2)}{2^{l+1}} + \frac{O(q_s)}{2^l} + O(q_h Adv_{\mathcal{A}}^{CDHP}(t'))$$

Therefore, we have the advantage

$$Adv_{\mathcal{P}}^{AKE}(\mathcal{A}) \leq \frac{O((q_s+q_e)^2)}{q} + \frac{O(q_h^2)}{2^l} + \frac{O(q_s)}{2^{l-1}} + O(2.q_h Adv_{\mathcal{A}}^{CDHP}(t'))$$

□

6.2. Other security features

- *Credential privacy:* In our scheme, the long-term private key of the client is not directly involved in any of the three communicated messages m_1, m_2 and m_3 between C and AP. Using the long-term private key K_{ap} and the information available in the request message m_1 received from C, AP computes $y_1 = g^{s_c}$. However, computing the long-term private key s_c of C is infeasible to AP. In addition, even if session ephemeral secret x is revealed to the adversary $\mathcal{A}$, $\mathcal{A}$ can compute $y_1 = g^{s_c}$, but it is infeasible to the adversary $\mathcal{A}$ to compute s_c due to the hardness of solving DLP. As a result, our scheme provides credential privacy even if the session ephemerals are revealed to the adversary. Most of the existing schemes fail to provide credential privacy when ephemeral secrets are revealed to the adversary.
- *Anonymity:* In our scheme, the identity information of a client is presented in the request message m_1 in the form of an encrypted message $C_1 = E_{k_1}[g_c, Right_c, t_1]$, where key $k_1 = g^x$ and x is the one-time session ephemeral key. In addition, the original identity ID_c is not directly available in the encrypted message. Since deriving the decryption key $k_2 = k_1 = g^x$ is computationally infeasible due to the hardness of solving DLP and $k-CAA$. Note that $T_1 = h_1(ID_{ap})xP + xQ_{nm} = xaP$, where $a = h_1(ID_{ap}) + s_{nm}$. Thus, given $aP = h_1(ID_{ap})P + Q - nm$ and $x(aP)$, computing x is same as solving ECDLP. Hence, obtaining the identity information from the communications between C and AP is infeasible to the polynomial-time adversary.
- *Perfect forward secrecy:* This security feature ensures that all past session keys are secure even if the long-term private keys of all participants are unexpectedly revealed to the adversary. In our scheme, the construction of the session key $sk = g^{(y_{ap}+s_{ap})(x_c+s_c)}$ involves the long-term private keys as well as the session-ephemeral secrets. Thus, computing the session keys of completed sessions even using the long-term keys alone is computationally infeasible due to hardness of solving CDHP.
- *Unlinkability and non-traceability:* This property ensures that except the communicating parties WBAN client and AP, no other parties including NM can link two different protocol sessions. In our proposed authentication scheme, an adversary is unable to derive any common piece of message from two different communicated messages since they are encrypted. In addition, from the above discussions, our proposed scheme provides anonymity. Therefore, in our scheme, it is hard to link two different messages without having appropriate secret information. As a results, our scheme prevents traceability attack and provides unlinkability feature.
- *Mutual authentication:* In our proposed scheme, each round of communicated messages is signed with the corresponding parties' long-term private keys. So generating forgery of communicated messages is hard to the adversary. From the communication message $m_2 = \{y_2, Auth_2, t_2\}$, WBANs client C confirm the validity of the AP, and send the confirmation message $m_3 = \{Auth_3\}$ to AP. Therefore, from the message $m_3 = \{Auth_3\}$, AP authenticates C, and agrees on the session-key derived in the protocol. Since finding collusion in the hash and forging the communication messages is hard, man-in-the-middle-attack is hard. Hence, C and AP securely authenticate each other and establish a secure session.
- *Resist impersonation attack:* This feature ensures that an adversary cannot establish a session with either WBAN client C or AP without the corresponding secret credentials. Suppose, the session ephemeral x_c of C is unexpectedly revealed to the adversary $\mathcal{A}$. In this case, even if $\mathcal{A}$ computes the valid request message with the retrieved values g_c, $Right_c$ from m_1, $\mathcal{A}$ cannot compute the session key $sk_c = y^{(x_c+s_c)/s_c}$ and then the valid confirmation message m_3 in the next round as it requires the C's private key s_c. On the other hand, $\mathcal{A}$ cannot also use the retrieved values x_c, g_c, and $Right_c$ to impersonate AP to C since each request message is generated freshly with the new random numbers. That is, one request generates ephemeral secret, say x_c, then the other request is generated with the different ephemeral, say $x_c' (\neq x_c)$. Thus, using the ephemeral secret of one session in another session is not possible. This is same as even if the ephemeral secret y_{ap} is unexpectedly revealed to the adversary $\mathcal{A}$, computing valid reply message is harder without the knowledge of AP's private key K_{ap} which is used to retrieve verification key $k_2 = g^{x_c}$. From the above discussions, we can observe that the user credentials are secure even if the session exposure attacks are launched by the adversary. In addition, our scheme also provides mutual authentication and unlinkability. This implies that any adversary without appropriate secret credentials can pass the authentication process. Thus, our scheme is secure against impersonation attacks.
- *Non-repudiation:* In our scheme, both client C and application provider AP mutually authenticate each other based on their identity information and sign authentication parameters included in the communicated messages. From Theorem 1, it is clear that generating a valid message without the corresponding secret credentials is infeasible due to the hardness of solving ECDLP. Hence our scheme provides security against man-in-the-middle attack, and provides mutual authentication between two communicating parties. This implies that the two parties do not disagree on their communicated messages as the identity credentials are unique to each party.
- *No key escrow:* As most of the existing authentication schemes, our scheme also does not satisfy the key escrow

Table 6 – The average execution timings for individual operations.

	TG_e (ms)	TG_1 (ms)	TG_2 (ms)	TG_{add} (ms)
AP	0.6309	1.2564	0.1345	0.0382
Client	27.2036	23. 1	3.9545	0.1655
	TG_{mul} (ms)	TG_H (ms)	T_Ω (ms)	T_h (ms)
AP	0.0309	2.6855	0.0071	0.0071
Client	0. 0364	54.5909	0.0073	0.0073

TG_e: Execution time for one pairing operation; TG_1: Execution time for one scalar multiplication operation in G_1; TG_2: Execution time for one exponentiation operation in G_2; TG_{add}: Execution time for point addition operation in G_1; TG_{mul}: Execution time for group multiplication operation in G_2; TG_H: Execution time for one hash-to-point operation in pairing groups; T_Ω: Execution time for one symmetric encryption/decryption operation (AES-128); T_h: Execution time for one hash function operation (SHA-256).

property since it is infeasible to derive the session-key of the completed session even using the master private key of NM.

7. Performance analysis

In this section, we presented the rigorous performance analysis of the proposed scheme compared with other existing authentication schemes proposed by Liu et al. (2014), Zhao (2014), Wang and Zhang (2015), Wu et al. (2016), and He et al. (2016).

Since JPBC library (De Caro and Iovino, 2011) supports efficient pairing operations and JAVA is platform-independent, the use of JPBC library provides efficient solutions for mobile applications. In this paper, we use the *Type A* pairings from the JPBC library (De Caro and Iovino, 2011) to evaluate the computational efficiency of our proposed scheme compared with other related existing schemes. *Type A* pairings are constructed on the curve $y^2 = x(x^2 + 1)$ over the field F_p for some prime $p = 3(\mod 4)$. It is a symmetric pairing and G_1 is the group of points $E(F_p)$. In addition, $\#E(F_p) = p + 1$ and $\#E(F_{p^2}) = (p+1)^2$ with embedding degree 2, and then G_2 is a subgroup of F_{p^2}. The order q, of G_1, is some prime factor of $p+1$. We assume the WBANs client as smart mobile device and application provider as High-end desktop. To compute the computational costs required for both registration as well as authentication, we use the Emulated Android Device with Quad Core Processor, 2 GB RAM and Android Mashmallow 6.0 × 86 OS for WBANs client, and Desktop is with Intel®; Core™ i7-6700 CPU @ 3.40GHz × 8 processor, 16 GB RAM and 64-bit Ubuntu 14.04 OS for the application provider AP. We run each operation in multiple of tens and then calculate the average execution timings using the following formula. Assume that T_m be the m-times execution of one cryptographic operation.

$$T_{avg} = \frac{T_{10} + T_{20} + \ldots + T_{100}}{10 + 20 + \ldots + 100}$$

We use the SunJCE (Java Cryptography Extension) library for AES-128 and SHA-256. The execution timings of individual cryptographic operations are presented in Table 6. Note that *Type A* pairing is the fastest pairing in both PBC and JPBC libraries (He et al., 2015).

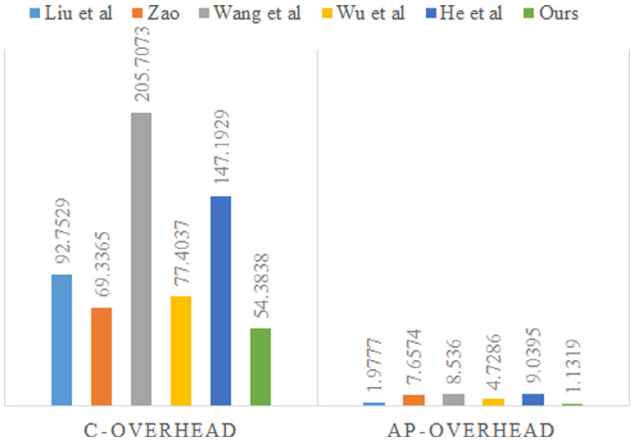

Fig. 2 – Comparison of computational cost of C and AP in milliseconds.

In Table 7, we compare the computation cost required for both client and application provider in our scheme and other related schemes. In our authentication and key agreement phase, the required computation cost for client is $2TG_1 + 2TG_2 + 1TG_{add} + 2TG_{mul} + 4T_h + 1T_\Omega \approx 54.3838$ ms and for application provider is $1TG_e + 3TG_2 + 2TG_{mul} + 4T_h + 1T_\Omega \approx 1.1319$ ms. Whereas other related schemes Liu et al. (2014), Zhao (2014), Wang and Zhang (2015), Wu et al. (2016), and He et al. (2016), respectively, requires the running times at client side approximately 92.7529 ms, 69.3365 ms, 205.7073 ms, 77.4037 ms, and 147.1929 ms, and at AP side approximately 1.9777 ms, 7.6574 ms, 8.536 ms, 4.7286 ms, and 9.0395 ms. The summary of computational overheads of various schemes is shown in Fig. 2, and we observe that our proposed authentication scheme significantly reduces the computation overheads for WBAN client as well as the application provider.

In addition, we estimated the communication overheads in various related schemes as follows: We assume that the size of parameters are as presented in He et al. (2016): Identity (ID) 32-bits, timestamp (TS) 32-bits, right (R) 64-bits, symmetric-key (SK) 128 bits, primes p 1024 bits and q 160 bits, and elements on G_1 1024 bits and G_2 512 bits.

- Liu et al. (2014): $2|q| + 3|G_1| + |TS| = 2(160) + 3(1024) + 32 =$ 3424 bits.
- Zhao (2014): $3|q| + |3|G_1| + |TS| + |R| = 3(160) + 3(1024) + 32 +$ $64 = 3648$ bits.
- Wang and Zhang (2015): $|q| + 3|G_1| + 2|TS| + |ID| = 160 +$ $3(1024) + 2(32) + 32 = 3328$ bits.
- Wu et al. (2016): $3|q| + 2|G_1| + |G_2| + 3|TS| + |ID| = 3(160) +$ $2(1024) + 512 + 3(32) + 32 = 3168$ bits.
- He et al. (2016): $|q|+3|G_1|+|R|+|ID| = 160+3(1024)+64+32 =$ 3328 bits.
- Ours: $3|q| + |G_1| + |G_2| + |R| + |ID| + 3|TS| = 3(160) + 1024 +$ $512 + 64 + 32 + 3(32) = 2208$ bits.

The summary of the computational overheads required in various related schemes is shown in Table 8. Our scheme also significantly reduces the communicational overhead as compared to the other related schemes.

Table 7 – Comparison of computational overhead for key agreement phase.

Scheme	Client	Application provider
Liu et al. (2014)	$4TG_1 + 2TG_{add} + 3T_h \approx 92.7529$ ms	$1TG_e + 1TG_1 + 1TG_{add} + 1TG_{mul} + 3T_h \approx 1.9777$ ms
Zhao (2014)	$3TG_1 + 4T_h + 1T_\Omega \approx 69.3365$ ms	$6TG_1 + 2TG_{add} + 5T_h + 1T_\Omega \approx 7.6574$ ms
Wang and Zhang (2015)	$1TG_e + 3TG_1 + 2TG_H + 2T_h + 1T_\Omega \approx 205.7073$ ms	$1TG_e + 2TG_1 + 2TG_H + 2T_h + 1T_\Omega \approx 8.536$ ms
Wu et al. (2016)	$3TG_1 + 2TG_2 + 1TG_{add} + 3T_h + 1T_\Omega \approx 77.4037$ ms	$1TG_e + 3TG_1 + 2TG_2 + 2TG_{add} + 2T_h + 1T_\Omega \approx 4.7286$ ms
He et al. (2016)	$4TG_1 + TG_H + TG_{add} + 4T_h + 1T_\Omega \approx 147.1929$ ms	$2TG_e + 4TG_1 + TG_H + TG_{add} + 4T_h + 1T_\Omega \approx 9.0395$ ms
Our proposed scheme	$2TG_1 + 2TG_2 + 1TG_{add} + 2TG_{mul} \approx 54.3838$ ms	$1TG_e + 3TG_2 + 2TG_{mul} + 4T_h + 1T_\Omega + 4T_h + 1T_\Omega \approx 1.1319$ ms

Table 8 – Comparison of communication overhead.

Scheme	Communication overhead (in bits)
Liu et al. (2014)	3424
Zhao (2014)	3648
Wang and Zhang (2015)	3268
Wu et al. (2016)	3168
He et al. (2016)	3328
Our proposed scheme	2208

Table 9 – Comparison of storage overhead.

Scheme	Client (in bits)	Application provider (in bits)
Liu et al. (2014)	2112	(160 + 1536n)
Zhao (2014)	(5544n + 32)	160
Wang and Zhang (2015)	1024	1024
Wu et al. (2016)	1084	1024
He et al. (2016)	1088	160
Our proposed scheme	1248	1024

Finally, in Table 9, we present the comparison of storage overheads for both the client and application provider. The storage overhead for client in our scheme is little more than authentication schemes proposed by Wang and Zhang (2015), Wu et al. (2016), and He et al. (2016). However, in order to reduce the system vulnerability when the user credentials unexpectedly revealed to an adversary, we use the life-time based pseudo-identity in our scheme, whereas other schemes cannot provide such facility. As a conclusion, our scheme reduces significantly the overheads of both client and application provider, and provides more security features as compared to the related existing schemes in the literature.

8. Conclusion

We have first analyzed limitations of the existing authentication schemes and shown that those schemes fail to protect session key as well as the privacy of the credentials when the session ephemeral secrets unexpectedly revealed to an adversary. We have proposed a new provably secure privacy preserving device authentication scheme in WBANs for industrial e-health applications. Through the rigorous security analysis, we have shown that our proposed scheme provides strong credentials' privacy and session-key security under the widely accepted CK-adversary model. We have estimated the computational overheads for both client and application provider for various related schemes using the execution timings calculated using JPBC library and SunJCE. In addition, we also compare the required communication overheads and storage overheads. The comparison results show that our proposed scheme provides reduced computational overheads along with more security features as compared to other existing schemes in the literature. Our scheme is suitable for developing privacy preserving e-health applications.

REFERENCES

Al-Riyami SS, Paterson KG. Certificateless public key cryptography. In: Proceedings of international conference on the theory and application of cryptology and information security. Springer; 2003. p. 452–73.

Bao F, Deng RH, Zhu H. Variations of diffie-hellman problem. In: Proceedings of international conference on information and communications security, Huhehaote, China. Springer; 2003. p. 301–12.

Bellare M, Neven G. Multi-signatures in the plain public-key model and a general forking lemma. In: Proceedings of the 13th ACM conference on computer and communications security. ACM; 2006. p. 390–9.

Boyko V, MacKenzie P, Patel S. Provably secure password-authenticated key exchange using diffie-hellman. In: Proceedings of international conference on the theory and applications of cryptographic techniques, Bruges, Belgium. Springer; 2000. p. 156–71.

Canetti R, Krawczyk H. Analysis of key-exchange protocols and their use for building secure channels. In: Proceedings of international conference on the theory and applications of cryptographic techniques, Innsbruck, Austria. Springer; 2001. p. 453–74.

Cao X, Zeng X, Kou W, Hu L. Identity-based anonymous remote authentication for value-added services in mobile networks. IEEE Trans Veh Technol 2009;58(7):3508–17.

Chen M, Gonzalez S, Vasilakos A, Cao H, Leung VC. Body area networks: a survey. Mob Netw Appl 2011;16(2):171–93.

Das AK, Chatterjee S, Sing JK. A new biometric-based remote user authentication scheme in hierarchical wireless body area sensor networks. Adhoc Sens Wirel Netw 2015;28(3/4):221–56.

De Caro A, Iovino V. jpbc: Java pairing based cryptography. In: Proceedings of the 16th IEEE symposium on computers and communications, ISCC 2011, Kerkyra (Corfu), Greece. Kerkyra, Corfu, Greece, June 28 - July 1: IEEE; 2011. p. 850–5.

ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans Inf Theory 1985;31(4):469–72.

He D, Chan S, Guizani M. Handover authentication for mobile networks: security and efficiency aspects. IEEE Netw 2015;29(3):96–103.

He D, Zeadally S, Kumar N, Lee JH. Anonymous authentication for wireless body area networks with provable security. IEEE Syst J 2016:1–12. doi:10.1109/JSYST.2016.2544805.

He D, Zeadally S, Wu L. Certificateless public auditing scheme for cloud-assisted wireless body area networks. IEEE Syst J 2018;12(1):64–73.
Hossain MS, Muhammad G. Cloud-assisted industrial internet of things (iiot)–enabled framework for health monitoring. Comput Netw 2016;101:192–202.
Li M, Yu S, Guttman JD, Lou W, Ren K. Secure ad hoc trust initialization and key management in wireless body area networks. ACM Trans Sens Netw 2013;9(2):18.
Li M, Yu S, Lou W, Ren K. Group device pairing based secure sensor association and key management for body area networks. In: Proceedings of the 2010 IEEE INFOCOM, San Diego, CA, USA. IEEE; 2010. p. 1–9.
Li T, Zheng Y, Zhou T. Efficient anonymous authenticated key agreement scheme for wireless body area networks. Secur Commun Netw 2017a;2017:1–8.
Li X, Ibrahim MH, Kumari S, Sangaiah AK, Gupta V, Choo KKR. Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks. Comput Netw 2017b.
Liu J, Zhang Z, Chen X, Kwak KS. Certificateless remote anonymous authentication schemes for wirelessbody area networks. IEEE Trans Parallel Distrib Syst 2014;25(2):332–42.
Movassaghi S, Abolhasan M, Lipman J, Smith D, Jamalipour A. Wireless body area networks: a survey. IEEE Commun Surv Tutor 2014;16(3):1658–86.
Odelu V, Das AK, Goswami A. A secure biometrics-based multi-server authentication protocol using smart cards. IEEE Trans Inf Forensics Secur 2015;10(9):1953–66. doi:10.1109/TIFS.2015.2439964.
Odelu V, Das AK, Wazid M, Conti M. Provably secure authenticated key agreement scheme for smart grid. IEEE Trans Smart Grid 2016:1. doi:10.1109/TSG.2016.2602282.
Omala AA, Kibiwott KP, Li F. An efficient remote authentication scheme for wireless body area network. J Med Syst 2017;41(2):25.
Patel M, Wang J. Applications, challenges, and prospective in emerging body area networking technologies. IEEE Wirel Commun Mag 2010;17(1):80–8.
Poon CC, Zhang YT, Bao SD. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. IEEE Commun Mag 2006;44(4):73–81.
Shamir A. Identity-based cryptosystems and signature schemes. In: Proceedings of workshop on the theory and application of cryptographic techniques. Springer; 1984. p. 47–53.
Shen J, Chang S, Shen J, Liu Q, Sun X. A lightweight multi-layer authentication protocol for wireless body area networks. Futur Gener Comput Syst 2018;78:956–63.
Shen J, Tan H, Moh S, Chung I, Liu Q, Sun X. Enhanced secure sensor association and key management in wireless body area networks. J Commun Netw 2015;17(5):453–62.
Shoup V. Sequences of games: a tool for taming complexity in security proofs. IACR Cryptol EPrint Arch 2004;2004:332.
Varshavsky A, Scannell A, LaMarca A, De Lara E. Amigo: Proximity-based authentication of mobile devices. In: Proceedings of international conference on ubiquitous computing, Innsbruck, Austria. Springer; 2007. p. 253–70.
Wang C, Zhang Y. New authentication scheme for wireless body area networks using the bilinear pairing. J Med Syst 2015;39(11):136.
Wu L, Zhang Y, Li L, Shen J. Efficient and anonymous authentication scheme for wireless body area networks. J Med Syst 2016;40(6):1–12.
Xiong H. Cost-effective scalable and anonymous certificateless remote authentication protocol. IEEE Trans Inf Forensics Secur 2014;9(12):2327–39.
Xiong H, Qin Z. Revocable and scalable certificateless remote authentication protocol with anonymity for wireless body area networks. IEEE Trans Inf Forensics Secur 2015;10(7):1442–55.
Zeng K, Govindan K, Mohapatra P. Non-cryptographic authentication and identification in wireless networks. IEEE Wirel Commun 2010;17(5):56–62.
Zhang F., Safavi-Naini R., Susilo W.. An efficient signature scheme from bilinear pairings and its applications. Public Key Cryptography–PKC 20042004;:277–290.
Zhang Z, Wong DS, Xu J, Feng D. Certificateless public-key signature: security model and efficient construction. In: Proceedings of international conference on applied cryptography and network security. Springer; 2006. p. 293–308.
Zhao Z. An efficient anonymous authentication scheme for wireless body area networks using elliptic curve cryptosystem. J Med Syst 2014;38(2):13.
Zimmerman TG. Personal area networks: near-field intrabody communication. IBM Syst J 1996;35(3.4):609–17.

Odelu Vanga is currently working as an Assistant Professor at Birla Institute of Technology & Science Pilani, Hyderabad Campus, Hyderabad. He has been awarded Outstanding Potential for Excellence in Research and Academics (OPERA) by BITS Pilani. He was selected as an Outstanding Young Foreign Scholar "Korean Research Fellowship (KRF-2017)" by the Korean Government (Global competition among 15 positions). He completed his Ph.D. in Network Security and Cryptography at Indian Institute of Technology, Kharagpur in 2016. He also completed his M.Tech. from Indian Institute of Technology kharagpur. His research spans over cryptography, network security, hierarchical access control, attribute-based encryption, remote user authentication, security in cloud computing, and Internet of Things. He is a Track Chair for the Intelligent Security Systems of Fifth International Conference on Mining Intelligence and Knowledge Exploration (MIKE-2017 & 2018). He is an active reviewer for several SCI-indexed journals including IEEE Transactions, Elsevier, Springer and Technical Program Committee member for several reputed International Conferences.

Sourav Saha received the B.Tech degree in Computer Science and Engineering from Central Institute of Technology, Kokrajhar, India. He is currently pursuing MS by Research with the Department of Computer Science and Engineering, Indian Institute of Information Technology, Sri City, India. His research interests include cryptography, network security and security in Internet-of-Things.

Rajendra Prasath is an Associate Professor with the Department of Computer Science and Engineering, Indian Institute of Information Technology, Sri City, India. He received his Ph.D. in Mathematics & Computer Science from University of Madras, Chennai; M.Tech. and Ph.D. in Computer Science and Engineering from Indian Institute of Technology (IIT), Kharagpur, India. In 2013, Rajendra started his postdoctoral position at the National University of Ireland, University College Cork (UCC), Cork, Ireland and developed the BMIDEA framework at the Department of Business Information Systems, UCC, Ireland. Currently, Rajendra is working on knowledge discovery tasks from scientific articles. Rajendra serves as one of the founding volume editors of

MIKE conference series. He is a professional member of ACM, International Rough Set Society (IRSS), Warsaw and Information Retrieval Society of India. His research interests include information retrieval, machine learning, unstructured text mining, textual case based reasoning, and big data analysis for business intelligence.

Lakshminarayana Sadineni received the M.S. degree in information technology from International Institute of Information Technology(IIIT)-Hyderabad, India. He is currently pursuing his Ph.D. with the Department of Computer Science and Engineering, Malaviya National Institute of Technology, Jaipur, India. He has done five months internship in Salesforce.com India Pvt Ltd. His research interests include cryptography, network security and security in Internet-of-Things.

Mauro Conti is an Associate Professor at the University of Padua, Italy. He obtained his Ph.D. from Sapienza University of Rome, Italy, in 2009. After his Ph.D., he was a Post-Doc Researcher at Vrije Universiteit Amsterdam, The Netherlands. In 2011 he joined as Assistant Professor the University of Padua, where he became Associate Professor in 2015. In 2017, he obtained the national habilitation as Full Professor for Computer Science and Computer Engineering. He has been Visiting Researcher at GMU (2008, 2016), UCLA (2010), UCI (2012, 2013, 2014, 2017), TU Darmstadt (2013), UF (2015), and FIU (2015, 2016). He has been awarded with a Marie Curie Fellowship (2012) by the European Commission, and with a Fellowship by the German DAAD (2013). His main research interest is in the area of security and privacy. In this area, he published more than 200 papers in topmost international peer-reviewed journals and conference. He is Associate Editor for several journals, including IEEE Communications Surveys & Tutorials and IEEE Transactions on Information Forensics and Security. He was Program Chair for TRUST 2015, ICISS 2016, WiSec 2017, and General Chair for SecureComm 2012 and ACM SACMAT 2013. He is Senior Member of the IEEE.

Minho Jo (M'07) is now a Professor in the Department of Computer Convergence Software, Korea University, Sejong Metropolitan City, South Korea. He received his BA in the Dept. of Industrial Engineering, Chosun Univ., S. Korea in 1984, and his Ph.D. in the Dept. of Industrial and Systems Engineering, Lehigh University, USA, in 1994, respectively. He is one of founders of Samsung Electronics LCD Division. He is the Founder and Editor-in-Chief of the KSII Transactions on Internet and Information Systems (SCI and SCOPUS indexed). He was awarded with Headong Outstanding Scholar Prize 2011. He is currently an Editor of IEEE Wireless Communications, Associate Editor of IEEE Internet of Things Journal, an Associate Editor of Security and Communication Networks, and an Associate Editor of Wireless Communications and Mobile Computing, respectively. He is now the Vice President of the Institute of Electronics and Information Engineers (IEIE), and was Vice President of the Korea Information Processing Society (KIPS). Areas of his current interests include LTEUnlicensed, cognitive radio, IoT, HetNets in 5G, green (energy-efficient) wireless communications, mobile cloud computing, network function virtualization, 5G wireless communications, optimization and probability in networks, network security, and massive MIMO.