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

Security in Body Area Network: A Survey

Ajit[1], Amita Malik[2]
[1,2]CSE Department, DCR University of Science & Technology, Murthal, Haryana, India

Abstract: Wireless Body Area Network is an Emerging field in the branch of Wireless Sensor Network for research due to its various applications in healthcare, entertainment, defense etc. In Body Area Network, sensors monitor the human's activities and actions like their health parameters so it is necessary to secure the privacy of the user and the medical information collected by the sensors from the body of the user. In this paper we discussed introduction, architecture, applications, issues, challenges and security approaches of Body Area Network. Various types of security protocols are discussed for Body Area Network and their comparison on the basis of their different types is also made.

Keywords: Asymmetric, Biometric, ECG, Hybrid, Key, Symmetric.

1. INTRODUCTION

A Body Area Network (BAN) consists of small sensors which are either attached to the body or implanted under the skin. A **Body Area Network** according to IEEE is a communication standard optimized for device of low power and operation around the human applications including medical, consumer electronics etc [1]. It means BAN uses low power sensors and used in human applications. 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.

Table 1: Comparison between WSN and BAN

WSN	BAN
In the environment	On the human body
More nodes	Less nodes
Lower accuracy	Higher accuracy
Lower security	Higher security
High power	Low power
More flexible to replace	Less flexible to replace
Not biocompatible	Biocompatible
Data loss less of an issue	Sensitive to data loss

The designing of sensor in BAN is also differs of 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. We have different types of sensors for different application in BAN. In medical field we have wearable and implantable sensors i.e. the sensors for ECG, temperature, motion, blood pressure etc.

1.1 ARCHITECTURE OF BAN

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

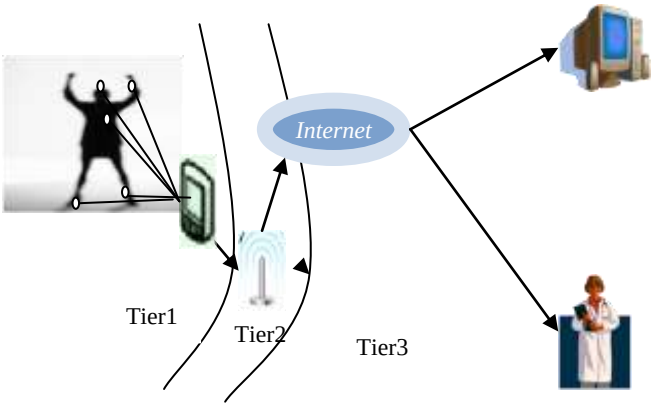

Figure 1: Architecture

a) **Tier 1 :** This tier provides 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 a network or 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.

1.2 APPLICATIONS OF BAN

There are various applications of body area network [5]. Their applications are like in healthcare [6], Entertainment etc. In all it can be said that BAN has only one application of monitoring. It monitors the activities of a person. Some applications of BAN are following:

There are various applications of body area network. Their applications are in healthcare, Entertainment etc. In all it can be said that BAN has only one application of monitoring. It monitors the activities of a person.

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 his BP, heart rate etc.
d) **Defense :** BAN monitors soldiers in defense services.
e) **Lifestyle** : BAN is also useful in emotion detection and posture detection.
f) **Assistance to disable person :** The BAN can also be useful for the person with disabilities like blindness, speech disability etc.

Rest of this paper is organized as follows: Section 2 outlines the issues and challenges followed by section 3, which include the security protocols of different types. Section 4 concludes the paper.

2. ISSUES AND CHALLENGES OF BAN

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

a) **Energy Constraint :** This network is battery oriented. We have to use 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 :** As comparable to WSN, we have to take size of node small. It is a challenge to make a node as small as possible.
d) **Sensor Effect on Body :** There is risk of irritation or allergy on the body after sensor implantation.
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 the body area network [11]. The information the network is so much critical. If security of a network is not handled properly it may life threatening. Some security 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.

3. SECURITY IN BAN

The security is the main challenge of the Body Area Network (BAN). Our main focus of this paper is to discuss various security problems and solutions to secure Body Area Network (BAN). There are various security solutions which are used for Wireless Sensor Network (WSN) but these solutions are not applicable to Body Area Network because of 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. Each area itself is a research issue. As we discussed above BAN has three tiers architecture so there are different security requirement for each tier. In tier 1, the security is to be on the sensors and their communication to each other and to Personal Digital Assistant (PDA) or smart phone. In tier 2 and 3 the security is provide on the communication from PDA to the medical server through internet. The security solutions on tier 1 should be lightweight because of the constraint on the sensors because these are energy constraints. But security on PDA and medical server may not be lightweight because they are not constraint to energy. The data which sense by the sensors of BAN is critical so we need to encrypt the data with the help of security key. The security key may be symmetric, asymmetric or hybrid.

3.1 ASYMMETRIC KEY BASED PROTOCOLS IN BAN

This is also called Public key cryptography. In this type of cryptography there are two keys private key and public key. The private key is secret and known to that particular sensor but public key is known to all. Encryption is done by the public key and the decryption is done by secret key. So, it is not required to send the keys securely. There are various algorithms which use public key cryptography to secure BAN. RSA and Elliptic Curve Cryptography (ECC) [12] are two well known algorithms which use public key cryptography. This type of cryptography is not good for BAN because it requires more memory and is computationally expensive. 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 rather than the real identity of the patient. Three participant 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 remote anonymous authentication. The Network cannot impersonate the client because it only gene rates the part of the key. An authentication protocol is proposed to access the information of sensors by smart phone or PDA [16]. It is efficient and lightweight certificateless authentication protocol for Body Area Network. Anonymity, mutual authentication and non- reputation are provided by this protocol. Three entities server, user and BNC (BAN Coordinator) are used.

The server generates the key for the network, user who want to access the BAN or request biological information from BNC. The server initializes the system and publishes the various system parameters like security, groups, hash functions etc. The user if want to access BNC need to register on the server. BNC first validate the user and then response with the requested information. Mutual authentication will be achieved between user and BNC. The comparison of various asymmetric key based approaches is shown in table 2 below.

Table 2: Comparison among various asymmetric key based approaches

S. No	Protocol/Author	Advantages/Characterstics	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 approach 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.
4	Lu Zhang et al [16]	Certificateless, Anonymous, Mutual Authentication and Lightweight authentication protocol, It provide authentication for user to access BNC.	The algorithm is very complex, need to simplify to get better performance and better computational complexity

3.2 SYMMETRIC KEY BASED PROTOCOLS IN BAN

Symmetric key cryptography is preferred for the BAN because it needs fewer resources like memory and computation as compared to Asymmetric key cryptography. In this type both encryption and decryption is done by the same key i.e. secret key. There are various algorithms which use this technique to secure BAN. Most of the research work has been done in this type and here also discussed various papers which use this technique. 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 preloaded and physiological value. The physiological value can be heart rate, pulse rate, electrocardiography etc. In [17] a 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. The schemes use the concept of using multiple reference frames, the existing distinction in physiological value between people and periodic refreshes of such reference frames to achieve independent generation of keys at the both sender and receiver. 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. The work has been done in this area and most of the work is to be done.

A biometric approach proposed [18] for authentication and for distribution of key in Body Area Network. Inter Pulse Interval (IPI) used as biometric trait in this paper. This technique uses symmetric key distribution for security purposes. At the transmission end the biometric trait used to send the key and at the receiving end the other sensor would capture its own copy of the trait and use it to get the key. IPI can be obtained from different physiological signal like ECG, PPG etc, heart rate etc. and measured at different parts of body like chest, fingertips and lower limbs etc. This approach ensures authenticity, confidentiality and integrity of data transmission between the master node and all the other sensors. A Plethysmogram (PPG) based technique [19] proposed to allow a common key in BAN. The sensors which want to securely communicate, measures the PPG signal for predefined duration of time. One of the two sensors generates an arbitrary key. The key hidden by using features derived from measured PPG signal. The hidden key is communicated to other nodes which uses their own features to un-hide that key. The key hiding and unhiding is based on fuzzy vault cryptographic primitive. The purpose of PKA (PPG based key Agreement) is to enable two sensors to obtain a common symmetric key, using PPG signal. The PPG signal is used to know volumetric change in the arteries. It can be measure by a pulse oximeter which can be attached to the finger. Two steps physiological feature generation and PPG based key agreement are used to key agreement.

The distributed key management technique BARI [20] proposed which use biometrics for key management in Body Area Network. It supports the use of biometric measurements as symmetric keys. The personal server issues new key refreshment schedule periodically. Each sensor refreshes the key in the slot allotted to them. Three types of keys are used in the scheme are communication key, administrative key and Basic key. The communication key is a network wide key and managed by personal server. The administrative key us used to refresh communication key and shared by multiple sensors. The Basic key is used to refresh administrative key when compromised and each sensor has its basic key. This technique maintains confidentiality, authenticity and integrity besides it routing is also secure with the help of communication key. A key management scheme [21] which use ECG signal for security in Body Area Network has proposed. This approach generates and distribute symmetric cryptographic key and protect the privacy of user. This protocol work in four steps which are key generation phase, key set up phase, key authentication and key update phase.

A highly flexible authentication and key establishment protocol based on ECG signal and fuzzy commitment is proposed in [22]. It provides long, random and distinctive keys. The fuzzy commitment can tolerate the high degree of noise in ECG signal. This protocol works by combining ECG signal and fuzzy commitment. In this technique symmetric key is used and there is no need of distribution of keys between sensors. A lightweight scheme for secure association of sensors and key management [23] in BAN is proposed. A group of sensor nodes establish initial trust through group device pairing (GDP), which is an authentication group key agreement protocol. Various kinds of secret keys can be generated on demand after deployment. Each device authenticates itself to the whole group as a legitimate member which is verified by a human. It based on symmetric key cryptography and there is no need of public key infrastructure, additional hardware and interface on sensors. A novel key agreement scheme that allows neighboring nodes in BAN to share a common key generated by ECG signal is proposed [24]. 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 [25]. 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 [26] 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. The comparison of various symmetric keys approaches is shown in the table 3 below.

Table 3: Comparison among various symmetric key based approaches

S. No	Protocol/Author	Advantages/Characterstics	Limitations
1	Carmen C. Y. et al.[18]	Provide Authenticity, Confidentiality, Integrity and uses biometric trait IPI	IPI cannot sense by some sensors like motion sensors so extra sensors required
2	Krishna K. Venkatasubramania n et al.[19]	Specially used for Soldiers, No need of initialization or set up between two sensors	Use Fuzzy vault scheme and complicated to implement on hardware
3	BARI [20]	Distributed key management protocol, besides confidentiality, authenticity, integrity also secure routing	Computation cost may be high because of using three types of key
4	Mohammed Mana et al[21]	Control Replaying, Secure Communication link, Efficient and Energy saving	Four phases makes its very complicated
5	ESKE [22]	Long, Random, Low Latency, Distinctive and Temporal variant keys, fuzzy commitment tolerate high degree of noise	Not applicable for replaying and non reputation attacks
6	Ming Li et al. [23]	Group pairing keys, No addition hardware required, it is efficient in both communication and computation	Key Management is a difficult task in Group Device Pairing
7	Zhaoyang Zhang et al[24]	Secure data communication in plug – n- play manner without key distribution, Energy efficient	Extracted features are not unique and vault size is not optimal
8	OPFKA [25]	Protocol is Secure, Efficient and Ordered, No pre distribution of keys are required, low computational cost, low memory storage, and low communication overhead	If the sending features are not matching with receiver signal then it may create problem of key establishment.
9	Sofia Najwa Ramli et al [26]	ECG based Authentication Protocol, No Possibility of records mixing of two patients	Verifies Authentication and data integrity only

3.3 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 [27] 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 [28] 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 intersensor 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 hybrid keys approaches is shown in the table 4 below.

Table 4: Comparison among various hybrid key based approaches

S. No	Protocol/Author	Advantages/Characterstics	Limitations
1	Jingwei Liu et al. [27]	Uses features of both asymmetric and symmetric key and provide more secure approach	Due to a hybrid approach it is also very complex
2	Abdulaziz Alsadhan et al. [28]	Minimal time complexity key management approach	Authentication not provided properly

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.

CONCLUSION AND FUTURE WORK

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. Although various approaches are used to secure BAN yet more 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]. Samaneh 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 Muhammad 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 Conference 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]. Lu Zhang, Jingwei Liu And Rung Sun."An Efficient And Light Weight Certificateless Authentication Protocol For Wireless Body Area". 5th International Conference On Intelligent Networking And Collaborative Systems, IEEE, 2013.
[17]. 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.
[18]. Carmen C. Y. Poon, Yuan-Ting Zhang, Shu-Di Bao "A Novel Biometrics Method To Secure wireless Body Area Sensor Networks For Telemedicine And M-Health," IEEE Communications Magazine ,April 2006.
[19]. Krishna K. Venkatasubramanian, Ayan BANerjee and Sandeep K. S. Gupta. " Plethysmogram-based Secure Inter-Sensor Communication in Body Area Networks", IEEE, 2008.
[20]. Syed Muhammad Khaliq-Ur-Rahman Raazi, Heejo Lee. "Bari: A Distributed Key Management Approach For wireless Body Area Networks," International Conference On Computational Intelligence And Security, IEEE, 2009.
[21]. Mohammed Mana, Mohammed Feham And Boucif Amar Bensaber. "Trust Key Management Scheme For Wireless Body Area Networks," International Journal Of Network Security, 2011.
[22]. Lin Yao, Bing Liu, Kai Yao, Guowei Wu, Jia Wang. "An ECG-Based Signal Key Establishment Protocol In Body Area Network," Symposia And Workshops On Ubiquitous, Autonomic And Trusted Computing, IEEE, 2010.
[23]. Ming Li, Shucheng Yu,Wenjing Lou and Kui Ren. "Group Device Pairing based Secure Sensor Association and Key Management for Body Area Networks," IEEE INFOCOM 2010.
[24]. 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.
[25]. 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.
[26]. 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.
[27]. Jingwei Liu and Kyung Sup Kwak. Hybrid Security Mechanisms for Wireless Body Area Networks," ICUFN, IEEE, 2010.
[28]. 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.