Protocol Design Issues in Implementing Security for Wireless Body Area Network

Ms. Sanchari Saha, Mr. Dinesh K Anvekar

***Abstract*— Recent technical advancements in low-power integrated circuits, ultra low-power RF (radio frequency) technology, wireless communications and micro sensors allowed the realization of Wireless Body Area Networks (WBANs). It is one of the latest technologies in health care diagnosis and management. The data of a person's vital body parameters and movements are collected by small wearable or implantable sensors and communicated using short-range wireless communication techniques. The main concern is to secure the data collected from WBAN. There are two important data security issues namely secure and dependable distributed data storage and fine grained distributed data access control for sensitive and private data. In this paper 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**

***Index Terms*— Security protocol, WBAN, WSN, Symmetric Key, Asymmetric Key, Hybrid Key.**

I. INTRODUCTION

Wireless body area network has emerged as a new technology for mobile health monitoring. WBAN operates in close vicinity to, on, or inside a human body and supports a variety of medical and non-medical applications. Basically, WBAN may be a communication network between the humans and computers through wearable Devices. So as to appreciate communication between these devices, techniques from Wireless Sensor Network and ad hoc networks may be used. A typical device node in WBAN ought to make sure the accurate sensing of the signal from the body, do low-level process of the sensor signal and wirelessly transmit the processed signal to an area process unit [2]. However, attributable to the everyday properties of a WBAN, current protocols designed for these networks don't seem to be forever compatible to support a WBAN.

WBAN 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 WBAN 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	WBAN
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: WSN & WBAN comparison

II. APPLICATIONS OF WBAN

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

a) Healthcare: WBAN 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. The opportunities for using BANs in the military are numerous. Some of the military applications for WBANs include monitoring health, location, temperature and hydration levels. A battle dress uniform integrated with a WBAN may become a wearable electronic network that connects devices such as life support sensors, cameras, RF and personal PDAs, health monitoring GPS, and transports data to and from the soldier's wearable computer. The network could perform functions such as chemical detection, identification to prevent casualties from friendly fire and monitoring of a soldier's physiological condition. Calling for support, his radio sends and receives signals with an antenna blended into his uniform. As a result, WBANs provide new opportunities for battlefield lethality and survivability

e) Lifestyle: WBAN is also useful in emotion and posture detection.

Manuscript received December 23, 2014.

Sanchari Saha, Associate Professor, Department of CSE, MVJCE, Bangalore, India.

Dr. Dinesh K Anvekar, HOD & Professor, Department of CSE, NMIT, Bangalore, India.

f) Assistance to disable person: The WBAN can also be useful for the person with disabilities like blindness, speech disability etc.

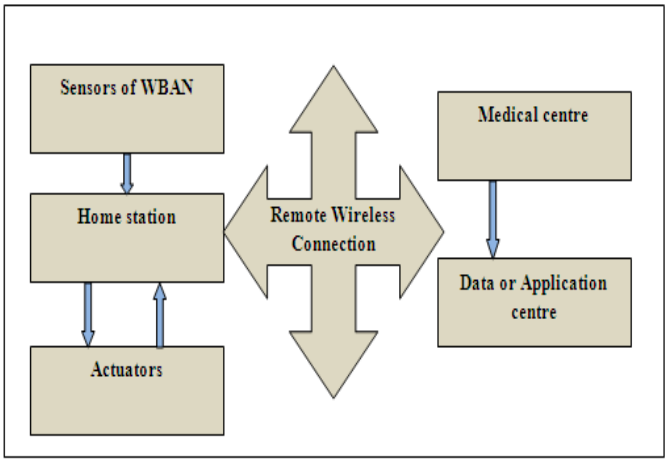

Figure1: WBAN data flow

III. Security Needs

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

The security solutions which are used for WSN are not applicable to WBAN 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 have discussed above that WBAN 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.

IV. Different Security Protocol Design Issues

A) Asymmetric key based protocols in WBAN

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 algorithms 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 WBAN.

B) Symmetric key based protocols in WBAN

Symmetric key cryptography is preferred for the WBAN 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 WBAN. 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.

C) Hybrid key based protocols in WBAN

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 [16] a hybrid security protocol for WBAN 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 [16] 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 WBAN 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

V. Comparison of different Security protocols

Security mechanisms are processes that are used to detect, prevent and endure security attacks. This sub-section discusses the problems regarding existing security mechanisms, as follows:

1) Cryptography

As wireless body area sensor networks alter sensitive physiological info, sturdy cryptographic functions are unit preponderating necessities for developing any secure attention application. These cryptographic functions give patient privacy and security against several malicious attacks.. Further, the selection of cryptography system depends on the computation and communication capability of the sensor nodes. Some argue that asymmetric crypto systems are

typically too high-priced for medical sensors and interchangeable crypto systems don't seem to be versatile enough [14].

2) Key Management

Key management protocols are measure basic necessities to develop a secure application. These protocols are used to set up and distribute varied forms of cryptographic keys to nodes within the network. Generally, there are three styles of key management protocols, namely, trusty server, key pre-distribution and self imposing [15].

3) Secure Routing

In home care or disaster eventualities sensor devices might require sending their data to alternative devices outside their immediate radio vary [16]. Therefore, routing and message forwarding could be a crucial service for end-to-end communication. So far, several of routing protocols are projected for sensor networks; however none of them are designed with strong security as a goal. Karlof-Wagner mentioned the actual fact that routing protocols suffer from several security vulnerabilities, like associate degree offender may launch denial-of-service attacks on the routing protocol.

4) Resilience to Node Capture

Resilience against node capture is one in all the foremost difficult issues in sensor networks. In real time healthcare applications, the medical sensors are placed on a patient's body, whereas, the environmental sensors are placed on hospital premises (e.g., ward room, operation area etc.) which can be simply accessible to attackers. Thus, an attacker might be able to capture a sensor node, get its cryptanalytic info and alter the sensor programming consequently. Later, he/she will place the compromised node into the network, which may endanger application success [16].The current cryptographic functions (i.e., node authentication and identification) might discover and defend against node compromised attacks to a point, however these compromised node attacks can't be detected instantly [17] that could be a massive issue for healthcare application..

5) Trust Management

Trust signifies the mutual association of any two trustworthy nodes (i.e., sensor node and information aggregator node), that are sharing their data. In [15] trust is outlined as "the degree to that a node ought to be trustworthy, secure, or reliable throughout any interaction with the node". Boukerche-Ren [13], evaluated the trust for mobile healthcare system.

6) Secure Localization WBANs facilitate mobility **for** patient's comfort, thus patient location estimations are required for the success of healthcare applications. Since, medical sensors' sense physiological information of a personal, they additionally ought to report the patient's location to a far off server. As a result, medical sensors need to remember of patient location, i.e., referred to as localization. In [17] the authors mentioned localization systems that were divided into: distance/angle estimation, position computation and localization algorithms, and more, they mentioned attacks on localization system.

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 different Security protocols

VI. CONCLUSION

In this paper various key aspects of WBAN including sensors used, application areas, technologies and standards, protocols, are outlined. There are many challenges that still need to be addressed, especially on high bandwidth and energy efficient communication protocols, interoperability between WBANs and other wireless technologies, and the design of successful applications. Future work will be concentrating on the design of a context aware mechanism which will carefully optimize security, safety and usability.

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 Ammaduddin. "A Survey of Challenges and Applications of Wireless Body Area Network (WBAN) and Role of A Virtual Doctor Server in Existing Architecture," Third International C onferences 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/1001.08 31, 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 Ahme d 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 multihop transmission in body area networks,‖ in 20th IEEE Int. Symp. on Personal, Indoor and Mobile Radio Communication. (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] J in 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 Netwo rks,‖ 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 Sr inivas Sampalli. A Security Suite For Wireless Body Area Networks,‖ International Journal Of Network Security & Its Applications (IJNSA), Vol.4, No.1, January 2012.
[17] 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

Sanchari Saha holds a Master of Engineering degree from CMRIT (VTU), Bangalore, and Bachelor of Engineering degree from NIT, Agartala. Currently, she is working as an Associate Professor in MVJCE, Bangalore, and also pursuing research work towards her PhD degree. She has published a text book titled "Object Oriented Modeling & Design pattern" which has been prescribed under VTU syllabus upon recommendation by VTU Vice Chancellor. She has published total 21 papers in reputed national & international journals and conferences. She has received gold medal from VTU for securing 1st rank during her Master's degree. She is a member of Indian Society for Technical Education.

Dr. Dinesh Anvekar is currently working as Head and Professor of Computer Science and Engineering at Nitte Meenakshi Institute of Technology (NMIT). He worked as Director Entrepreneurship and Professor of Computer Science at CMRIT. He obtained his Bachelor degree from University of Visvesvaraya college of Engineering. He received his Master and Ph.D degree from Indian Institute of Technology. He received best Ph. D Thesis Award of Indian Institute of Science. He has completed two Nokia sponsored projects in Indian Institute of Science during 1997-1998. He has 15 US patents issued for work done in IBM Solutions Research Center during 1998-99, Bell Labs during 1993-94, and Lotus Interworks during 2000-04, and for Nokia Research Center, Finland. He has authored one book and over 55 technical papers. He has received Invention Report Awards from Nokia Research Center, Finland, Lucent Technologies (Bell Labs) Award for paper contribution to Bell Labs Technical Journal and KAAS Young Scientist Award in Karnataka State, India. He is a Fellow of IETE and Senior Member of IEEE. He has supervised over 40 undergraduate and graduate engineering projects and research students in the Indian Institute of Science.