International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 3, Issue 11, November 2014

SECURITY MECHANISM IN BODY AREA NETWORK-A SURVEY

Divya R[1], Sundararajan T.V.P [2], Deepak KR[3],Nagarajan P[4] ,GokulPrasath Y[5]

Abstract— **Wireless Body Area Network is an Emerging technology in Wireless Sensor Network for various applications in healthcare, entertainment, defense etc., In Body Area Network, sensors are used to monitor the human's activities and their actions like health parameters so it is necessary to secure the privacy of the user and the necessary information are collected by the sensors from the body of the user. In this paper we discussed introduction, architecture, issues, challenges, and security approaches of Body Area Network. Different types of security protocols are discussed for Body Area Network and their comparison is also made.**

Index Terms— Body Area Network, Security, Asymmetric, Symmetric, Hybrid, Key.

I. INTRODUCTION

A Body Area Network(BAN) is also defined as a standard for short range and wireless communication which are either attached to the body or implanted under the skin which provides real time monitoring. BAN is used in healthcare network for continuously monitoring of the patient in which various sensors are attached to the patient's body. Values are taken by various sensors and then analyzed [1]. It is very easy for patient to make physical movement. For the people having physical disabilities BAN is very useful. For the disabilities many inventions are made such as artificial hands, muscle tension monitoring, and speech disability and even some inventions are made for blind people. Body Area Network differs with wireless sensor network in various features like security, power efficiency etc. Table 1 shows comparison [2] between BAN and WSN.

WSN	BAN
In the environment	On the human body
More nodes	Less nodes
Less accuracy	More accuracy
High power	Low power
Lower security	Higher security
More flexible to replace	Less flexible to replace
Mobile	Stationary

Table 1:Comparison between BAN and WSN

The designing of sensor in BAN is also differs from WSN. However, the basic components of sensor in both the networks are same like transceiver, microcontroller, memory and A/D controller. Sensors in BAN are miniaturized and compatible to body. There are different types of sensors for different application in BAN. In medical field wearable and implantable sensors i.e. the sensors for ECG, temperature, motion, blood pressure etc.

II. ARCHITECTURE OF BAN

In Body Area Network sensors, smart phones, access point and remote server are defines the architecture. The architecture of BAN is divided into three tiers. The architecture of BAN [3] is shown in Figure 1.

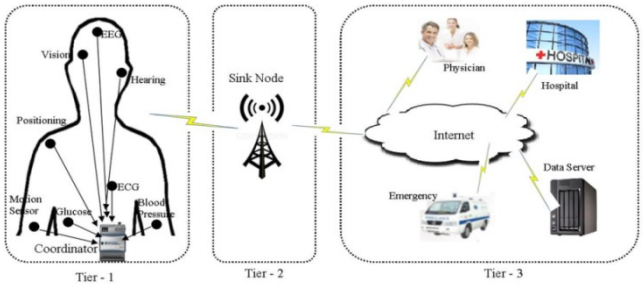

Figure 1: Architecture

a) **Tier 1:** This tier provides the communication between sensors and smart phone. This tier is also known as intra BAN [4]. Its design is very critical because of direct relationship of sensors with body.
b) **Tier 2:** This tier is also called as inter-BAN. It is used to provide communication between sensor coordinator and PDA to access point. This tier is used to create connection between BAN to internet.
c) **Tier 3:** This tier is also called as beyond-BAN or extra-BAN tier. It can enhance the coverage range of the system i.e. remotely access the data of the patient to the hospital or doctor.

ISSN: 2278 – 909X

APPLICATIONS OF BAN

There are various applications of body area network [5], like in healthcare [6], entertainment etc. In all it can be said that BAN can monitors the activities of a person. Some applications of BAN are following:

a) **Healthcare:** BAN widely used in the medical field for monitoring the patient [7]. Patients of critical disease can be monitor at their home. It monitors ECG, EMG, EEG etc.
b) **Entertainment:** This network is used in computer games, music players, headphones etc.
c) **Sports and Fitness:** This network is also useful in monitoring the sport person by sensing hid BP, heart rate etc.
d) **Defense:** BAN monitors soldiers in defense services.
e) **Lifestyle:** BAN is also useful in emotion and posture detection.
f) **Assistance to disable person:** The BAN can also be useful for the person with disabilities like blindness, speech disability etc.

ISSUES AND CHALLENGES OF BAN

There are various issues and challenges in BAN [4, 8 and 9]. These are following:

a) **Energy constraint:** Since it is battery oriented network, have to use in efficient memory mechanism [10] to use it for a long time.
b) **Low computational power:** In BAN, sensors have limited memory and less computational power. Try to perform small bit computation on this network.
c) **Node size:** Comparing with WSN, we have to take size of node is small.
d) **Sensor effect on body:** There is risk of irritation or allergy on the body after implantation of sensor.
e) **Strength:** It is a challenge to make low possibility of a node to failure.
f) **Minimize idle listening and collision:** Idle listening means an active listening to the idle channel. These both are responsible for energy wastage. It is a challenge to minimize them.
g) **Sensor and environmental interference:** Network congestion and signal attenuation are responsible for these problems. Data may be lost by this interference.
h) **Security:** Security is a big issue in BAN [11]. The information is so much critical. If security of a network is not handled properly it may life threatening. Some issues are following:
    - Data modification: Attacker may modify or delete data on the network. It may result failure of system.
    - Replaying: Resend the information for misleading the observer.
    - Authenticity: It is a challenge to make the network authenticate otherwise it leads to data loss.
    - Denial of service: It is necessary to make network Dos free. Denial of service may lead improper working of network.

III. SECURITY IN BAN

BAN has main challenge on security. The main focus of this paper is to discuss various security problems and solutions to secure BAN. The security solutions which are used for WSN are not applicable to BAN because various resource constraints like energy, memory etc. To make BAN secure we have to work in the area of confidentiality, authorization, authentication, non repudiation, integrity control. As we discussed above BAN has three tiers architecture so there are different security requirement for each tier. In tier 1, the security can be on the sensors and their communication and to Personal Digital Assistant(PDA) or smart phone. The security solutions on tier 1 should be lightweight because of the constraint on the sensor because these are energy constraints. In tier 2, and 3 the security can provide on the communication from PDA to the medical server through internet. The security on PDA and medical server may not be lightweight because they are not energy constraint. The data which is sense by the sensors of BAN is critical so we need to encrypt the data with the help of security key. The security may be of symmetric, asymmetric or hybrid.

ASYMMETRIC KEY BASED PROTOCOLS IN BAN

This is a public key cryptography were there are two keys private key and public key. The private key is a secrete key known to the particular sensor but public key is known to all. Encryption is done by the public key and decryption is done by secrete key. So, it is not required to send the keys securely. There are various algorithm present in public key cryptography to secure BAN. RSA and Elliptic curve cryptography(ECC) [12] are two known algorithm for the public key cryptography. But it requires more memory and is computationally expensive. So, it is not well suited for BAN. A protocol for strong authentication has been proposed in [13]. It presents three elliptic curve based key agreement protocol with authentication via hidden public key transfer, pre-shared password and with only fractional variations from a common unauthentication base protocol. A secure and efficient data storage scheme has proposed in [14]. This scheme performs dynamic integrity checking in BAN. It utilizes multiple secret sharing policies guarantee data confidentiality and dependability in terms of patient related data storage and access. By using this approach only authorized user can access data stored in BAN. This scheme supports quick integrity checking for data sharing.
A certificateless remote anonymous [15] authentication protocol proposed in this paper. Even doctors cannot disclose the private information of the patient. This approach uses an anonymous account index. Three resources used in this protocol are network manager, WBAN client and application provider (AP). The WBAN client requests for service from the application provider, the network manager manage the network and authenticity and the application provider provides the services in the network. This protocol is based on CL-PKC means Certificateless Public key cryptography. Three steps of this protocol are initialization, registration and

ISSN: 2278 – 909X

remote anonymous authentication. The Network cannot impersonate the client because it only gene rates the part of the key.

SYMMETRIC KEY BASED PROTOCOLS IN BAN

Symmetric key cryptography is preferred for the BAN because it needs some resources like memory and computation as compared with Asymmetric key cryptography. In this type both encryption and decryption is done by the same key i.e. secret key. There are various algorithms are proposed to secure BAN. The difficult part of cryptography is key management. Key generation and key distribution are two main aspects of key management. First we need to generate the key and then distribute the key over a secured channel. There are various ways to generate the key. We can also preload the keys to the sensors or generate the key from physiological values or may be combination of both. The physiological value can be heart rate, pulse rate, electrocardiography etc. A [16] security suite has been proposed for BAN which use IAM (Independent and Adaptive Key Management) and KEMESIS (Key Management Scheme for security in Inter Sensor communication), techniques for security. In these schemes, the use of a randomly generated keys are used for encryption and decryption at sender and receiver independently and there is no need of key distribution or exchange keys among sensors. There are various ways to distribute the key. The keys can be distributed to the sensors before deployment. This approach is inflexible. The keys can be distributed with the help of bio channels like Inter Pulse Interval (IPI) etc.
A security suite has been proposed for BAN which use a novel key agreement scheme that allows neighboring nodes in BAN to share a common key generated by ECG signal [7]. The IJS (Improved Jules Sudan) is proposed for message authentication. The ECG-IJS key agreement can secure data communication over BAN without any key distribution overhead. The proposed key generated form is a universally measurable physiological stimulus (ECG) that is unique and distinctive for each person. A secure and efficient Ordered Physiological Feature based Key Agreement (OPFKA) for BAN is proposed in [18]. Two sensors agree on a symmetric cryptographic key generated from the overlapping physiological signal features. In this approach there is no need of pre distribution of keys. The secret features computed from the same physiological signal at different parts of the body by sensors with some overlapping but not the same completely. The OPFKA is developed to transfer the secret features of one sensor to another such that two sensors can identify the overlapping ones. It is secure, efficient and feasible protocol. The generated features by each sensor are ordered to form feature vector. The sender sends the secret features along the noisy data to receiver. The receiver generates a key according to the common features. The sender identifies the common features in its own feature vector and computes the key accordingly. The purpose of OPFKA is enable secure inter-sensor communication in a BAN. A biometric based security [19] is proposed for data authentication within BAN. The sender's ECG feature is selected as the biometric key for data authentication in BAN. There is no possibility of Mixed up records of one patient with another patient.

HYBRID KEY BASED PROTOCOLS IN BAN

This cryptography is either a combination of both asymmetric and symmetric key or use the concept of two keys like preloaded key and master key. In [20] a hybrid security protocol for BAN is proposed to support securing communication wireless channel. This protocol has a good tradeoff between security and resource constraints. A hybrid type of key management technique [21] is proposed which is a combination of physiological values and preloaded keys. The Local Binary Pattern (LBP) used by ECG based agreement to generate common keys to be agreed upon for encryption and decryption to make the inter sensor communication more secure. The two main concepts of this approach are feature generation and key agreement. Master key is preloaded in the remote medical server of the BAN to authenticate personal server. If a personal server is compromised by an adversary, medical server revokes the existing key of personal server. Personal server is recovered by using the master secret key.

The comparison of various asymmetric, symmetric and hybrid keys approaches is shown in the table 2 below.

ASYMMETRIC KEY			
S.No	Protocol/Author	Advantages/Characteristics	Limitations
1	Jin-Meng HO [13]	Authentication protocol, use pre shared password.	Computational cost is high.
2	Rung Fan et al [14]	Secure efficient data storage approaches use orthogonal vectors.	More emphasis is given to storage than security
3	Jingwei LIU et al [15]	It is a certificateless authentication protocol and user index is used on the place of user real identity.	Very complex algorithm.
SYMMETRIC KEY			
4	Zhaoyang Zhang et al [17]	Secure data communication in plug-n-play manner without key distribution, energy efficient.	Extracted features are not unique and vault size is not optimal.
5	OPFKA [18]	Protocol is Secure, Efficient and Ordered, no pre distribution of keys are required, low computational cost, low memory storage, and low communication overhead.	Extracted features are not unique and vault size is not optimal.
6	Sofia Najwa Ramli et al [19]	ECG based Authentication Protocol, No Possibility of records mixing of two patients.	Verifies Authentication and data integrity only.
HYBRID KEY			
7	Jingwei Liu et al [20]	Uses features of both asymmetric and symmetric key and provide more secure approach.	Due to a hybrid approach it is also very complex
8	Abdulaziz Alsadhan et al [21]	Minimal time complexity key management approach	Authentication not provided Properly

Table 2: comparison of various cryptographic keys approaches.

ISSN: 2278 – 909X

We have discussed and compared various types of security techniques based on asymmetric key, symmetric key and hybrid key for BAN. There are advantages and limitations of every approach in terms of energy, complexity etc. The asymmetric key approaches are not much efficient but simple to manage and the symmetric key approaches are efficient but have much complexity to manage. The hybrid techniques combine the features of both and provide security for BAN.

IV. CONCLUSION

In this paper we have discussed various security approaches to secure Body Area Network. We have discussed many symmetric, Asymmetric and hybrid key security mechanisms in BAN. The detail comparison among these approaches is also done in this paper. Various approaches are also used to secure BAN. Further work has to be done to make it more secure and efficient network. In future there is a requirement of a protocol which is more efficient and more secure than existing protocols for Body Area Network.

REFERENCES

[1] ANN-KRISTIN KOCK. "Medical Body Area Networks, "Seminar Kommunikationsstandards in der Medizin, SS 2010.

[2] Omer Aziz, Benny Lo, Ara Darzi, And Guang-Zhong Yang. "Body Sensor Network, "EBook, 2006.

[3] Samanesh Movassaghi, Mehran Abolhasan "Wireless Body Area Networks: A Survey". IEEE COMMUNICATIONS SURVEYS & TUTORIALS, 2013.

[4] Yasmin Hovakeemian, Kshirasagar Naik "A Survey On Dependability In Body Area Networks". Medical Information & Communication Technology (ISMICT), 5th International Symposium, 2011.

[5] Min Chen, Sergio Gonzalez, Athanasios Vasilakos, Huasong Cao, Victor C. M. Leung. "Body Area Networks: A Survey". Journal Mobile Networks And Applications, 2011.

[6] Deena M. Barakah AND Muhhammad Ammad-uddin. "A Survey of Challenges and Applications of Wireless Body Area Network (WBAN) and Role of A Virtual Doctor Server in Existing Architecture," Third International Conferences on Intelligent Systems Modeling and Simulation, IEEE, 2012.

[7] S. Ullah, P. Khan, N. Ullah, S. Saleem, H. Higgins, and K. Kwak, "A review of wireless body area networks for medical applications," arXiv preprint arXiv:1001.0831, vol. abs/1001.0831, 2010.

[8] Shah Murtaza Rashid Al Masud."Study And Analysis Of Scientific Scopes, Issues And Challenges Towards Developing A
Righteous Wireless Body Area Network ", International Journal Of Soft Computing And Engineering (IJSCE), 2013.

[9] Shakeel Ahmed Shah, Syed M.K Raazi, Rahat Ali Khan."Wireless Senor Networks Health Monitoring: Trends And Challenges". Journal Of Emerging Trends in Computing and Information Sciences, 2012.

[10] H. Kwon and S. Lee, "Energy-efficient multi-hop transmission in body area networks," in 20th IEEE Int. Symp. on Personal, Indoor and Mobile Radio Commun. (PIMRC), pp. 2142 –2146, Sept. 2009.

[11] Ming Li Wenjing Lou And Kui Ren,. "Data Security And Privacy In Wireless Body Area Networks," IEEE Wireless Communications, 2010.

[12] Malan D. J., Welsh, M., Smith, M. D., "A public-key infrastructure for key distribution in tinyos based on elliptic curve
cryptography," First IEEE International Conference on Sensor and Ad Hoc Communications and Networks (SECON04),2004.

[13] Jin-Meng Ho. "A Versatile Suite of Strong Authenticated Key Agreement Protocols for Body Area Networks," IEEE,2012.

[14] Rung Fan, Ling-Di Ping, Jian-Qing Fu, Xue-Zeng Pan."The New Secure and Efficient Data Storage Approaches for
Wireless Body Area Networks," IEEE, 2010.

[15] Jingwei LIU , Zonghua ZHANG, Kyung Sup KWAK, Rung Sun. "An Efficient Certificateless Remote Anonymous Authentication Scheme for Wireless Body Area Networks", IEEE ICC 2012.

[16] Raghav V. Sampangi, Saurabh Dey, Shalini R. Urs And Srinivas Sampalli. A Security Suite For Wireless Body Area Networks," International Journal Of Network Security & Its Applications (IJNSA), Vol.4, No.1, January 2012.

[17] Zhaoyang Zhang, Honggang Wang, Athanasios V. Vasilakos, And Hua Fang "ECG-Cryptography And Authentication In Body Area Networks," IEEE Transactions On Information Technology In Biomedicine, Vol. 16, No. 6, November 2012.

[18] Chunqiang Hu, Xiuzhen Cheng, Fan Zhang, Dengyuan Wu, Xiaofeng Liao, Dechang Chen . "OPFKA: Secure and Efficient Ordered-Physiological-Feature-based Key Agreement for Wireless Body Area Networks," IEEE INFOCOM, 2013.

[19] Sofia Najwa Ramli, Rabiah Ahmad, Mohd Faizal Abdollah, Eryk Dutkiewicz. "A Biometric-based Security for Data Authentication in Wireless Body Area Network (WBAN)," ICACT, IEEE, 2013.

[20] Jingwei Liu and Kyung Sup Kwak. Hybrid Security Mechanisms for Wireless Body Area Networks," ICUFN, IEEE,2010.

[21] Abdulaziz Alsadhan and Naveed Khan. "An LBP based key management for Secure Wireless Body Area Network(WBAN)," 14th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, 2013.

Author Details:

[1]**Divya R**, *PG Scholar, Department of ECE, BannariAmman Institute of Technology, Erode, T.N, India.*

[2]**Sundararajan T V P**, *Professor, Department of ECE, BannariAmman Institute of Technology, Erode, T.N, India.*

[3]**Deepak K R**, *Assistant Professor, Department of ECE, BannariAmman Institute of Technology, Erode, T.N, India.*

[4]**Nagarajan P,** *PG Scholar, Department of ECE, BannariAmman Institute of Technology, Erode, T.N, India*

[5]**GokulPrasath Y,** *PG Scholar, Department of ECE, BannariAmman Institute of Technology, Erode, T.N, India*

ISSN: 2278 – 909X