www.ijecs.in
*International Journal Of Engineering And Computer Science ISSN: 2319-7242*
*Volume 6 Issue 1 Jan. 2017, Page No. 20104-20107*
*Index Copernicus Value (2015): 58.10, DOI: 10.18535/ijecs/v6i1.44*

# Survey on Efficient Certificateless Access Control for Wireless Body Area Networks

***Jeena Sara Viju*[#1], *Sruthy S*[#2]**
[#1]PG Scholar, Computer Science and Engineering
Sree Buddha College of Engineering, Ayathil, Kerala
[#2]Assistant Professor, Computer Science and Engineering
Sree Buddha College of Engineering, Ayathil, Kerala

***Abstract*—**Recent developments and advances in the field of wireless communication has led to the discovery of Wireless Body Area Networks (WBANs). The wearable computing devices made it easy to monitor the health issues of patients. The WBANs are widely used taking into account its numerous advantages. Many publications are available mentioning the various challenges of WBANs. In this paper, a survey is performed on the current state-of-art of WBANs based on the latest standards and publications. Open issues and challenges within each area are also explored as a source of inspiration towards future developments in WBANs.

***Keywords*— Wireless Body Area Networks, Signcryption, certificateless cryptography, access control.**

## I. INTRODUCTION

In the last few years the consideration of specialists toward WBANs has greatly increased. Wireless Body Area Networks (WBANs) are wireless network of computing devices that are wearable. These wearable computing devices helps doctors to monitor the health problems of their patients easily. In WBAN, miniaturized sensors and actuators are placed in or on the body. These sensors and actuators enhance and support new medical and healthcare services. The patients can leave the hospital and they can stay where ever they are comfortable as the doctors will be able to monitor their patients' condition through WBANs. Sampling, processing and transmitting physiological signals of patient are performed by the embedded sensors. The information collected can be continuously sent to the doctors, nurses or the person in charge without any delay so that the treatment can be opted quickly. The applications of WBANs are not only limited to medical field but also to non-medical fields. One of the significant medical applications is remote health checking. In the past, health observing was done through number of electrical equipment.

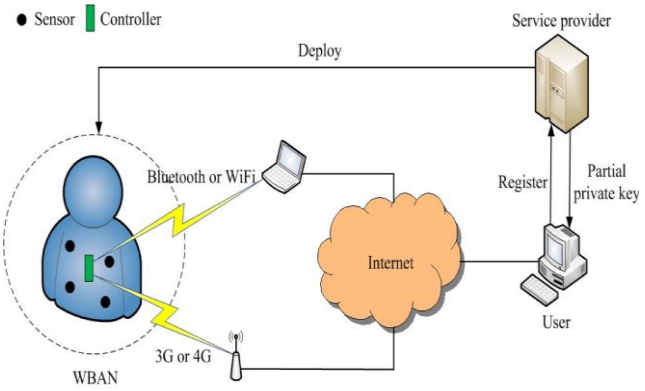


Fig. 1 Network model of Wireless Body Area Networks

Sensor nodes and a controller are present in WBANs. The communication is possible with sensor nodes and the controller whereas the controller not only communicates with the sensor nodes but also with the service provider. The service provider (SP) is used to deploy the WBAN. A user should be authorised by service provider before accessing the collected information. The registration for both the user and the WBAN is done by service provider and partial private key production for the user and the private keys for the WBAN is also performed by service provider. That is, the role of the KGC in the CLC is performed by SP. When a user needs to access the monitoring data of the WBAN, it first sends a query message to the WBAN. Then controller checks the authentication of the user. If the user is authorised, then the controller sends collected data to the user in a secure way. Otherwise, the query request will be refused by the controller.

In this paper latest studies in WBANs are considered, the challenges in each underlying subfield are presented, and survey the important results in the field.

## II. APPLICATIONS OF WBANs

The applications of WBANs are not limited to medical field but its applications are numerous. The applications span a wide area such as military, ubiquitous health care, sport, entertainment and many other areas. The main characteristic in all WBAN applications is improving the user's quality of life. Many varieties of WBANs are available today. It is not compulsory that it should be fixed in the body. It may be fixed or sometimes movable as well taking into consideration the comfort of the user. Some in-body and on-body applications are mentioned in Table I.

Table I: Applications of WBANs

| | | | |
|---|---|---|---|
| WBAN Applications | Medical | Wearable WBAN | Assessing soldier fatigue and battle readiness. |
| | | | Aiding professional and amature sport training. |
| | | | Sleep staging. |
| | | | Asthma. |
| | | | Wearable health monitoring. |
| | | Implant WBAN | Cardiovascular diseases. |
| | | | Cancer detection. |
| | | Remote control of medical devices | Ambient assisted living. |
| | | | Patient monitoring. |
| | | | Tele-medicine systems. |
| | Non- medical | | Real time streaming. |
| | | | Entertainment applications. |
| | | | Emergency (non medical). |

## III. COMMUNICATION ARCHITECTURE

The communication architecture of WBANs can be separated into three different tiers and is depicted in figure 2.

- Tier-1: Intra-WBAN communication
- Tier-2: Inter-WBAN communication
- Tier-3: Beyond-WBAN communication

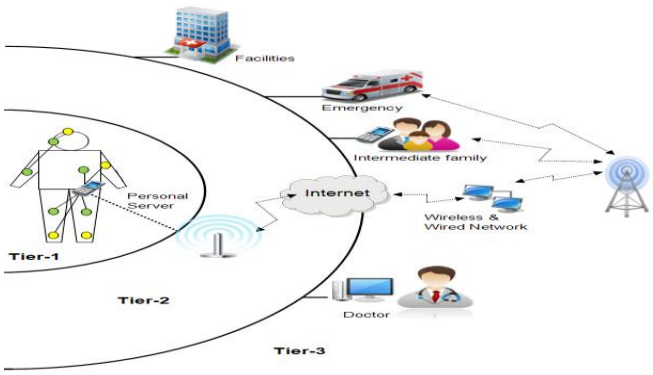


Fig. 2 Communication Architecture of WBANs

**Tier-1: Intra-WBAN communication** – It depicts the network interaction of nodes and their respective transmission ranges (2 meters) in and around the human body.

**Tier-2: Inter-WBAN communication** – In the case of Tier-2 the communication is between the PS and one or more access points (APs).

**Tier-3: Beyond-WBAN Communication** – This communication tier design tier is for use in metropolitan areas. A gateway such as a PDA can be used to bridge the connection between Tier-2 and this tier.

## IV. RELATED WORK

Medical monitoring is an important Wireless Sensor Networks (WSN) application. In order to collect information such as heart rate, temperature, blood oxygen saturation level or even electrocardiogram (ECG) signals, wireless sensors can be placed on patients in a hospital or homecare setting. Correct WSN design depends on accurate traffic models. The traffic models are used in selecting the correct routing and MAC protocols for the network [1].

An approach which provides high end security for the patient's sensitive physiological data and assures maximum privacy for the patients is proposed. Cryptography mechanism called Paillier cryptosystem, which ensures the security of data is used. This approach has a unique homomorphic property of producing the sum of plaintexts while encrypting the product of cipher texts [2].

High end security for wireless medical sensors data are ensured. Three data servers are used to store the patient's split value of physiological data. More security is thereby offered to the patient's data.

The security vulnerabilities in data discovery and dissemination of WBANs is discussed. A

lightweight and confidential data discovery and dissemination protocol which is based on the unique features and application requirements of WBANs, is proposed. In order to maintain confidentiality, low-complexity symmetric cryptographic techniques are used [3].

Channel coding is used here. This is to overcome the problem that occurs while designing an energy aware transmission schedule for a wireless node. By transmitting at reduced power levels, energy is being conserved. Channel coding conserves energy by transmitting at reduced power levels over longer durations [4]. This was performed instead of transmitting packets at constant power for a fixed duration. The transmitter should be idle in order to allow recovery.

While referring the BAN in telemedicine and m-health, it is known as BASN. Both BAN and BASN appear similar. In the case of BASN, every node consists of a biosensor or a medical device. These units are provided with a sensing unit. Firstly BAN was proposed to connect personal consumer electronic devices in order to make it convenient to the user [5]. BASN was setup for many reasons.

The continuous vital sign monitoring capabilities are provided by the TSN system. It has the potential to provide continuous vital sign monitoring capabilities without the exhaustion of any manpower. It provides support to the present health problems. By collecting the human body signals, the most relevant health information of the patient is made available at all times [6].

The most important requirement for healthcare systems is their ability to work continuously. The working period is not limited to a short period but it should work over long time. These features are satisfied by AlarmNet [7]. Heterogeneous devices are used in a common architecture. The network will be used for the patient's medical needs and is capable of providing notifications.

The development in the field of wireless technology have opened new healthcare challenges. The small sensors placed in wireless body area networks are used to collect the vital signals of human body. Ultra-low-power wireless connectivity which is udsed among devices is seen as a key technology enabling unprecedented portability for monitoring physiological signs. BAN helps in identifying the health problems earlier itself thereby the patient can be saved from health issues. The quote "prevention is better than cure" is achieved through this latest technology [8].

The concept of virtual sensors are used to design a new approach for BSN applications. This approach relies on SPINE2 framework. Virtual sensors allow abstracting even complex systems that behave like sensors, thus favoring code modularity and reuse. If a programmer needs to update an implementation of a virtual sensor or changing environmental conditions require that a different implementation strategy is adopted, it is sufficient to replace that portion of code without changing the rest of the system implementation [9].

## V. CONCLUSION

Wireless Body Area Networks are widely used nowadays and therefore many new technologies are being developed in this field. In this paper, a survey is performed on the new technologies based on WBANs. This helps it easier to understand the latest technologies as well as to spot out the problems with the upcoming technologies.

## REFERENCES


[1] Geoffrey G. Messier and Ivars G. Finvers " *Traffic Models for Medical Wireless Sensor Networks*", IEEE COMMUNICATIONS LETTERS, VOL. 11, NO. 1, JANUARY 2007

[2] Navya D, Rashmi M, "*Securing Remote Medical Sensor Data by Adapting Paillier Cryptosystem Mechanism*", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 5, Special Issue 10, May 2016.

[3] Daojing He, Member, IEEE, Sammy Chan, Member, IEEE, Yan Zhang, Senior Member, IEEE, and Haomiao Yang, Member, IEEE," *Lightweight and Confidential Data Discovery and Dissemination for Wireless Body Area Networks*", ieee journal of biomedical and health informatics, vol. 18, no. 2, march 2014

[4] Pavan Nuggehalli, Member, IEEE, Vikram Srinivasan, Member, IEEE, and Ramesh R. Rao, Senior Member, IEEE*," Energy Efficient Transmission Scheduling for Delay Constrained Wireless Networks*", IEEE transactions on wireless communications, vol. 5, no. 3, march 2006.

[5] Carmen C. Y. Poon and Yuan-Ting Zhang, The Chinese University of Hong Kong Shu-Di Bao, The Chinese University of Hong Kong and Southeast University," *A Novel Biometrics Method to Secure Wireless Body Area Sensor Networks for Telemedicine and M-Health".*

[6] Fei Hu, Member, IEEE, Meng Jiang, Member, IEEE, Mark Wagner, Member, IEEE, and De-Cun Dong, Senior Member, IEEE,

"*Privacy-Preserving Telecardiology Sensor Networks: Toward a Low-Cost Portable Wireless Hardware/Software Codesign*", ieee transactions on information technology in biomedicine, vol. 11, no. 6, november 2007.

[7] Anthony D. Wood, John A. Stankovic, Gilles Virone, Leo Selavo, Zhimin He, Qiuhua Cao, Thao Doan, Yafeng Wu, Lei Fang, and Radu Stoleru, University of Virginia," *Context-Aware Wireless Sensor Networks for Assisted Living and Residential Monitoring".*

[8] Maulin Patel And Jianfeng Wang, Philips Research North america, "*Applications, Challenges, And Prospective In Emerging Body Area Networking Technologies".*

[9] Nikhil Raveendranathan, Stefano Galzarano, Vitali Loseu, Raffaele Gravina, Roberta Giannantonio, Marco Sgroi, Roozbeh Jafari, and Giancarlo Fortino," *From Modeling to Implementation of Virtual Sensors in Body Sensor Networks",* IEEE SENSORS JOURNAL, VOL. 12, NO. 3, MARCH 2012.