A Certificate Less Encryption and Signature Scheme with Efficient Revocation for Securing Inter-Body Wireless Sensor Network

Narayana K R
M. Tech Student
Department of Computer Science & Engineering
MVJ College of Engineering Bangalore, India

Ms. Sanchari Saha
Assistant Professor
Department of Computer Science & Engineering
MVJ College of Engineering Bangalore, India

Abstract

the rapid increase in healthcare demand has seen novel developments in health monitoring technologies, such as the body area networks (BAN) paradigm. In wireless body area network is a wireless network inside the body there are some devices are embedded, may be on the surface mounted on the body in a fixed position. The wireless body area network has two types of communication- Intra-body communication and Inter-body communication. To ensure the security and privacy of the patient’s health status in the wireless body area networks (WBAN’s), it is difficult to provide security for Inter-body communication between the smart portable devices (SPD) held by WBAN client and the application provider such as hospital, physician or medical staff. In this project, to ensure security for Inter-body communication, a remote authentication protocol with some features like non-repudiation, client anonymity, key escrow resistance and revocability in WBAN’s is proposed. Firstly, there is a certificate less encryption scheme and a certificate less signature scheme with efficient revocation against short-term key exposure. Secondly we have certificate less anonymous remote authentication with revocation will be constructed by incorporating the proposed encryption scheme and signature scheme. This mechanism is highly scalable and suitable for large scale WBAN’s.

Keywords: Anonymity, remote authentication, revocation, certificate less cryptography, wireless body area network

I. INTRODUCTION

The global current paradigm in healthcare is the notion of continuous remote patient monitoring using a network of wireless sensors. These healthcare sensor network systems consisting of body area networks (BAN) and infrastructure area networks, avoid the need for a manual self-administered health system and may enable users to take control of their health disorders in the future. BAN technology envisions miniaturized sensors worn or implanted on the body, continuously monitoring health parameters and acting to prevent the onset of critical health events. For example, diabetics now have access to an automatic insulin pump which monitors glucose levels and administers insulin when glucose levels are high. Similar technologies will one day result in devices which can minimize incidences of heart attack or stroke. They could prevent frequent hospital visits and save costs for both the individual patient and a nation’s healthcare system. According to a recent report from Parks Associates, the U.S. market for wireless home-based healthcare applications and services will expand with an annual growth rate of over 180% and become a $4.4 billion industry in 2013 . Statistics such as these indicate a rising demand for portable health monitoring devices e.g., BANs, which are currently undergoing tremendous research and development. At the heart of BAN technology is the need for short range data communications, both from sensors to a decision maker (usually a hub node) or from the hub node to an actuator e.g. insulin delivery system [3].

Wireless data communications based on radio frequency (RF) have been successfully developed using popular protocols such as Bluetooth, Zigbee, and ANT [4]. A major drawback of wireless RF propagation for miniaturized medical portable monitoring devices is the high power consumption which limits the practical duration of operation. Most current research claim that Zigbee and ANT have a battery life of three years, but this is at a low operating data rate e.g. 1 byte transmitted per 5 minutes [4]. The IEEE 802.15.4 standard for low power Zigbee protocol indicates a transmission power output of 0 dBm (1 mW). Continuous operation at the maximum data rate of 250 kb/s generally consumes a normal Lithium ion battery in a matter of hours. It is evident that new approaches to ultra-low power wireless technology are required for improving next generation BAN technology.

Intra-body communications and extra-body communications are two basic communication modes in WBANs, which respectively allow sensors to communicate with each other and the SPD, and enable SPD to communicate with the remote application providers (APs) such as the hospital, physician or medical staff. Possible applications of WBANs range from long-term daily living monitoring to location tracking and medical status monitoring [1]. A scenario of WBANs is shown in Fig. 1.
Fig. 1: A typical wireless body area networks.

Despite of the potential benefits, it is desirable and more prudent to secure WBANs due to the sensitive nature of the medical data collected by WBANs, open medium of the communication channel and the ad hoc nature of the WBANs [8], [9]. Taking the extra-body communication in WBANs as an example, there are several security goals a practical communication protocol must achieve, including:

Anonymity: The adversary may establish the profile of a particular WBAN client by eavesdropping the communicating activities of this client. Thus, it is essential to protect the anonymity of the WBAN clients, and any failures to do so may result in violation of WBAN clients privacy and raise legal issues.

Mutual authentication: On one hand, the malicious adversary can access the service free of charge by impersonating as the legitimate WBAN clients. On the other hand, the malicious attacker may extract the sensitive personal health data from the target WBAN client by mounting the AP impersonation attack. Thus, the mutual authentication should be offered between the WBAN clients and requested remote AP.

Session key establishment: Due to the sensitive nature of the data collected by the medical sensors, a session key should be established between WBAN client and the requested AP to secure their subsequent communication. This study is devoted to investigating the basic cryptographic primitive for meeting these desired properties.

A. Applications Of WBANS:

WBAN applications can be categorized based on the type of sensors/actuators, radio systems, network topologies, and use cases. We enumerate here several pioneer healthcare WBAN research projects, as well as platforms for HCI applications.

1) WBANS for Healthcare:
WBANs extend conventional bedside monitoring to ambulatory monitoring, providing a point of care to patients, the elderly, and infants in both hospital-based and home-based scenarios. Monitoring, autonomous diagnostic, alarm, and emergency services, as well as management of electronic patient record databases can all be integrated into one system to better serve people.

2) WBANS for HCI:
Traditional computer interfaces, like keyboards, mice, joysticks, and touch screens, are all replaceable by potential WBAN devices capable of automatically recognizing human motions, gestures, and activities. Disabled people can benefit from novel WBAN platforms based on a series of miniature sensors. The intra-body communications (IBC) applications proposed in [4] can be used to assist handicapped people. For example, an IBC enabled sensor embedded inside the shoes of a blind person can be used to send voice information such as the current location to him/her by an IBC enabled facility, such as a doorway or crosswalk. IBC enabled eyeglasses that can display texts, working with IBC enabled speakers, can help deaf people comprehend audio broadcast announcements.

II. LITERATURE SURVEY

A. Enabling Technologies For Wireless Body Area Networks: A Survey And Outlook

A wireless body area network is a radio-frequency-based wireless networking technology that interconnects tiny nodes with sensor or actuator capabilities in, on, or around a human body. In a civilian networking environment, WBANs provide ubiquitous networking functionalities for applications varying from healthcare to safeguarding of uniformed personnel. This article surveys pioneer WBAN research projects and enabling technologies. It explores application scenarios, sensor/actuator devices, radio systems, and interconnection of WBANs to provide perspective on the trade-offs between data rate, power consumption, and network coverage. Finally, a number of open research issues are discussed.

Advantages:
Uses ZIGBEE for low data rate and low power consumption and network coverage.

B. A Survey On Intrabody Communications For Body Area Network Applications:
The rapid increase in healthcare demand has seen novel developments in health monitoring technologies, such as the body area networks (BAN) paradigm. BAN technology envisions a network of continuously operating sensors which measure critical physical and physiological parameters e.g., mobility, heart rate and glucose levels. Wireless connectivity in BAN technology is key to its success as it grants portability and flexibility to the user. While radio frequency (RF) wireless technology has been successfully deployed in most BAN implementations, they consume a lot of battery power, are susceptible to electromagnetic interference and have security issues. Intrabody communication (IBC) is an alternative wireless communication technology which uses the human body as the signal propagation medium. IBC has characteristics that could naturally address the issues with RF for BAN technology. This survey examines the on-going research in this area and highlights IBC core fundamentals, current mathematical models of the human body, IBC transceiver designs, and the remaining research challenges to be addressed. IBC has exciting prospects for making BAN technologies more practical in the future.

Advantages:
- Uses human body for interaction, that overcomes the limitations of radio frequency wireless network.

Disadvantages:
- Low battery power.
- Less security.

C. Sensor Networks For Medical Care:
Sensor networks have the potential to greatly impact many aspects of medical care. By outfitting patients with wireless, wearable vital sign sensors, collecting detailed real-time data on physiological status can be greatly simplified. However, there is a significant gap between existing sensor network systems and the needs of medical care. In particular, medical sensor networks must support multicast routing topologies, node mobility, a wide range of data rates and high degrees of reliability, and security. This paper describes our experiences with developing a combined hardware and software platform for medical sensor networks, called CodeBlue. CodeBlue provides protocols for device discovery and publish/subscribe multihop routing, as well as a simple query interface that is tailored for medical monitoring. We have developed several medical sensors based on the popular MicaZ and Telos mote designs, including a pulse oximeter, EKG and motion-activity sensor. We also describe a new, miniaturized sensor mote designed for medical use. We present initial results for the CodeBlue prototype demonstrating the integration of our medical sensors with the publish/subscribe routing substrate. We have experimentally validated the prototype on our 30-node sensor network test bed, demonstrating its scalability and robustness as the number of simultaneous queries, data rates, and transmitting sensors are varied. We also study the effect of node mobility, fairness across multiple simultaneous paths, and patterns of packet loss, confirming the system’s ability to maintain stable routes despite variations in node location and data rate.

Advantages:
- Codeblue provides protocols for device discovery and publish multihop routing.
- ECG sensors to get data from client.

Disadvantages:
- Codeblue
- Lack of reliable communication.
- Lack of security

D. The Advanced Health And Disaster Aid Network: A Light-Weight Wireless Medical System For Triage
Advances in semiconductor technology have resulted in the creation of miniature medical embedded systems that can wirelessly monitor the vital signs of patients. These lightweight medical systems can aid providers in large disasters who become overwhelmed with the large number of patients limited resources, and insufficient information. In a mass casualty incident, small embedded medical systems facilitate patient care, resource allocation, and real-time communication in the Advanced Health and Disaster Aid Network (AID-N). We present the design of electronic triage tags on light weight, embedded systems with limited memory and computational power. These electronic triage tags use non-invasive, biomedical sensors (pulse oximeter, electrocardiogram and blood pressure cuff) to continuously monitor the vital signs of a patient and deliver pertinent information to first responders. This electronic triage system facilitates the seamless collection and dissemination of data from the incident site to key members of the distributed emergency response community. The real-time collection of data through a mesh network in a mass casualty drill was shown to approximately triple the number of times patients that were triaged compared with the traditional paper triage system.

Advantages:
- It gives information from incident site to key members of community.
- It consumes very low power and less energy.
- It is error-prone and burdensome.
E. GRS:
The Green, Reliability, and Security of Emerging Machine to Machine Communications

Machine-to-machine communications is characterized by involving a large number of intelligent machines sharing information and making collaborative decisions without direct human intervention. Due to its potential to support a large number of ubiquitous characteristics and achieving better cost efficiency, M2M communications has quickly become a market-changing force for a wide variety of real-time monitoring applications, such as remote e-healthcare, smart homes, environmental monitoring, and industrial automation. However, the flourishing of M2M communications still hinges on fully understanding and managing the existing challenges: energy efficiency (green), reliability, and security (GRS). Without guaranteed GRS, M2M communications cannot be widely accepted as a promising communication paradigm. In this article, we explore the emerging M2M communications in terms of the potential GRS issues, and aim to promote an energy-efficient, reliable, and secure M2M communications environment. Specifically, we first formalize M2M communications architecture to incorporate three domains — the M2M, network, and application domains — and accordingly define GRS requirements in a systematic manner. We then introduce a number of GRS enabling techniques by exploring activity scheduling, redundancy utilization, and cooperative security mechanisms. These techniques hold promise in propelling the development and deployment of M2M communications applications.

Advantages:
- Energy efficient
- Reliable
- Secure M2M communication

F. ECG-Cryptography And Authentication In Body Area Networks:

Wireless body area networks (BANs) have drawn much attention from research community and industry in recent years. Multimodal healthcare services provided by BANs can be available to anyone, anywhere, and anytime seamlessly. A critical issue in BANs is how to preserve the integrity and privacy of a person’s medical data over wireless environments in a resource efficient manner. This paper presents a novel key agreement scheme that allows neighboring nodes in BAN store area common key generated by electrocardiogram (ECG) signals. The improved Jules Sudan (IJS) algorithm is proposed to set up the key agreement forth message authentication. The proposed ECG-IJS key agreement can secure data communications over BANs in a plug-n-play manner without any key distribution overheads. Both the simulation and experimental results are presented, which demonstrate that the proposed ECG-IJS scheme can achieve better security performance in terms of several performance metrics such as false acceptance rate (FAR) and false rejection rate (FRR) than other existing approaches. In addition, the power consumption analysis also shows that the proposed ECG-IJS scheme can achieve energy efficiency for BANs.

Advantages:
- The ECG-IJS key agreement can secure data communication in plug n play manner.
- Consumes less power

G. Certificateless Remote Anonymous Authentication Schemes For Wireless Body Area Networks:

Wireless body area network (WBAN) has been recognized as one of the promising wireless sensor technologies for improving healthcare service, thanks to its capability of seamlessly and continuously exchanging medical information in real time. However, the lack of a clear in-depth defence line in such a new networking paradigm would make its potential users worry about the leakage of their private information, especially to those unauthenticated or even malicious adversaries. In this paper, we present a pair of efficient and light-weight authentication protocols to enable remote WBAN users to anonymously enjoy healthcare service. In particular, our authentication protocols are rooted with a novel certificateless signature (CLS) scheme, which is computational, efficient, and provably secure against existential forgeries on adaptively chosen message attack in the random oracle model. Also, our designs ensure that application or service providers have no privilege to disclose the real identities of users. Even the network manager, which serves as private key generator in the authentication protocols, is prevented from impersonating legitimate users. The performance of our designs is evaluated through both theoretic analysis and experimental simulations, and the comparative studies demonstrate that they outperform the existing schemes in terms of better trade-off between desirable security properties and computational overhead, nicely meeting the needs of WBANs.

Advantages:
- Efficient and secure.
- Service provider has no privilege to disclose real identity of users.
- It meets the need of WBAN’S.

III. EXISTING SYSTEM

In exiting system the centre generates two keys for both WBAN client and application provider. There is an authentication b/w both client and AP. Certificateless Remote authentication protocol and Certificateless encryption is used.
A. **Drawbacks Of Existing System:**

- Increased routing overhead that leads to increase in the data leakage.
- Time delay increases due to long authentication process.

IV. **PROPOSED SYSTEM**

A. **System Model:**

The considered anonymous and revocable certificateless remote authentication protocol consists of three types of entities: the WBAN client, the AP, and the KGC. • *WBAN client:* Before accessing the wide range of services offered by the APs, the WBAN clients should be registered with KGC and preloaded with the public parameters. For safety reasons, a WBAN client must be revoked from the system in case KGC detects the misbehaviour of users or this user declares that his/her private key is compromised.

- *AP:* Similarly, the APs, such as hospitals, clinics, medical institutions or even weather forecast centres, should also be registered with KGC and preloaded with public parameters before they provide pervasive healthcare monitoring and treatment remotely to WBAN clients. The revocation of the APs is necessary as well in case the APs violate the system rules.

- *KGC:* KGC is in charge of the enrolment and eviction of WBAN clients and APs. In general, KGC cannot be fully trusted since it is usually acted by a commercial organization. By considering the commercial benefits, it is natural for the KGC to misbehave such as illegally collecting clients’ sensitive health information or accessing the services provided by APs free of charge. Therefore, the key escrow problem, where the KGC impersonates the clients or APs without being observed, should be avoided in our protocol.

![Fig. 2: System model](image)

B. **System Architecture:**

![Fig. 3: System Architecture](image)
Module explanation:
There are six modules in the project:
- Sensor node deployment.
- Mutual authentication.
- Session key establishment.
- R-CLS and R-CLE scheme.
- Remote authentication protocol.
- Security analysis

C. Sensor Node Deployment:
Here sensor nodes can be initialized with some number of nodes say (N=20), Before accessing the wide range of services offered by the APs (Application provider), the WBAN (Wireless body area network) clients will be registered with Key generation center (KGC) and preloaded with the public parameters. In similar Application providers will be registered in Key generation center.

D. Mutual authentication:
WBAN client and AP should be allowed to authenticate each other to resist impersonation attack from malicious intruders.

E. Session Key Establishment:
Here, mutual authentication will be offered between the WBAN clients and requested remote AP and due to the sensitive nature of the data collected by the medical sensors, a session key will be established between WBAN client and the requested AP to secure their subsequent communication.

F. R-CLE And R-CLS Scheme:
Here, a certificateless encryption scheme and a certificateless signature scheme with efficient revocation against short-term key exposure, is processed. We also propose the first R-CLE scheme against decryption key exposure, and the first R-CLS scheme against signing key exposure.

Choose a random integer \( x \in \mathbb{Z}_p \) as well as a random generator \( g \in G \), and compute \( g^1 = gx \). Pick a random element \( g^2 \in R G \) and three hash functions \( H_1, H_2 \) and \( H_3 \) such that \( H_1 ID \rightarrow G, H_2 : T \rightarrow G, H_3 : GT \times G \rightarrow M \), where \( ID, T \) and \( M \) denote the identity space, time space and message space respectively. Set an initially empty revocation list \( RL=\emptyset \) as well as a state \( st = BT \). Here, \( BT \) refers to a binary tree with \( N \) leaves.

Ini-Par-Pri-Key-Gen: Once receiving an identity \( I D \), KGC first checks whether the identity \( I D \) exists in the RL or not, and aborts this algorithm if this identity has already been revoked. After that, KGC stores the identity \( I D \) in the leaf node \( \eta I D \), which is randomly chosen from the binary tree \( BT \).

G. Key-Upd:
For each node \( \theta \in \text{KUNode}(BT, RL, T) \).

H. Par-Pri-Key-Gen:
This algorithm will abort in case \( \text{KUNode}(BT, RL, T) \cap \text{Path}(\eta I D) = \emptyset \).

I. User-Key-Gen:
The user \( I D \) selects a secret value \( tI D \in \mathbb{Z}_p \) as its user secret key \( uskI D \), and computes his public key[1].

J. Encrypt:
Choose \( r \in \mathbb{Z}_p \) and compute the ciphertext.

K. Revoke:
In case the insider attacker \( I D \) has been detected or the private key of the user \( I D \) get compromised, the leaf node \( \eta I D \) associated with identity \( I D \) along with the revocation

L. Remote Authentication Protocol:
Here, KUNodes algorithm is used to achieve the efficient revocation function (Key Update). After that R-CLE and R-CLS scheme phases, a certificateless anonymous remote authentication with revocation is constructed by incorporating the proposed encryption scheme and signature scheme. It consists of the Setup, Key Generation, Key Update, Authentication and Revocation phases.
**M. KUNode Algorithm:**

Definition: Given a binary tree BT, a revocation list RL, and time Tk, the KUNode algorithm outputs a set of nodes for the key update. The formal specification of KUNode algorithm is described in Algorithm 1. The nodes in the binary tree BT are uniquely encoded as strings, and BT is depicted by all of its nodes descriptions. If a user, who is assigned to the leaf node η, is revoked within the time period Tj, then the item (η, Tj) will be inserted into the revocation list RL. Path(η) refers to the set of nodes on the path from the leaf node η to the root node (both η and root node inclusive). If x is a non-leaf node, then xleft and xright denote left and right child of x respectively. A pictorial example of KUNode(BT, RL, Tk) algorithm is shown in Fig. 3. The root node will be returned by the KUNode algorithm in case no user has been revoked. If a user u7 (assigned to the leaf node M) has been revoked, the set of nodes Path(M) = {R, B, F, M} will be inserted into the set X, and the set Y = {A, E, N} will be returned. For the revoked user u7, Path(M) ∩ Y = ∅, whereas other unrevoked users at least have a node y ∈ Y such that y is contained in the set of nodes on the path from the root node to their corresponding assigned leaf node.

When a user (e.g., a client or a remote server) joins the system, KGC first assigns a random leaf node η of a complete binary tree BT to this user, and then issues a set of initial partial private keys (identity component of partial private key) to this user, where each key in this key set is corresponding to each node on Path(η). To exclude revoked users, the KGC distributes the key updates (time component of partial private key) for a set KUNode(BT, RL, T) at time period T. In this way, only non-revoked users are able to generate the full partial private key since non-revoked users have at least one key corresponding to a node in KUNode(BT, RL, T) according to the complete subtree method.

![Fig. 4: An example of KUNodes algorithm](image)

**N. Security Analysis:**

In this phase, the security of the proposed protocol will be analyzed according to security requirements such as Anonymity, Mutual Authentication, Session Key Establishment, Non-Repudiation, Revocable and Forward Security. It has to provide highly secured system.

**Q. Advantages of Proposed System:**

- By using reliable routing techniques, we can avoid data loss.
- All personal information can be reached successfully to the respected destination securely.
- Time delay can be reduced.
V. RESULTS

A. Scenario 1:

The above scenario show the deployment wireless nodes with base stations. First we need to initialize some node to transfer the data, in our project we are deploying some 32 nodes. In which one will be the source that is WBAN client or SPD(smart portable device), and the other node will be application provider, the other node will be the sink where it helps to transfer the information from WBAN client t application provider.

B. Scenario 2:

In this screenshot we can see all the nodes that is source (WBAN client or SPD), sink which helps to transfer the data, KGC (key generation center) which establishes key and send to WBAN client and application provider for authentication and the application provider that is physician, hospital etc.
C. Scenario 3:

![Figure 6](image)

Fig. 6: KGC is establishing key and sending the key to application provider for authentication

D. Scenario 4:

![Figure 7](image)

Fig. 7: finding the malicious nodes

To transfer the data it should select the neighbouring nodes, if it selects the malicious nodes it revokes that node and start finding the new one, once it start select the node which is not malicious then it starts sending the information to it. Because of this malicious node there may be loss of data as shown in the screenshot.

Scenario 5:
A Certificate Less Encryption and Signature Scheme with Efficient Revocation for Securing Inter-Body Wireless Sensor Network

The probability of security is more when you compare it with the existing system; the green line on the graph shows the security of the proposed system.

Scenario 6:

As we compare with the existing system the proposed system is less time consuming, the green line shows the proposed systems the red line shows the existing systems.

VI. CONCLUSION AND FUTURE WORK

The main aim of the project is to transfer the information from WBAN client to the application provider securely, so for that security propose we are using the remote authentication routing protocol and the R-CLS,R-CLE scheme for authentication purpose. By using all this schemes and all we can send the information to application provider securely. By using reliable routing techniques we can avoid data loss, all personal information can be reached successfully to the respected destination securely and time delay can be reduced. In future there is a need to provide more security and avoid overhead.

ACKNOWLEDGMENT

NARAYANA K R, thanks to Ms. SANCHARI SAHA, who is always encouraging and motivating me to do research activities. I am also very thankful my families and friends.
REFERENCES