International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 03 | Mar-2016 www.irjet.net p-ISSN: 2395-0072

Ensuring Authenticity and Revocability for Wireless Body Area Network using Certificateless Cryptography

Ms. S.Padma [1], Dr.D.C.Joy Winnie Wise [2], Mr. S. Malaiarasan[3] , Ms. N. Rajapriya[4]

[1]PG Student, Dept. of CSE, Francis Xavier Engineering College, Tamil Nadu.
[2] Dr.D.C.Joy Winnie Wise, Professor&Head, Dept. of CSE, Francis Xavier Engineering College, Tamil Nadu.
[3] Mr. S. Malaiarasan, Assistant Professor, Dept. of CSE, Francis Xavier Engineering College, Tamil Nadu.
[4]Ms. N. Rajapriya, Assistant Professor, Dept. of CSE, Francis Xavier Engineering College, Tamil Nadu.

Abstract - *Recently, with the technical advancements in wearable medical sensors and wireless communication techniques, Wireless Body Area Network (WBAN) has emerged as a new technology for e-health care service. The wearable medical device (WMD) aims at collecting an individual's medical data unobtrusively and ubiquitously. The security of the data collected from a WBAN remains a major unsolved concern. So, a certificateless remote anonymous authentication protocol is used to overcome the above challenges and to prevent the leakage of user's private information from unauthorized users. It eliminates the need for distributing clients account information to the application providers and also it achieves forward security. However the revocation functionality of anonymous remote authentication for the WBANs has not been considered in case the private key of the user has been leaked or the misbehaviour of the user has been detected. To address the demand a certificateless remote authentication protocol with efficient revocation is proposed. KUNodes algorithm is used to achieve the efficient revocation function. The revocation mechanism is highly scalable and it is especially suitable for the large-scale WBANs. The proposed authentication protocol is computationally efficient and it is provably secure against existential forgery compared with the existing one. Several key applications ranging from remote health monitoring to military/fitness training can be enabled by remote authentication in WBANs.*

Key Words: **Certificateless, Revocation, Remote health monitoring, Sensors, Session key establishment.**

1. INTRODUCTION

Wireless Body Area Network (WBAN) has emerged as one of the latest technologies for mobile health monitoring. With WBANs, patients' health-related parameters can be monitored remotely, continuously using the wearable sensors attached to the human body using the wireless communication channels. The data collected from the sensors is then processed and delivered to a medical server or an application provider (AP) using a portable personal device (PPD).The efficient communication between these devices is achieved by adapting the techniques in wireless sensor networks. Several applications including remote health monitoring can be enabled using the two basic modes of communication namely the intra-body (between the WBAN sensors and the PPD) and the extra-body communication (between the PPD and the APs) as shown in Fig.1. Possible applications of WBAN include monitoring the soldiers in defence services, monitoring the sports person by sensing the heart rate and providing assistance to disabled person.

The patient related data stored in the WBAN plays a major role in medical diagnosis, so it is desirable to secure the data stored in the application provider or the medical database. The security solutions used for WSN are not applicable to BAN because of various resource constraints like energy, memory etc. Stringent security mechanisms are required in order to ensure the strictly private and confidential character of the medical data. So a certificateless remote anonymous authentication protocol with efficient user revocation is proposed to address the challenges. The proposed system mainly focuses on efficient user revocation against short term key exposure. The revocation method used for Identity-based encryption is applicable to revoke the users. Revocation of inside user (WBAN client or AP) takes place in case the private key of the user has been compromised or the misbehaviour of the user has been detected.

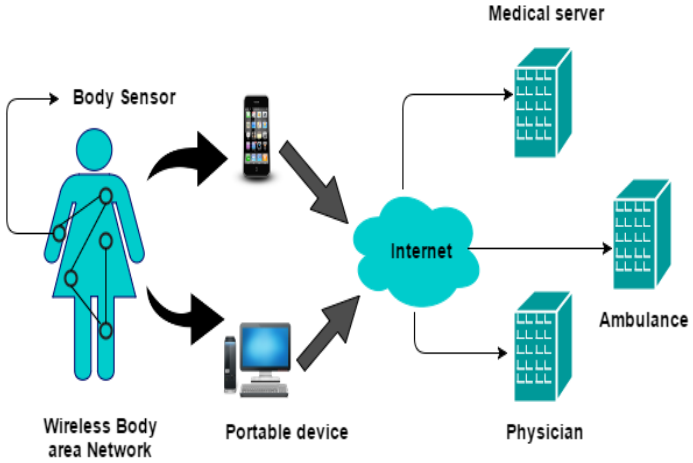

Fig -1: Architecture of WBAN

2. RELATED WORKS

Identity-based remote authentication protocol [1] [2] has been proposed to overcome the drawbacks caused by the public key certificates. It eliminates the need for certificates but the dependence on a private key generator (PKG) to generate the private keys of the user inevitably introduces a problem of key escrow resilience. To address the key escrow problem, 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].In a certificateless remote authentication protocol the complete private key of the user consists of the partial private key generated by the key generating centre and the user secret key. Since the user secret key cannot be accessed by the key generating centre it resolves the key escrow resilience.

Even though the certificateless signature scheme is computationally efficient and secure against existential forgery the anonymous 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. However the revocation of the user in the existing protocol still remains a non-trivial problem. The existing solutions are not practical for use due to enormous computation. This paper enhances the certificateless remote authentication protocol [9] by incorporating the revocation functionality. In the proposed scheme elliptic curve cryptography [8] is used for generating the keys for the WBAN clients and the APs and KUNode algorithm is used to achieve efficient revocation.

3. DESIGN OBJECTIVES

The proposed authentication protocol satisfies the following design objectives.

- **Mutual authentication:** WBAN clients and the application providers authenticate each other to verify their identities and to avoid potential malicious attacks.
- **Forward Security:** The information transmitted using the previous session key will still remain secure even if the complete private key of the user has been corrupted.
- **Key escrow resilience:** The Network manager which acts as the key generating center cannot impersonate the legitimate users without being observed.
- **Revocation:** It is necessary to revoke the user in case if the expired client to enjoy the services offered by the APs free of charge or if the secret key of a WBAN client or an AP has been exposed.
- **Anonymity***:* Any outsider except for the requesting client and the application provider is unable to link a particular protocol session to a particular identity. Further, the real identity of the requesting client cannot be revealed by anyone other than the requested AP.
- **Session Key establishment:** A session key is established between the WBAN clients and the application providers to secure their subsequent communication due to the sensitive nature of the data.

4. SYSTEM DESIGN

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

- **Network Manager (NM):**

It acts as a key generating center and is responsible for the enrollment 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. It is very likely for the NM to impersonate the WBAN client or an AP. Therefore, it is desirable to avoid the key escrow problem.

- **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. For security purpose WBAN client must be revoked in case the NM detects the misbehavior of the user or if the user declares that its private key is compromised.

- **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.

The proposed scheme uses the revocation approach adapted for the Identity-based encryption. Specifically, the user's private key is made up of three parts: an initial partial private key, a time refresh key and the user secret key.

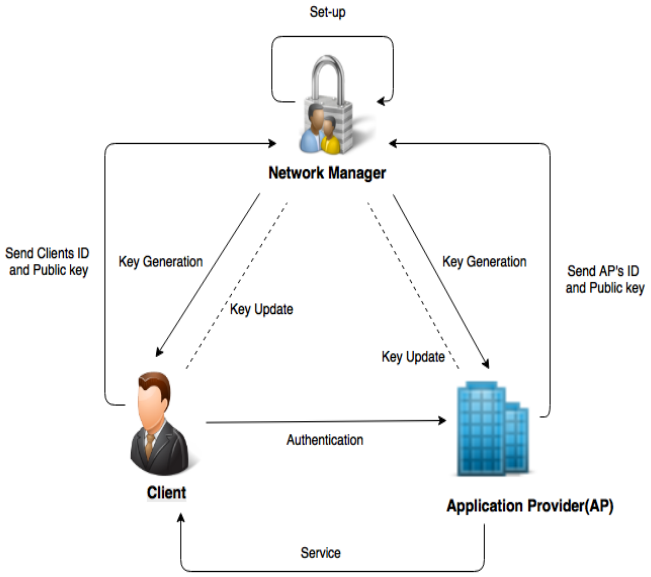

Fig -2: System Design

The initial partial private key is preloaded to the user during the registration phase and it remains constant, whereas the time refresh key will be updated in every time period and it is transmitted over a public channel. The user cannot generate the partial private key if he/she is unable to get the new time refresh key. To revoke the user the network manager just stops issuing the time refresh key. The proposed scheme incorporates the idea of certificateless encryption scheme and a certificateless signature scheme with efficient revocation against short-term key exposure.KUNode algorithm is used to achieve efficient revocation.

KUNode Algorithm:

KUnode(BT,RL,T):
X,Y←ϕ;

∀(η_i,T)ϵ RL
if $T_i \leq T$ then add Path(η_i) to X
end if

∀xϵ X
if $x_L \notin X$ then add x_L to Y
end if
if $x_R \notin X$ then add x_R to Y
end if

if Y= ϕ then add root to Y
end if
return Y

5. PROPOSED PROTOCOL

The proposed protocol consists of 5 phases: Initialization, key generation, key update, Authentication and Revocation.

5.1 Initialization:

- NM selects the master secret key s, revocation list RL and a binary tree BT.
- Select a random generator, g ϵ_R G.
- Compute $g_1=g^x$ and select a random element g_2 ϵ_R G.
- Select three hash functions $H_1, H_2, H_3, H_4, H_5, H_6$ such that H_1: $ID \rightarrow G$; H_2: $T \rightarrow G$; H_3: G_T x G→M ;H_4 : M x ID x G x $T \rightarrow G$;H_5 : {0,1}* x G x ID x $G^4 \rightarrow Z_p^*$ where ID,T and M denotes the identity space, time space and message space respectively.
- Initially the revocation list RL=ϕ and state st=Binary tree with N leaves.
- NM then publishes the params {F_p , E/F_p , g, g_1, g_2, P,H_1…H_6,$MAC_{(.)}$(.)} as system parameters and loads them into WBAN clients and the APs.

5.2 Key generation:

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

- An application provider with the identity ID selects the secret value x_{ID} ϵ_R Z^*_p as its user secret key usk_{ID}.
- Compute its public key using the user secret key, $upk_{ID}=g \wedge x_{ID}$.
- AP then sends its ID and the public key to NM.
- On receiving the identity ID, NM checks whether the ID is in the revocation list RL
- If the ID exists in the RL the NM aborts the algorithm.
- Otherwise it initializes the node for the corresponding ID if it has not been initialized yet.

Node Initialization:

- NM stores the received identity ID in the leaf node
- The leaf node is chosen randomly from the binary tree .
- For each node θ ϵ Path(η_i), NM selects $s_{\theta 1}^{ID}$ ϵ_R Z^*_p and stores ($s_{\theta 1}^{ID}$, $s_{\theta 2}^{ID}$) in the node θ that satisfies $s_{\theta 1}^{ID} + s_{\theta 2}^{ID} = s \bmod p$.

- If the node is already initialized, NM retrieves $s_{\theta 1}^{ID}$ from this node and Selects q_θ^{ID} ϵ Z^*_p
- Computes ($m_{\theta 1}^{ID}$, $m_{\theta 2}^{ID}$) =($g_2 \wedge s_{\theta 1}^{ID}.H_1(ID)) \wedge q_\theta^{ID}$, $g \wedge q_\theta^{ID}$).
- It then returns the initial partial private key $psk_{ID=}$ $\{(m_{\theta 1}^{ID}, m_{\theta 2}^{ID})\}_{\theta \epsilon Path(\eta i)}$ to the corresponding user.

Similarly, a WBAN client with the identity ID_C is provided with the initial partial private key, user secret key and the user public key before it access .

5.3 Key Update:

For each node θ Є KUnode(BT,RL,T) NM generates the time refresh key and broadcast it to the corresponding user using the following steps.

- NM retrieves $s_{\theta 2}^{ID}$ from the node θ and selects $r_\theta^{ID} \in_R Z^*_p$.
- Computes the time refresh key $(u_{\theta 1}^{ID}, u_{\theta 2}^{ID})=(g_2 \hat{} s_{\theta 2}^{ID} .H_2(T))\hat{} r_\theta^{ID}, g\hat{} r_\theta^{ID})$ and sends it to the corresponding user.

On receiving the time refresh key, AP with an identity ID_{AP} computes the partial private key as follows:

- Choose θ Є KUnode(BT,RL,T) if KUnode(BT,RL,T)∩Path(η_{ID})= ϕ
- Select $r_{ID}, s_{ID} \in_R Z^*_p$
- Compute the partial private key $psk_{ID,T}=(psk^1_{ID,T}, psk^2_{ID,T}, psk^3_{ID,T})=(m_{\theta 1}^{ID}. u_{\theta 1}^{ID}. (H_1(ID))\hat{} r^{ID}. H_2(T))\hat{} s^{ID}, m_{\theta 2}^{ID}. g\hat{} r^{ID}, u_{\theta 2}^{ID}. g\hat{} s^{ID})$
- Using the partial private key and the time refresh key the complete private key of the AP is generated.
- Similar steps are carried out for the WBAN client.

5.4 Authentication:

WBAN client and the requested AP performs mutual authentication.

- Select an ephemeral key at random $t \in_R Z_p^*$.
- Compute the token $T_A= g^t$ and select the time t_c
- Select $s,t \in_R Z^*_p$ and compute $\sigma =(\sigma_1, \sigma_2, \sigma_3)= (psk^1_{ID(c),T} . (H_1(ID_{(C)}))^s. (H_2(T))^t. (H_4(T_A||ID_C|| T||upk_{IDC}))\hat{} usk_{IDC}, psk^2_{ID(c),T}.g^s, psk^3_{ID(c),T}.g^t)$.
- Compute $r= H_5(T_A ||ID_C||\sigma||upk_{IDC}||t_c)$
- Compute $l=\hat{e}(g_1,g_2)^r$, $p=upk_{ID(AP)}\hat{}r$
- Compute $C_0=H_3(l,p)$ XOR $H_5(T_A ||ID_C||\sigma||upk_{IDC}||t_c)$, $C_1=g^r, C_2=H_1(ID_{AP})^r, C_3=H_2(T)^r$
- Send the request message $Req=(C_0, C_1, C_2, C_3)$ to the AP.

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

- Compute $l= \hat{e}(C_1, psk^1_{ID(AP),T}) / \hat{e}(C_2, psk^2_{ID(AP),T}). \hat{e}(C_3, psk^3_{ID(AP),T})$, $p=C_1\hat{}usk_{ID(AP)}$
- $T_A ||ID_C||\sigma||upk_{IDC}||t_c = H_3(l,p)$ XOR C_0 . Reject this session if time 't'is invalid.
- Compute $r= H_5(T_A ||ID_C||\sigma||upk_{IDC}||t_c)$
- Select an ephemeral key at random $w \in_R Z_p^*$ and compute the token $T_B= g^w$
- Compute $key=H_4(ID_{AP}, ID_C, T_A, T_B, upk_{ID(AP)}, upk_{ID(C)}, T_A^w)$
- 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 $key=H_4(ID_{AP}, ID_C, T_A, T_B, upk_{ID(AP)}, upk_{ID(C)}, T_B^t)$
- 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.

5.5 Revocation:

If the private key of the user has been compromised or if the attacker has been detected the leaf node associated with the identity along with the revocation time will be returned to the NM. NM then updates the revocation list.

6. SECURITY ANALYSIS

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.

The anonymity of the client is achieved by adopting the method of certificateless encryption. So anyone who attempts to eavesdrop the real identity of the WBAN client needs to face the decryption operation. 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.

7. CONCLUSION

This paper discusses about the security weakness of the existing remote anonymous authentication protocol and proposes an enhanced certificateless remote authentication protocol featured with efficient revocation and short-term key exposure resistance. 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. Furthermore, the security properties of the proposed protocol have been proved in the random oracle model.

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] 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] 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] H. Xiong, "Cost-effective scalable and anonymous certificateless remote authentication protocol," *IEEE Trans. Inf. Forensics Security*, vol. 9,no. 12, pp. 2327–2339, Dec. 2014.