International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 02 Issue: 03 | June-2015 www.irjet.net p-ISSN: 2395-0072

Ensuring Certificateless Remote Anonymity and Authenticity wireless Body Area Network

[1]Basavashri B, [2]Manjula M
[1]M.Tech (CSE) Student, VTU, Atria Institute of Technology, India
[2]Assistant Professor, Dept. of CSE, VTU, Atria Institute of Technology, India

---

Abstract:*Wireless technology has advanced to be become a vital part of our lives starting from mobile communication to health care departments. Wireless body area network is one of the wireless sensor technologies for the health care service. the leakage of privacy is one of the main issue in WBAN especially to those unauthenticated or even malicious adversaries.in order to provide the security to theWBAN users in this paper we are developing a new certificateless remote anonymous authentication protocol to give the strength to remote WBAN users to anonymously enjoy the health care service. Our authentication protocol also demonstrated that they outperform the existing schemes in terms of better trade-off between desirable security properties andcomputational overhead, nicely meeting the needs of WBANs.*

Keywords: Anonymous authentication, certificate less signature, wireless body area network, healthcare

INTRODUCTION:

Wireless Body Area Network (WBAN) based on a low cost wireless sensor network technology could greatly benefit patient monitoring systems in hospitals, residential and work environments.WBAN could be seen as a special purpose wireless sensor network with a number of additional system design requirements. The new standard will define the PHY (Physical) and MAC (Medium Access Control) layer management issues which could be used to develop a low cost, ultra-lowpower and highly reliable wireless network. These functionalities are controlled primarily by PHY and MAC layers in conjunction with the application layers. Existing WBAN standard islikely to be based on the IEEE 802.15.4 MAC layer and a new PHY layer. Use of aWBAN will also allow the flexibility of setting up a remote monitoring system via either the internet or an intranet. For such medical systems it is very important that a WBAN cancollect and transmit data reliably, and in a timely manner to the monitoring entity. In the existing application of WBAN leakage of privacy is one of the most important concerns of potential users. This issue is especially challenging in WBAN due to its unique characteristics such as open medium channel, signal noise, mobile terminals, flexible infrastructure, and so on. By carefully examining intrinsic characteristics of WBAN and also considering the existing remote user authentication here we present two novel certificateless remote anonymous authentication protocols. For example in a remote health care application authorized patients should anonymously access and sharemedical services, and the doctors only need to know the bio-information of the patient, whereas all the rest private information such as name and id number must be kept unknown.

Our proposed work:

By examining the characteristics of WBAN and considering the existing remote authentication schemes here we develop a new certificate less signature (CLS) scheme which is cost effective, efficient and secure. This CLS scheme then serves as a design basis for two remote anonymous authentication protocols. Here the protocol use anonymous account index instead of WBAN clients real identity to access WBAN service.

Figure1 shows the system architecture of WBAN in order to get a treatment from the physicians, emergency ceneter,primary care provider initially WBAN client has to attach the sensors to their body the information that is collected in the sensors is transferred the computer, mobile phones or pda the collected information is thentransferred to the phisycians,tele medicine services.in order to provide the secure communication between the client and the physicians here we are proposing two remote anonymous authentication protocol. Initially the WBAN client has to send the registration request to the network manager (Step 1).Network manager reply's to client by giving a ticket to get the treatment from the application provider (step 2).once the client gets the permission from network manager then he will authenticate with application provider(step 3)here the application providers are the physicians, emergencycentres. If the authentication request received by the client is valid then application provider reply's to client whether the authentication is successful or not to (step 4).If authentication is successful then the client gets the particular treatment from the applicationprovider.

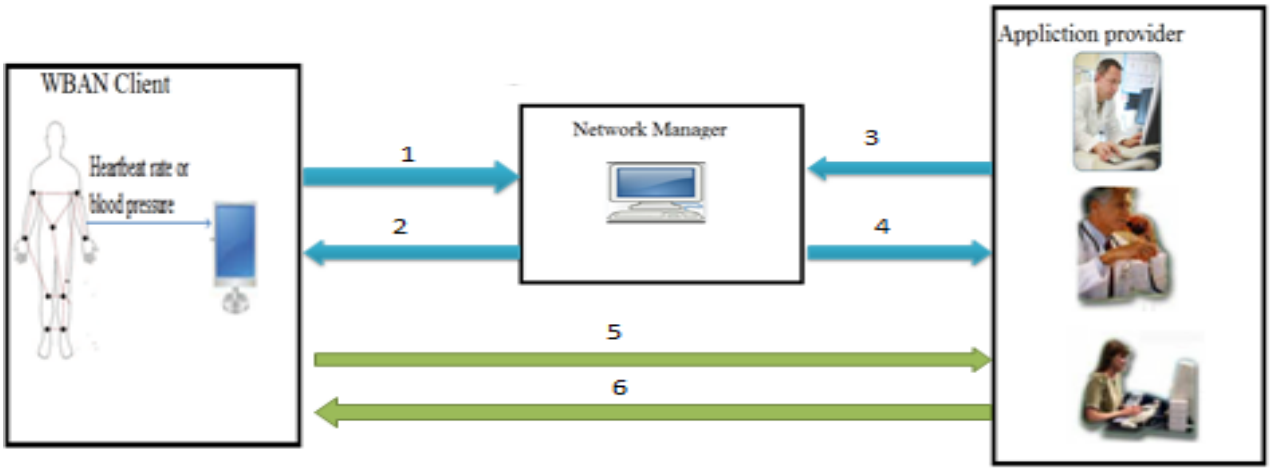

Fig1: System architecture of WBAN

CERTIFICATELESSIGNATURE SCHEME:

In order to provide the security for wireless body area network we use our new certificateless signature scheme to design a remote anonymous authentication protocol. The authentication protocol preserves the anonymity for WBAN client.

A certicate less signature scheme consists of six algorithms:

Setup:

This algorithm is done by network manager so he will acts as a private key generator (PKG).

- G1 and G2 be a pairing operator
- Let l be a security parameter.
- PKG picks a random integer $S_{PKG} \epsilon Z_q^*$ as its private key
- hen he computes $Q_{PKG}=S_{PKG}P$ as its public key
- Then he publishes system parameter where S_{PKG} is kept secret.

Set partial private key:

Here the signer is client he selects a random integer $s1 \epsilon z_q$ as his partial secret key

Set partial public key:

Here the client computes $Q_1=s_1P$ has its partial public key.

Partial private key extract:

- This algorithm is performed by network manager. When a client request the secret key to his identity (ID) network manager computes the other secret key to client. Where ID is the other partial public key of the client.
- Secret key of the identity is given as $S2=S_{PKG}$ Q2 where Q2=H (ID,Q1).Both secret key and public key is given to the signer in a secret channel.
- For a signer <ID, Q1> is public key and <S1, S2> is private key

CL-SIGN:

- To sign message the signer chooses random integer $k \in Z_q$ and computes as:
- $r=e(Q_2, Q_{PKG})^K$
- v=h (mIIr,p)
- $U=KS_2- vs_1Q2$
- The pair (v, U)$\epsilon(Z_Q^*,G1)$ is considered as signature

CL-VERIFY:

This algorithm is computed by the application provider and he will acts as a verifier.

T

On receiving the message m and signature <v,U> the verifier computes:

- Q2=H (ID, Q1)
- Accepts the signature if and only if:
- V=h (m I I r, p)

AUTHENTICATION PROTOCOLS FOR WIRELESS BODY AREA NETWORK:

Preliminary version authentication protocol:

The protocol takes a new certicate less signature scheme as a design basis .Network manager initially generates an account index for each requesting WBAN client and uses it for signature generation and verification. If client wants to login he needs to send the signature of the message issued by the network manager along with the account index to the corresponding application provider. Application provider then verifies the client's signature using the account index and the Networkmanager (NM) signature by NM public key. It is obviousthat the role of AP is only to verify the generated

signature, and the information in hand does not allow it to recover thereal identity of the client. Our protocol can be described as:

Initialization Phase:

This is the initial step in the preliminary version authentication protocol takes place by network manager which generates key and establishes the systemparameter. By considering the security parameter l NM determines its public, private pair(Q_{NM},S_{NM}).Where Q_{NM}=S_{NM} P and gives the system parameter as <I, G1,G2, q, P, e,H, h,Q_{NM}> as defined in the certificate less signature algorithm. Application provider also as a key pair as<Q_{AP},S_{AP}>where Q_{AP}=S_{AP}P.

Registration phase:

This step is performed by the WBAN client with network manager to access an applicationprovider. The following step should be performed in the registration phase. In this step WBAN client chooses his own partial private key while obtain another partial private key using an algorithm partial-private-key-extract. Network manager then issues a ticket=<m,σ> to client where m=rightIIindc$_v$andσ is the corresponding signature on m.in the same way the WBAN client store a group of Q_{AP} for different application provider. Two predetermined functions h(.) and message authentication code are loaded simultaneously for access.

Authentication phase:

The WBAN client performs the following steps to anonymously authenticate by himself to the application provider.

- Selects a random K, t Є Z_q^* and compute T=tP andT'= tQ_{AP}
- Pick up the current time t_c of the requesting WBAN terminal.
- then calculates v=h(σ||tc||r,T)
- Computes U=KS_2-vs_1Q2.
- Computes the session key=h (v,T).
- Send the request message as(v, U, m, σ, t_c, T')
- When the AP receives Req(v, U, m, σ,t_c, T') it Checks the validity of <M, σ> and t_c.
- Then AP rejectsthe request if m and t_c are not valid. Otherwise,the AP does the following:
- Verifies v=h(σIItc||r,T)
- Computes the session key=h(v,T)
- Compute MAC_{key}(V) as the reply. On receiving the reply from application providerWBAN client checks the integrity of MAC_{key}(V) with session key.WBAN client quitsthe currentsession if it produces negative result otherwise WBAN client authenticates with the application provider.

Security enhanced authentication protocol:

In the preliminary version, all the requested authentication information, including the account index and the corresponding right of the client, is carried in the request message. This may allow one sophisticated adversary to determine whether two different sessions are initiated by the same client, and may also allow NM to trace the client's real identity from the session information.to avoid this here we are proposing security enhancedauthentication protocol. This protocol also consists of three phases like initialization, registration, and authentication phase.

Initializationphase:

Initialization phase is same as like preliminary version authentication protocol.

Registration phase:

This process is as the same as preliminaryversion but NM issues <I, indc$_v$, right> to AP, where I =indc$_v$P, instead of sending aticket <m, σ> to client

Authentication phase:

The WBAN client performs thefollowing steps to anonymously authenticate him/herself to the requested AP

- Select at random k,t $\in Zq^*$ and computes T= t p,T'=tQ_{AP} and I'=I+T
- Pick up the current time t_c of the WBAN client and computes v=h(t_c||r,T)
- ComputesU=KS_2-vs1Q_2
- Computes the session key=h(v,T)
- Send a service request message Req = (v, U, t_c, T', I ')

When the application provider receives the request it checks the current time of the requesting WBAN client and also computes the session key. If the current time tc of the requesting WBAN terminal is valid then AP accepts the request or else rejects the request. Then application provider computes MAC_{key}(V) as the reply to respective WBAN client. When WBAN client receives the reply message from the application provider it checks the integrity of MAC_{key}(V) with session key if the integrity is not valid then WBAN client will not authenticate to the respective AP or else it authenticates with AP.

Conclusion: In this paper we developed a new certificate less remote anonymous authentication protocol for wireless body area network. The authentication protocol gives the full security to WBAN users when they access network medical service through WBAN terminal. in order to develop the protocol we use novel certificate less signature scheme as a cryptographic primitive.We formally proved that our certificate less signature scheme has a potential to achieve more desirable security properties with less computational cost than the existing schemes. The advantage of our designed protocol is anonymity here either the client or the application provider do not have to reveal their true identity of user even given all the session information.

Results:

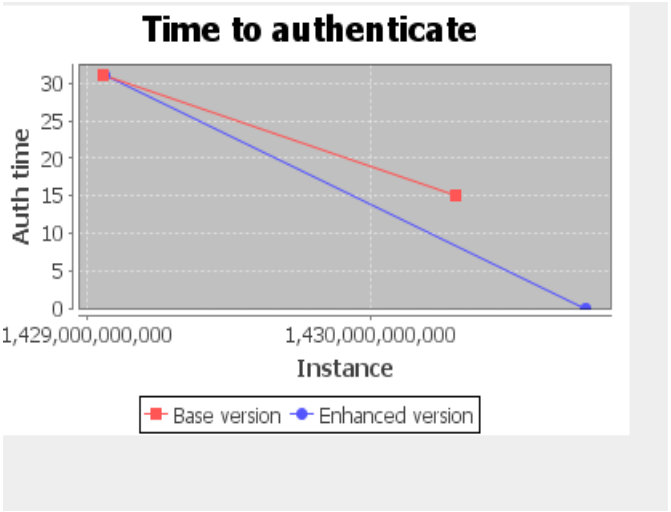

Fig 2: Application provider

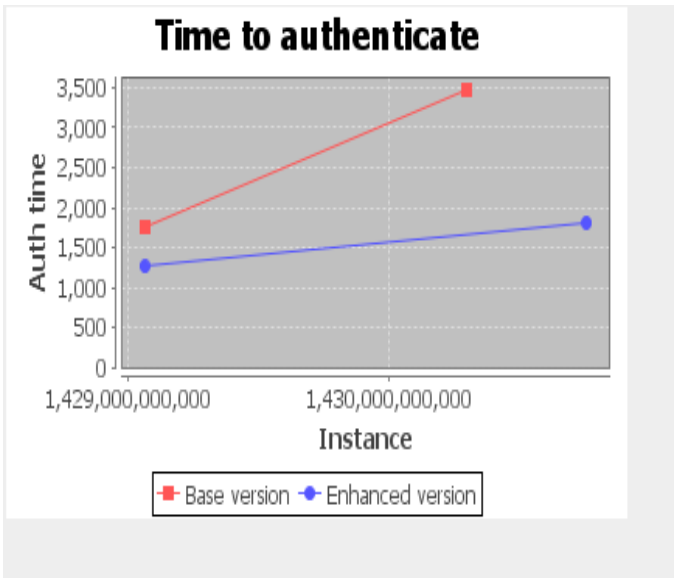

Fig 3: WBAN client

REFERENCES:

[1] Performances Enhancement in Wireless Body Area Network (WBAN) by International Journal of Engineering and Innovative Technology (IJEIT) Volume 3, Issue 2, August 2013.

[2] A Comprehensive Survey of MAC Protocols for Wireless Body Area Networks by A. Rahim, N. Javaid, M. Aslam, Z. Rah man, U. Qasim, Z. A. Khan

[3] M. Chen et al., "Body Area Networks: A Survey," Mobile Networks and Applications, vol. 16, pp. 171-193, 2011

[4]P. Abichar, A. Mhamed, and B. Elhassan, "A Fast and Secure Elliptic Curve Based Authenticated Key Agreement Protocol for Low Power Mobile Communications," Proc. Int'l Conf. Next Generation Mobile Applications, Servicespp235-240, 2007

