ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 3, April 2016

Authentication System Based on Certificateless Cryptography in Wireless Body Area Networks

S.Padma[1], D.C.Joy Winnie Wise[2]

[1]M.E student, [2]Professor and Head

[1, 2] Department of CSE, Francis Xavier Engineering College, Tamilnadu, India

[1]spadma93@yahoo.com

[2]joywinniewise@yahoo.com

***Abstract*—** As a subgroup of Wireless sensor network, Wireless Body Area Network (WBAN) has been recognized as one of the emerging techniques for improving the healthcare service. However the security and privacy of user's physiological information remains a major concern. Even though many remote anonymous authentication protocols have been proposed, it raises challenges such as forward security and scalability. This paper proposes a new certificateless remote anonymous authentication protocol that efficiently addresses the above challenges. Apart from the security requirements provided by the existing protocols it also achieves forward security, scalability and inherent key escrow. Our protocol ensures that even the network manager which serves as a key generating centre cannot impersonate the legitimate users. Performance evaluation demonstrates that the proposed authentication protocol outperforms all the other existing schemes in terms of computational cost.

***Keywords*—** Wireless Body Area Network, Forward security, Anonymous, inherent key escrow, scalability, Certificateless**.**

I. INTRODUCTION

Recently, with the technological advancement in sensors, low power integrated circuits and wireless communication, Wireless Body Area Network (WBAN) has emerged as one of the promising techniques. As a subgroup of wireless sensor networks, it is mainly designed to monitor the health conditions of the patients for early risk detection. A WBAN makes use of wireless sensor nodes that can either be implanted inside the human body or worn externally. These intelligent sensors monitor various vital signs such as temperature, pressure and ECG and provide feedback to the user. Data collected by the various sensors are analyzed and then transmitted to the medical servers or Application providers (APs). The reliable message transmission between the sensors and the application providers is achieved using a Portable Personal Device (PPD).Fig.1 shows the architecture of WBAN in which the information from the body sensor is transmitted to the portable personal device which in turn is transmitted to the medical servers through the internet.

With the rapid development in the WBAN, the security and the privacy of the data that is being transmitted over the internet is a major unsolved concern. These data should be made accessible only by the authorized parties. Even though various security solutions are proposed for Wireless Sensor Networks (WSN) they are not applicable to WBAN due to resource constraints such as energy, memory etc…To address the security issues in WBAN, this paper proposes a new certificateless remote anonymous authentication protocol by incorporating the idea of certificateless cryptography. Different from the previous existing protocols, our protocol also provides forward security, scalability and key escrow resilience.

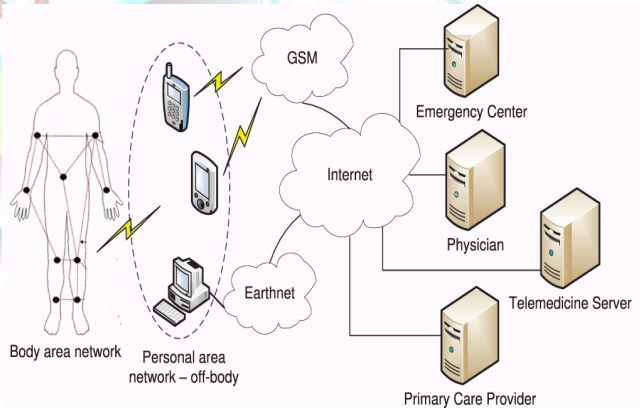

Fig. 1 WBAN Architecture

II. RELATED WORKS

Identity-based remote authentication protocol [1] [2] has been proposed to overcome the drawbacks caused by the public key certificates. However it has a major disadvantage of key escrow resilience. To overcome this disadvantage Liu et al suggested a pair of

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 3, April 2016

light weight and efficient certificateless remote anonymous authentication protocols [3] based on the certificateless signature scheme. It is implemented by incorporating the idea of certificateless cryptography [6] and Identity-based remote authentication protocol [4][5]. Even though the certificateless signature scheme is computationally efficient and secure against existential forgery the existing remote authentication protocol raise challenges such as achieving forward security and eliminating the need for distributing the clients account information to the APs. So a scalable remote anonymous authentication protocol is proposed to achieve forward security and scalability with improved computational efficiency. In this scheme elliptic curve cryptography [8] is used for generating the keys for the WBAN clients and the APs.

III. System Analysis And Design

A. *Objectives*

The proposed authentication protocol satisfies the following design objectives.

1.) *Anonymity:* Any outsider except for the requesting client and the application provider is unable to link a particular protocol session to a particular identity.

2.) *Mutual authentication:* WBAN clients and the application providers authenticate each other to verify their identities.

3.) *Session Key establishment:* A session key is established between the WBAN clients and the application providers for secure subsequent communication.

4.) *Forward Security:* Even if the private key of the participant has been corrupted the session key will not be compromised.

5.) *Key escrow resilience:* Even the Network manager which acts as the key generating center cannot impersonate the legitimate users.

B. *System Model*

The proposed system consists of three types of entities.Fig.2 shows the system design of the proposed protocol.

1.) *Network Manager (NM):* It acts as a key generating center and is responsible for the registration of WBAN clients and the APs. Instead of a completely trusted third party it is assumed to be a commercial organization that that can derive commercial benefits.

2.) *WBAN client:* It includes wearable sensors, biosensor or a portable medical device. It should be registered with the Network Manager before they access the service offered by the AP and needs to be preloaded with the public parameters.

3.) *Application Provider (AP):* Application providers may be hospital, physicians or any other medical servers. It should also be registered with NM before they offer the service requested by WBAN clients. It is also preloaded with the public parameters.

C. *Proposed protocol*

To remedy the weaknesses in the existing protocol, a scalable certificateless remote authentication protocol with anonymity and forward security for WBANs is proposed. The major contributions can be summarized as follows:

- A secure and lightweight certificateless remote authentication protocol is proposed by elaborately incorporating the certificateless encryption and two-party authenticated key agreement protocol.
- Experimental simulation reveals that our protocol outperforms the previous protocols in terms of communication overhead and computation cost.

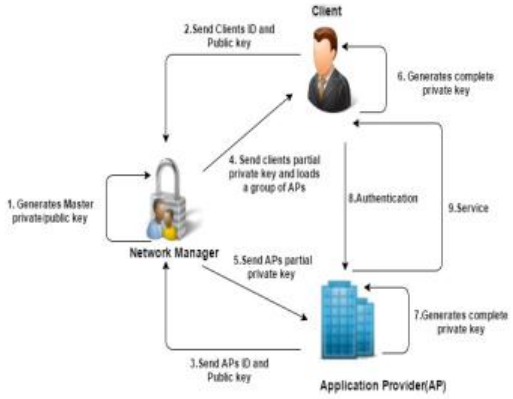

Fig. 2 System design

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 3, April 2016

In the proposed protocol ephemeral key is chosen during the establishment of the session key and the session key is generated using this ephemeral key and the private key. So the exchanged data in the previous session will still be secure even if the long-term private key of the participant has been corrupted thereby achieving forward security. By adopting the encryption technique to realize anonymity, the proposed protocol eliminates the delivery of clients' account information to APs, and thus provides better scalability.

An Efficient Bilinear Pairing-Free Certificateless Two-Party Authenticated Key Agreement Protocol is used to generate the session key which is used for secure communication. In this protocol the number of scalar multiplication is 4. It provides much better performance than the existing protocol and it is more suitable for practical applications.

D. Advantages

- Achieves Forward security.
- Provides Scalability.
- Reduces the computational time.
- Provides better performance.

It consists of 3 phases: Initialization, Registration and Authentication.

1.) Initialization: NM performs the following operations initially.

NM generates a prime p and publishes the params $\{F_p , E/F_p , G , P\}$ according to the definition in certificateless signature scheme.

- NM randomly picks $s \in Z_m^*$ as its master private key and compute its public key $P_{NM}=s.P$
- For a security parameter r, NM selects a Message Authentication Code and four secure hash functions $H_1:\{0,1\}^r \rightarrow Z_m^*$, $H_2:\{0,1\}^* x \{0,1\}^* x G x G \rightarrow Z_m^*$, $H_3:\{0,1\}^* x \{0,1\}^* x G x G x G \rightarrow Z_m^*$, $H_4:\{0,1\}^* x \{0,1\}^* x G x G x G x G \rightarrow Z_m^*$
- NM then publishes the params $\{F_p , E/F_p , G , P\}$ as system parameters and loads them into WBAN clients and the APs.

2.) Registration: An AP needs to perform the following operations with NM before it offer the services to the requested WBAN clients.

An AP with the identity ID_A chooses a secret value $s_A \in Z_m^*$ and determines the user secret key sk_A and computes the public key $pk_A=s_A.P$.

- AP sends its identity and the public key to the NM.
- On receiving the identity and the public key of the AP,NM selects at random $q_A \in_R Z_m^*$.
- NM then computes $Q_A=q_A.P$, $g_A=H_1(ID_A \| Q_A \| pk_A)$, $d_A=q_A + g_A .x$
- Partial Private key (d_A , Q_A) is then transmitted secretly to the AP by the NM.

Similarly a WBAN client with the real identity ID_c performs the above operations with NM before it access the service provided by the client. The only difference is that it selects a pseudo-identity ID_R and sends it to NM along with its identity and the public key. Finally, NM transmits the partial private key (d_c , Q_c) and a group of APs $\{ID_A , Q_A , pk_A\}$ to the clients secretly.

3.) Authentication: WBAN client with the pseudo-id ID_R performs the following steps:

- Select an ephemeral key at random $t \in_R Z_m^*$.
- Compute the token $T_A= t.P$ and select the time t_c
- Compute $m=H_2(ID_R , pk_R , Q_R , T_A , t_c)$
- $R_1=m.P$, $R_2=H_3(m(pk_A + Q_A + g_A P_{NM}) \text{ XOR } (ID_R \| pk_R \| Q_R \| T_A \| t_c)$
- Then the WBAN client sends the request message to the AP $R=(R_1 , R_2)$

Once the AP receives the request message, it authenticates the WBAN client by performing the following steps:

- Compute $(ID_R \| pk_R \| Q_R \| T_A \| t_c) = H_3((s_A+d_A)R_1) \text{ XOR } R_2$
- Check the validity of the time t_c and $H_2(ID_R , pk_R , Q_R , T_A , t_c)=R_1$ is satisfied.
- Select an ephemeral key at random $w \in_R Z_m^*$ and compute the token $T_B= w.P$
- Compute $K_A^1=(s_A+d_A+T_A)(pk_R+Q_R+H_1(ID_R,Q_R).P_{NM})$ and $K_A^2=(s_A+d_A+T_A)(T_B+Q_R+H_1(ID_R , Q_R).P_{NM})$
- Compute key=$H_4(ID_R \| ID_A \| T_A \| T_B \| K_A^1 \|$

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 3, April 2016

K_A^2)

- Send the reply message $MAC_{key}(T_B)$ and send ($MAC_{key}(T_B)$,T_B) to the WBAN client.

On receiving the reply message WBAN client performs the following steps:

- Compute $K_A^1=(s_R+d_R)(pk_A+Q_A+H_1(ID_A,Q_A).P_{NM}+ T_B)$ and $K_A^2=(d_R+T_A)$)$(pk_A+Q_A+H_1(ID_A,Q_A).P_{NM}+ T_B)$

- Compute key=$H_4(ID_R \| ID_A \| T_A \| T_B \| K_A^1 \| K_A^2)$

Check the freshness of $MAC_{key}(T_B)$ using key. If it is successful the WBAN client authenticates the AP and regards this key as the session key for subsequent secure communication.

IV. SYSTEM IMPLEMENTATION

A. SYSTEM MODULES

- Initialization
- Registration
- Authentication
- Security analysis

B. MODULE DESCRIPTION

1). Initialization

In this phase NM selects the master secret key and computes the master public key as shown in Fig.3. Whenever a new WBAN client or AP enters, it must be initialized with the NM. NM is responsible for generating the keys for both the WBAN client and the APs. It also loads the system parameters to the WBAN clients and the APs.

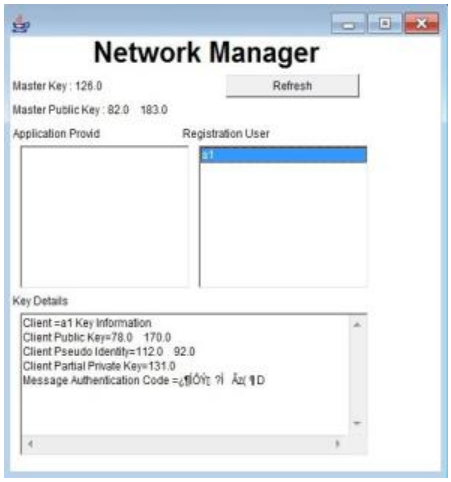

Fig.3 Client's Key Generation by NM

2.) Registration

All the APs must be registered with the NM before they can provide the requested services to the WBAN clients. An AP with the identity ID_{AP} selects its private key and computes the public key. This AP then sends its identity and the public key to the NM. On receiving this NM computes the partial private key and transmits it secretly as shown in Fig.4 and Fig.5. Similarly, all the WBAN clients must be registered with the NM before it accesses the medical services provide by the AP.

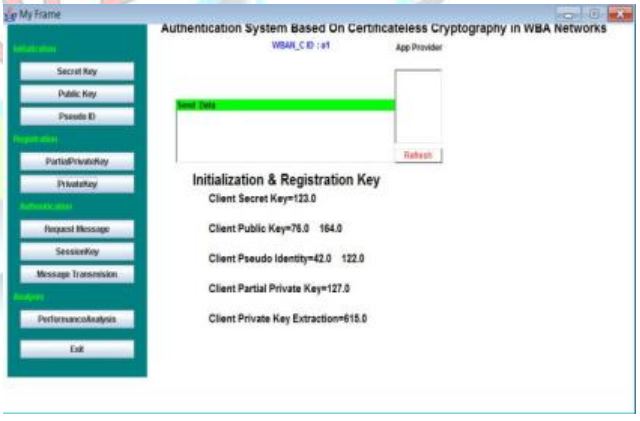

Fig.4 Client's Key Information.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 3, April 2016

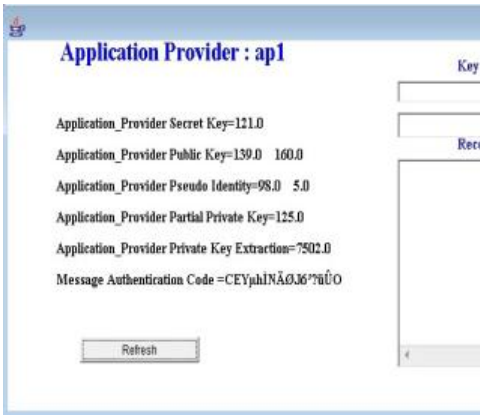

Fig.5 Application Provider's Key Information

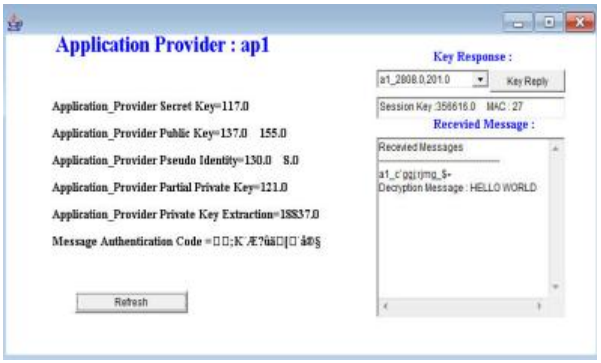

Fig.7 Received Message

3.) Authentication

Both the WBAN client and the AP authenticate each other to avoid potential malicious attacks. Initially the client selects a random ephemeral key and a time t_c. It generates a request message for authentication as shown in Fig.6 and transmits it to the target AP.

On receiving this, the requested AP checks the validity of the time t_c and selects a random ephemeral key. It then computes the key and sends the Message authentication code of the token T_B using key to the WBAN client. The WBAN client then checks the validity of the received MAC using the key computed by it. If it is valid the computed key is accepted as a session key by both the WBAN client and the AP as shown in Fig.7.

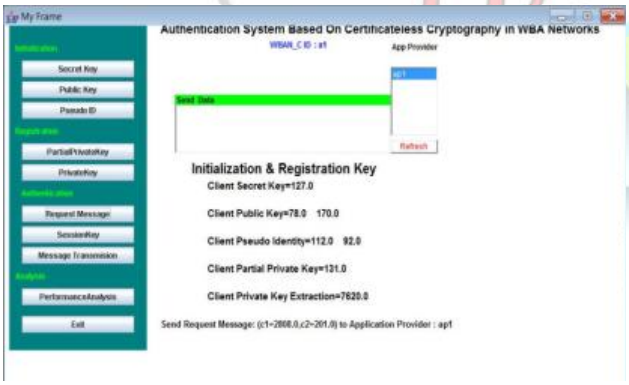

Fig.6 Request Message for Authentication

V. SECURITY ANALYSIS

A. *Forward Security*

The exchanged data in the previous session will still be secure even if the long-term private key of the participant has been corrupted .The proposed protocol offers the property of forward secrecy which assures that even if the complete private key of the client or AP is corrupted the session key established in the previous round will not be disclosed. In the proposed protocol it is obvious that the session key is computed not only using the complete private key but also an ephemeral key which will be selected at random by the client and the AP.

B. Anonymity

The real identity of the requesting client cannot be revealed by anyone. Anonymity means that except for the requesting WBAN client and the requested AP, any outsider (including the NM) is unable to link a particular protocol session to a particular identity.

In the proposed protocol, the anonymity of the requesting WBAN client is achieved by adopting the certificateless encryption. On the one hand, the AP can decrypt the Req = (C_1, C_2) using its full private key and then obtain the pseudo-identity I DC and the public key of the client. However, the real identity pertaining to this pseudo-identity cannot be revealed by the AP.

On the other hand, the pseudo identity of the requesting client is only involved in Req = (C_1, C_2) in our protocol. Any third party who eavesdrops on the communication channel and wants to reveal the real identity of the WBAN client faces the decryption operation.

C. Mutual authentication

It is a security feature in which a client process must prove its identity to a server, and the server must prove its identity to the client, before any

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 3, April 2016

application traffic is sent over the client-to-server connection.

WBAN client and AP should be allowed to authenticate each other to avoid potential malicious attacks. In the proposed protocol both the WBAN client and the AP authenticates each other before a session key is shared between them for secure communication.

D. Key Escrow Resilience

NM cannot impersonate the registered client or AP without being detected. The NM generates only the partial private key of the WBAN client and sends it to it. The client then generates the complete private key using its secret key and the partial private key provided by the NM. So it is impossible for the NM to impersonate the client or the AP.

E. Scalability

The account information of the WBAN client does not need to be distributed to the APs before this client requests the services. Though a group of

public keys and identities of the APs should be preloaded to the client. Thus, the proposed protocol provides better scalability.

F. Session Key Establishment

A session key is a single use symmetric key used for encrypting all messages in one communication session. After the successful authentication between the WBAN client and the APs they share a session key which is generated using their complete private key and the ephemeral key. An efficient bilinear pairing-free certificateless authenticated key agreement protocol is used for session key generation. It requires only 4 scalar multiplications and it has the best performance among the related protocols. It also reduces the computational time of the protocol. Christo Ananth et al. [7] discussed about a method, Wireless sensor networks utilize large numbers of wireless sensor nodes to collect information from their sensing terrain. Wireless sensor nodes are battery-powered devices. Energy saving is always crucial to the lifetime of a wireless sensor network. Recently, many algorithms are proposed to tackle the energy saving problem in wireless sensor networks. There are strong needs to develop wireless sensor networks algorithms with optimization priorities biased to aspects besides energy saving. In this project, a delay-aware data collection network structure for wireless sensor networks is proposed based on Multi hop Cluster Network. The objective of the proposed network structure is to determine delays in the data collection processes. The path with minimized delay through which the data can be transmitted from source to destination is also determined. AODV protocol is used to route the data packets from the source to destination.

Certificateless protocols usually require that the KGC should be unable to compute previously established session keys even if it knows all publicly available information. In certificateless protocols, the KGC that has learned the ephemeral secrets of any session should not be able to compute the session key. The proposed protocol alleviates the key escrow problem in ID-based cryptography and at the same time reduces the cost and simplifies the use of the technology when compared with traditional PKC.

VI. PERFORMANCE EVALUATION

In this section we compare the efficiency of the proposed protocol with the existing protocol. The comparison result is shown below.Fig.8 compares decryption time of the proposed protocol which is very low when compared with the existing protocol.

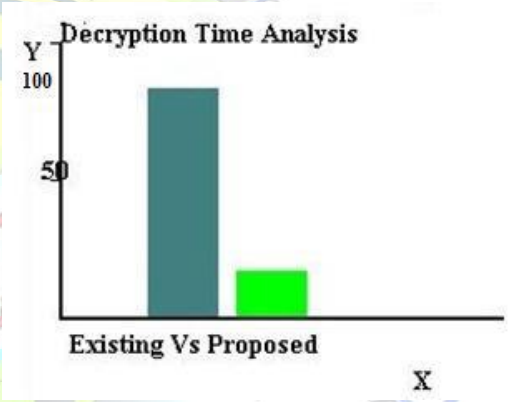

Fig.8 Decryption Time

Figure.9 verifies the integrity of the message by comparing the received message with the send message. Therefore the proposed protocol is assured to offer the property of message integrity.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 3, April 2016

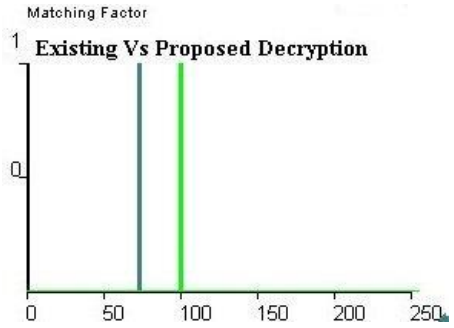

Fig.9 Comparison of Send and Received Messages

The performance comparison between the proposed protocol and the existing protocol in terms of verification time is shown in figure.10. Obviously, it is observed that the proposed protocol takes a much lower time to verify the received messages compared with the existing one. The fact drawn from figure.9 and figure.10 indicates that compared with the most efficient remote anonymous authentication protocol, the reduction in the verification time reaches 16%. Also the proposed protocol requires only 4 ECC based scalar multiplications which reduce the computation time. Therefore the proposed protocol

outperforms the existing scheme in terms of computation time and communication overhead

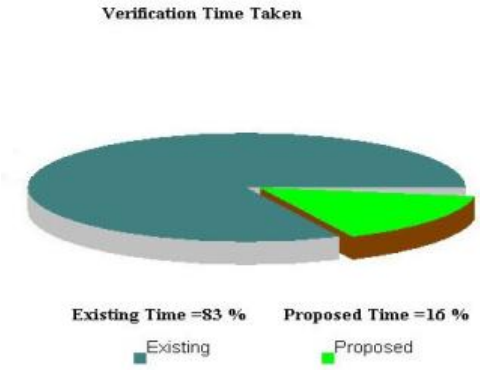

Fig.10 Verification Time Taken

VII. CONCLUSION

The security weaknesses of the existing certificateless anonymous remote authentication protocols for WBANs is analysed and a secure, lightweight, scalable certificateless remote authentication protocol is proposed. The proposed protocol satisfies a set of essential requirements such as forward security and scalability which have not been fulfilled by the existing protocol. By adopting the encryption technique to realize anonymity, it eliminates the delivery of clients' account information to APs, and thus provides better scalability. The significant performance advantages of the proposed protocol over existing protocols have been shown by extensive performance analysis. Due to its lower communication overhead and computation cost, the proposed protocol is more suitable for low-power mobile terminals in WBANs.

REFERENCES

[1] X. Cao, X. Zeng, W. Kou, and L. Hu, "Identity-based anonymous remote authentication for value-added services in mobile networks,"*IEEE Trans.Veh.Technol.*, vol. 58, no. 7, pp. 3508–3517, Sep. 2009.

[2] C. C. Tan, H. Wang, S. Zhong, and Q. Li, "IBE-lite: A lightweight identity-based cryptography for body sensor networks," *IEEE Trans. Inf.Technol. Biomed.*, vol. 13, no.6, pp. 926–932, Nov. 2009.

[3] J. Liu, Z. Zhang, X. Chen, and K. S. Kwak, "Certificateless remote anonymous authentication schemes for wirelessbody area networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 332–342, Feb. 2014.

[4] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," *Proc. 21st Annu. Int. Cryptol. Conf. (CRYPTO)*, 2001, pp. 213–229.

[5] F. Hess, "Efficient identity based signature schemes based on pairings," in *Proc. 9th Annu. Int. Workshop Sel. Areas Cryptogr. (SAC)*, 2002,pp. 310–324.

[6] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Proc. Adv. Cryptol. (ASIACRYPT)*, 2003, pp. 452–473.

[7] Christo Ananth, T.Rashmi Anns, R.K.Shunmuga Priya, K.Mala, "Delay-Aware Data Collection Network Structure For WSN", International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST), Volume 1,Special Issue 2 - November 2015, pp.17-21

[8] A. Cilardo, L. Coppolino, N. Mazzocca, and L. Romano, "Elliptic curve cryptography engineering," *Proc. IEEE*, vol. 94, no. 2, pp. 395–406, Feb. 2006.

[9] Yong-Jin Kim, Yong-Min Kim, Yong-Jin Choe, Hyong-Chol O, "An Efficient Bilinear Pairing-Free Certificateless Two-Party Authenticated Key Agreement Protocol in the eCK model" Journal of Theoretical Physics and Cryptography (IJTPC), Vol. 3 Issue 2322-3138, July – 2013.