iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** X **Month of publication:** October 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 3 Issue X, October 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Enhanced Remote Authentication System Based On Certificateless Cryptography in Wireless Body Area Network

S.Padma[1], D.C.Joy Winnie Wise[2]
[1]M.E student, [2]Professor and Head, Department of CSE
Francis Xavier Engineering College, Tamilnadu, India

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.

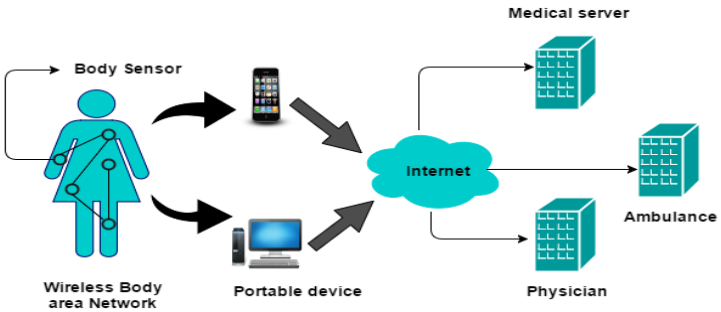


Fig. 1 WBAN Architecture

Volume 3 Issue X, October 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

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 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] [7] 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.

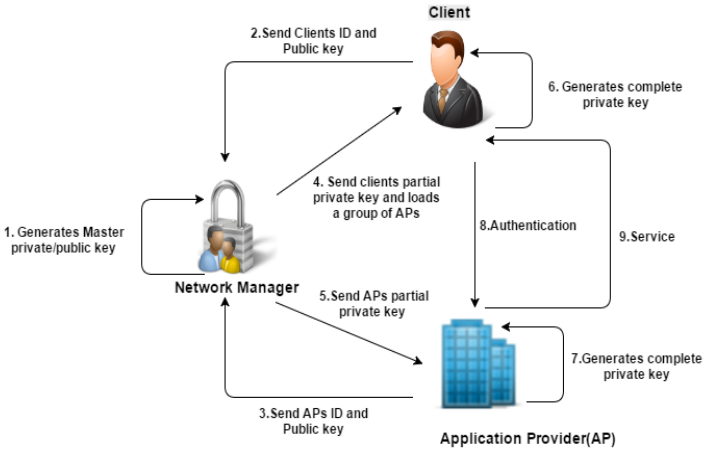


Fig. 2 System design

C. *ProposedPprotocol*

A scalable and anonymous certificateless remote authentication protocol is proposed. 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 $H_1:\{0,1\}^r \rightarrow Z_m^*$, $H_2:\{0,1\}^* x \{0,1\}^* \; x \; G \; x \; G \rightarrow Z_m^*$, $H_3:\{0,1\}^* x \{0,1\}^* \; x \; G \; x \; G \; x \; G \rightarrow Z_m^*$, $H_4:\{0,1\}^* x \{0,1\}^* \; x \; G \; x \; G \; xG \quad x \; G \rightarrow Z_m^*$

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

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. SECURITY ANALYSIS

A. Forward Security

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 proposed protocol achieves the anonymity of the client by adopting the method of certificateless encryption. The pseudo-identity of the requesting client is only involved in the request message for authentication so anyone who attempts to eavesdrop the real identity of the WBAN client needs to face the decryption operation.

Volume 3 Issue X, October 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

C. Mutual Authentication

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

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. Session Key Establishment

After the successful authentication between the WBAN client and the APs they share a session key for secure transmission of messages, which is generated using their complete private key and the ephemeral key.

V. PERFORMANCE EVALUATION

Advanced Pairing-Free Certificateless Two-Party Authenticated Key Agreement protocol [9] is used for generating the session keys which is being used for secure communication. It reduces the computational time and also increases the performance of the designed system. The protocol used for session key generation in the existing scheme requires nine elliptic curve scale multiplications. But the proposed protocol is designed to compute only four scalar multiplications which is computationally efficient.Fig.2 and Fig.3 shows that the proposed protocol outperforms the existing protocols in terms of computational time.

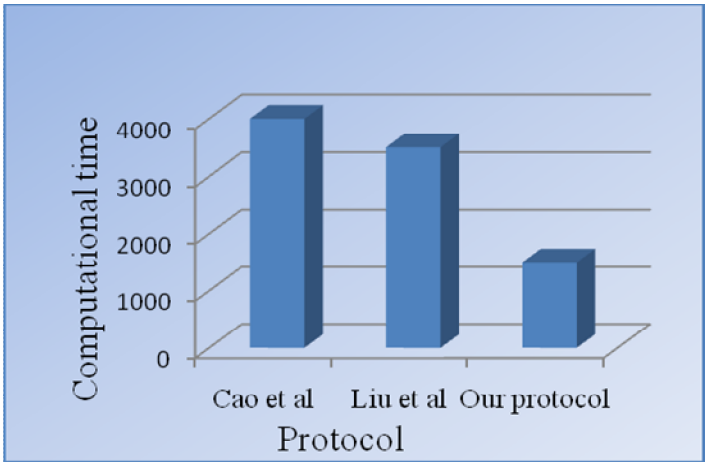


Fig. 3 Computational time for WBAN Clients

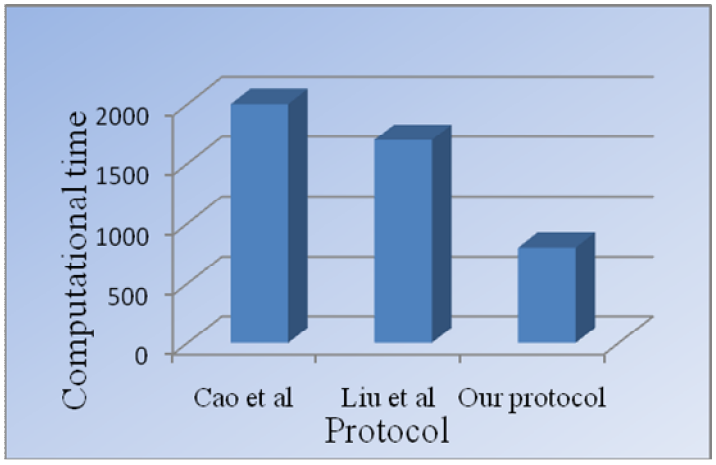


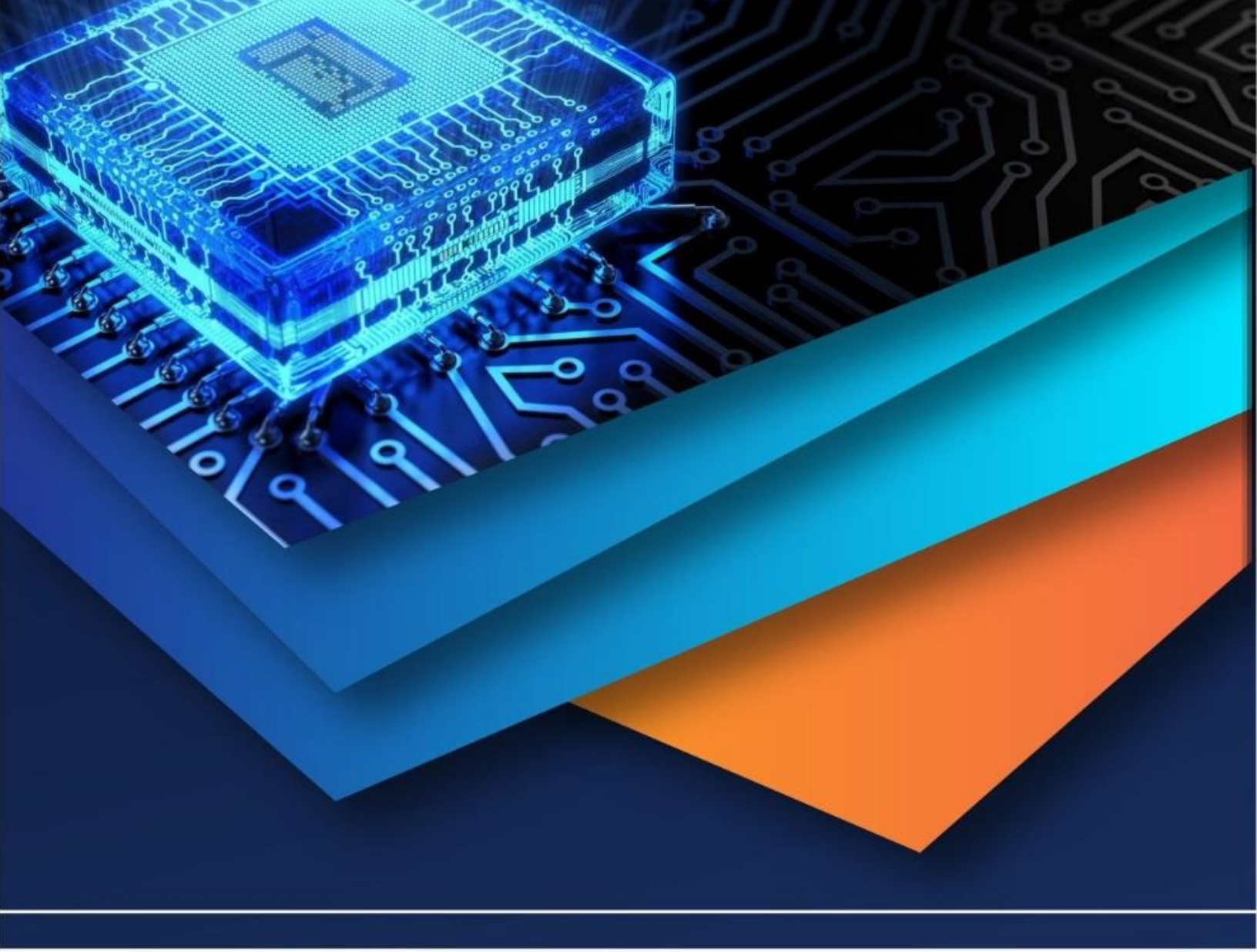
Fig. 4 Computational time for Application Providers

VI. CONCLUSION

This paper discusses about the security weakness of the existing remote anonymous authentication protocol and proposes an enhanced certificateless remote authentication protocol that achieves forward security and scalability. The computational cost of a pairing is much higher than the elliptic curve scalar multiplications. Therefore the proposed protocol uses a pairing free method for session key generation which improves the performance of the designed protocol. Thus the proposed protocol outperforms the existing schemes in terms of computational cost and efficiency.

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. 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] Z. Zhang, D. S. Wong, J. Xu, and D. Feng, "Certificateless public-key signature: Security model and efficient construction," in Proc. 4th Int. Conf. Appl. Cryptogr. Netw. Security (ACNS), 2006, pp. 293–308.
[8] 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.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY