A SECURE AND EFFICIENT PROTOCOL FOR WIRELESS BODY AREA NETWORKS

Sharmila R
Technical Writer
Vpro Technologies
Sharmimol22@gmail.com

Sandhiya.R S
Research Analyst
Vpro Technologies
Sandhiyars93@gmail.com

Abstract-*Wireless Body Area Networks are expected to play roles in the field of patient-health monitoring, which gains the tremendous attention among the researchers in recent years. it establishes a secure communication architecture between sensors and the users while addressing the prevalent security and the privacy concerns. In this paper, we propose communication on BANs architecture and design to secure that the data communications between the sensors and the data consumers by employing Cipher text-Policy Attribute-Based Encryption and signature to store the data in Cipher text format at the data sink that ensuring data security. Our schemes that achieves on role-based access control by employing an access control tree defined by the attributes of the data. We analyze the scheme and it providing the message authentication, collusion resistance, efficient and feasible.*

***Keywords*- Cipher text, Authentication, Body Area Network**

INTRODUCTION

Body area networking is a technology for real time monitoring on the physiological signals to support the various medical applications. It enables the rapid development of wireless sensor networks and the biomedical engineering techniques. A typical body area networks (BAN) consist of a number of wearable and implanted by the sensors to monitor the parameters of human body and the surrounding environments. It can assist the human body by providing life support and visual/audio feedback, etc.

Unlike conventional sensor networks, BANs are deal with the medical information about more stringent security and privacy requirement. The lack of adequate security protections may not only lead to a breach of the patient's privacy, but also give a chance for the adversaries to threat the patients by modifying the data from the BAN which may result in wrong diagnosis and treatments. Since wireless communication is one of the most vulnerable aspects of a BAN are securing the inter-sensor communications plays a critical role in securing the BAN.

The BANs rely on cryptographic keys to perform authentication and to provide data confidentiality and the integrity. The Keys are usually distributed to sensors in key distribution protocols. Which are typically requiring some form of keying information pre-deployment?

However, with increasing the size of a BAN, the traditional approaches are involving a considerable latency during the network initialization, owing to the needs for information Pre-deployment.We intend to provide an efficient security scheme with the prosperities of plug-n-play and transparency. i.e., the users can add, remove and tune the sensors of a BAN without reconfiguring the Network but can still enjoy the benefits of secure communications. The characteristics can help to minimize the communication overhead during the initialization process and thus reveal with the less information are identifiable for the patient. For instances, Plethysmogram and PSKA have been presented to avoid key information on Pre-deployment. The security level of these techniques are not high enough due to the limitations are placed by the size of feature and the high complexity of computing chaff points are analyzed.

Inthis paper, we propose communication on BANs architecture and design to secure that the data communications between the sensors and the data consumers by employing Cipher text-Policy Attribute Based Encryption and signature to store the data in Ciphertext format at the data sink that ensuring data security.The features are computed from the physiological signals to measure at the different parts of human body and to enable the sensors agree on a symmetric cryptographic key is an authenticated and securing the inter-sensor communications. i.e., initialization is not required. It does not require any key pre-distribution. It exploits the dynamic and complex the human body of nature. This works as follows: 1) The features generated in each sensor are ordered to form feature vector and the sensor collecting the data to knows that the order of features. 2) The sender sends a secret features along with a large number of data to the receiver. 3) The receiver that generates a key according to the common features and then returns the indexes of matching features. 4) The sender identifies the common features in its own feature vector and computes the key accordingly. The keys are long and random to prevent brute force attacks. They are efficient in terms of computational, communication and the storage that are possessed on the properties of time variance and distinctiveness.

The main contributions of the paper are following that are:

1) We propose a secure and efficient scheme is an authenticated key agreement between two sensors in a BAN.

2) We analyze its efficiency and feasibility.

3) We compare OPFKA with PSKA in terms of the security levels, the resistance against brute force attacks and other aforementioned design goals. Our results are demonstrated on the superiority of OPFKA over PSKA.

4) We estimate on the performance of OPFKA in terms of computational, communication and storage.

II. RELATED WORK

The Most previous work on BAN security is focus on the issues such that encryption, key management and access control. In order to secure that the intersensor communications, the idea of employing physiological signals are first introduced in which the features derived from the physiological signal simultaneously measured at different parts of the body that are used to generate the actual key shared by the sensors.Then to establish a common set of features in simple error correction can be employed to correct the differences between the physiological features generated at different sensors. Based on this Idea is proposed to employ that the Inter-Pulse-Interval (IPI) is to generate the cryptographic keys by encoding the IPIs into a 128-bit binary key.

However, the results of real world experimental study is to indicate that the Hamming distance of two IPIs that are obtained from the same subject and the different subjects are 60 and 65, respectively. Though suggested that error correction can be used to improve

The matches of features derived from the same human body. Thus the scheme is still not practical. Since, the Hamming distance of the IPIs is the same person by making the error correction still varies from 0 to 40. It lies on the translational and rotational errors that can produce drastically different values when IPIs are naively encoded into binary.

In existing system, as a sensor that collects patient information, it distribute on all the information to authorized doctors and other experts securely. However, the Data should be transmitted in a secure channel and it securing that the wireless communication channels. Node authentication is most fundamental step towards a BANs on initial trust establishment, key generation and subsequent for secure communications. There existing research on the embedded sensors is to establish a session key with each other by leverage physiological signals such as Electrocardiograph (ECG).

The most relevant existing research along three lines:

(1) secure that individual devices within a BANs;
(2) secure that the communications within a BANs;
(3) identity-based Cryptography for BANs.

In proposed system, we propose a novel encryption and the signature scheme based on CP-ABE. It has been secure that the communication problem and it provides the required security services for BANs. A sensor can control the access with data. It has produced by constructing an access structure. For example, by constructing the access structure, the data requires that only doctors or experts in GWU hospital, Vascular Surgery Center or Cardiac Surgery Center can have the access right.

The Data is stored in Cipher text format on data sink and the trust. We put on the data sink was drastically decreased as the key does not decrypt the data sink is stored in cipher text. However, the scheme belongs to the asymmetric encryption. Which implies a high computational cost? This problem is too addressed by using the scheme of session key and then the data is encrypted by symmetric encryption based on the session key.

III. SYSTEM DESIGN

In the design of BAN security mechanisms is face to critical challenges: In how to properly regulate the access while providing strong access control to the BAN controller? Toverify the identity of the person we propose to design an attribute based on security.

This scheme is not only differentiated by encryption mechanisms but also it is a role-based strong access control. To protect against the information is to exposure due to theft or loss of the BAN controller, the personnel identification should be verified when they connect with the controller. If the control is to access the controller, the attribute-based encryption over IBE will be investigated. Similarly, access structures are used to control the access rights for different users of the BAN controller.

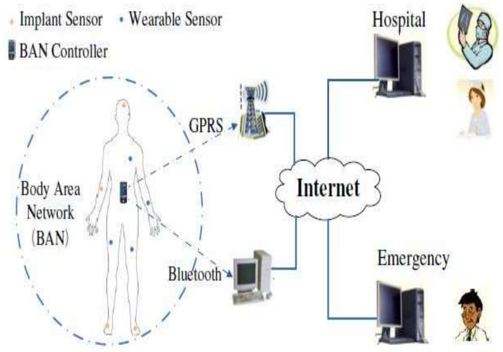

Fig:BAN architecture of a healthcare application

IV. FEATURE EXTRACTION

A BAN is a network that interconnects the physiological and the environmental monitoring sensors that are implanted inside a human body. These sensing devices are collect physiological and contextual information of a human body for a regular interval and it transmit to a highly capable sink node are further processing over on multihop wireless communications.

We assume that all sensors are implanted, these are able to measure that the appropriate physiological signals. We also assume that the entity it does not have a physical contact with a human body that cannot collect any physiological signal and that only legitimate sensors can contact with the human body.

Thus attackers are mainly able to monitor the traffic on the wireless medium are not secure. Furthermore, we assume that the malicious entities that cannot compromise the sensors in a BAN without being detected. such that the sensorsare under the supervision of the host and the caretaker. The threats faced by a BAN are primarily from adversaries that can eavesdrop on the traffic of the BAN, replay old messages, and inject messages to compromise the confidentiality of the BAN communications or spoof the BAN sensors identities. Adversaries may also break the key distribution process by using the physiological signal data obtained from another person if the scheme does not have sufficient distinctiveness.

In this paper, we focus solely on designing a secure and efficient scheme to ensure the security of inter-sensor communications within a BAN. Communications from the sink onwards can utilize conventional security schemes such as Secure Socket Layer (SSL) is given the considerable capabilities of the entities involved. Note that in this paper, we do not consider denial of service (DoS) attacks such as jamming, electromagnetic interference and battery depletion.

A. Network Model

There are two main entities in this system: BAN of the patient and external users. In particular, the BAN consists of one BAN controller and a number of devices. These devices are usually the sensors that are monitoring the body of parameters or movements, the human body that control by providing life support, visual feedback, etc. The BAN devices that are communicate with the BAN controller directly or via the multihop communications. The BAN controller communicates with not only the BAN devices but also the Internet.

In this paper, we assume that the existence of a trusted third party KS. i.e., the key distribution server which is able to verify that the identity of a legitimate external user and it distribute for credentials to the external user accordingly. The identity of the external user is a set of attributes that are describing the basic information from the user. KS is not required to online when an emergency-room doctor needs to communicate with the BAN of a patient. i.e., it does not become a single point-of-failure for the system.

B. Adversary Model

In this paper, we consider a both types of adversaries outlined in this Section: 1) passive adversaries that eavesdrop messages transmitted (wirelessly) within the BAN and the external user; 2) Active adversaries to manipulate the transmitted messages. We also consider the collusion of multiple adversaries.

C. Security Requirements

Now, we end the requirements of secure communications in a BAN:

- Accessing the Control: The security mechanism must be able to commonly enforce the different access with the rights for the different users.
- Authentication: In a BAN, an active adversary may alter the content for the sequence and timing of transmitted message. Thus, a security mechanism must properly authenticate the messages by receiving the BAN as well as by the external users.

V. CONCLUSION

WBAN is an emerging and technology that will change the experiences of revolutionarily. It brings the replacement set of challenges for the terms of quantity sensor deployment and density, energy potency, security, privacy, and wireless technology. During this survey, we have review the present development on Wireless Body Area Network and also that we have targeted in security problems faced by this technology. Specifically, this work will present the outline of variations between the Wireless Body Area Network and the Wireless sensor Network. We tend to conferred variations of design in WBAN and different kind of Wireless sensor network. Several key applications can get pleasure from the advanced integration of WBAN and rising wireless technologies. They embrace remote health observance, military, sports training and plenty of others. It's additionally necessary to focus on here that WBAN poses with numerous sorts of security issues. Thus, we tend to believe that the WBAN needs to a robust security system and a part of its authentication.

REFERENCES

[1] Chunqiang Hu, Xiuzhen Cheng, Fan Zhang, Dengyuan Wu, XiaofengLiaoy, Dechang Chen, "OPFKA: Secure and Efficient Ordered-Physiological-Feature based Key Agreement for Wireless Body Area Networks".

[2] Chunqiang Hu, Nan Zhang, Hongjuan Li, Xiuzhen Cheng and Xiaofeng Liao, "*Body Area Network Security: A Fuzzy Attribute-Based Signcryption Scheme*", *VOL. 31, NO. 9, SEPTEMBER 2013.*

[3] Ramesh Kumar et al., RajeswariMukesh,"*State Of The Art: Security In Wireless Body Area Networks*" *International Journal of Computer Science & Engineering Technology (IJCSET).*

[4] Ming Li and Wenging Lou, KuiRen, "*Data Security and Privacy in Wireless Body Area Networks*"*Worcester Polytechnic InstitituteIllinois Institute Of Technology.*

[5] Ajit, Amita Malik, "*Security in Body Area Network: A Survey*" *International Journal of Enhanced Research in Management & Computer Applications, ISSN: 2319-7471 Vol. 3 Issue 5, May-2014, pp: (70-76), Impact Factor: 1.147, Available online at:***www.erpublications.com**

[6] Nahid.Kittur, P. MeenaPriyaDharshini, "*Review of Key Management Technique for Wireless Body Area Networks*" International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056 Volume: 02 Issue: 04 | July-2015 www.irjet.net p-ISSN: 2395-0072.

[7] Pablo Picazo-Sanchez, Juan E. Tapiador, Pedro Peris-Lopez and Guillermo Suarez-Tangil, "*Secure Publish-Subscribe Protocols for Heterogeneous Medical Wireless Body Area Networks*" Sensors 2014, www.mdpi.com/journal/sensors