An enhanced mutual authentication with secure user anonymity for two tier wireless body area network

Muhammad Furqan*, Asim Zeb†, Muhammad Naeem†, Muhammad Imran Khan†, Aamer Khan†, Ishtiak Al Mamoon‡

Abstract

When multipurpose and specially vital signs wearable sensory devices emerged as the new development field, WBAN (Wireless Body Area Networks) dawned, which was a point of interest for saftey care for intense care patients. As wireless body area networks uses wireless channel for data collection and transmission, which contains patient's sensitive information. Due to this new challenge, need of light-weight design of security protocols for this new technology is the need of the day. Recently a light-weight intialization / authentication protocol for it is presented which needs enhanced security with less computational cost. Therefore, some areas needed to be identified and incoorporated in this protocol to make it more efficient and strong. Inspite of equivalent cost the compared results are showed for the improved proposed protocol which clearly depicts the enhanced security by introducing usage of timestamp and Diffie–Hellman algorithm for authentication. Broadly accepted Burrows Abadi Needham logic is used to analyze the security of proposed protocol.

Keywords: Wearable-sensor, Body-area-networks, light-weight-Protocol, IOT, Sensors, Security.

Introduction

A body area network is properly defined by IEEE 802.15 as, "an optimized standard communication for light weight devices and process within and around the human body and others to provide range of applications mostly includes field like health care, utility electronics, military and other"(Toorani, 2015).

WBAN emerged as the new era of technologies designed for remotely keeping an eye on patient's health obtaining specific information with the help of sensors attached or implanted in the body. Mainly the devices that comprise WBAN are actuators and sensor nodes. The sensor nodes can work easily on or within the body of a person to compute certain body indicator parameters e.g. ECG, movements, thermal signatures, blood pressure, heart beat etc. (Karulf, 2008).

* Department of Physical and Numerical Sciences, Qurtuba University of Science and Information Technology, Peshawar, Pakistan. asimzeb1@gmail.com, onlyfurqan@gmail.com

† Department of Computer Science, Abbottabad University of Science and Technology, Havelian, Abbottabad, Pakistan.

‡ ECE Department, Presidency University Bangladesh, ishtiakm@pu.edu.bd

Design of specific sensors or nodes is for the particular purpose according to the requirements of users e.g. ECG sensor, heart rate level sensor etc. As far as network is concerned WBAN has the following three types of nodes:

i. Coordinator: This is the node which works like an access to the outer domain / world or any corresponding other WBAN, also known as controller node.
ii. End Nodes: These nodes are for specific functions according to the application for which they are used. End nodes do not have sending messages capability.
iii. Relay: These nodes are for joining nodes and act as the relays. They are comprising of parent / child nodes and relay messages.

Standard such as IEEE 802.15.6 based for WBAN, is designed for describing standards for close range, using less power and extremely steady wireless transmission of data with the capability to support various communication data rates for respective applications. Moreover, this standard makes sure the discretion, integrity, authentication, privacy protection, and security in the replays. There are three security levels which have to must adopt by the all the nodes and the hubs:

- Communication without Security – Level 0.
- Without Encryption Authentication – Level 1.
- With Encryption Authentication – Level 2.

When security of a certain process is concern, a hub along-with node jointly need to adopt or choose one of these levels relevant to the security level needed (Toorani, 2015). WBAN medical applications have produced many benefits but also brought some challenges to this sector. The main benefit in nut shell is the remote monitoring without any limitations. Privacy and security are considered as the main challenges on the other hand such that their hazards can make at risk the privacy of the patient making his/her life more miserable. The kind of data WBANs are dealing with is usually personal and private.

If the appropriate security measures are not taken, then this can lead to patient's humiliation, wrong treatments; often leading to death, relationship issues and loss of job or medical insurance. Therefore, it's a primary task to provide security and privacy to this kind of data. Following short range and precise security mechanisms are compulsory for integrity, secure group management, privacy, authentication and

authorization (Al-Janabi, Al-Shourbaji, Shojafar, & Shamshirband, 2017).

Before going in detail of the mechanism related to security to be set up in a WBAN, first knowing the WBAN architecture's communication within, with outside world and with other related WBANs is needed. Fig. 1 shows the different devices with respect to the location of the device for certain application (Chatterjee, Das, & Sing, 2014).

Location of sensors in WBANs cannot be classified as a fixed because the body continuously changes the position. Mostly WBANs system is consists of the following three separate levels for communication, (Al-Janabi et al., 2017):

i. Nodes present on or within the body known as intra-BAN communications,
ii. Between two bodies known as inter-BAN communications, and
iii. Between body nodes and remote server known as beyond-BAN communications.

According to this architecture, tier1 is bound to the sensors or nodes present on or within body. Tier2 related to the communication of some patients or related devices via medium like Bluetooth, infrared etc. Tier3 is the connectivity of tier1 and tier2 with the outside world via internet.

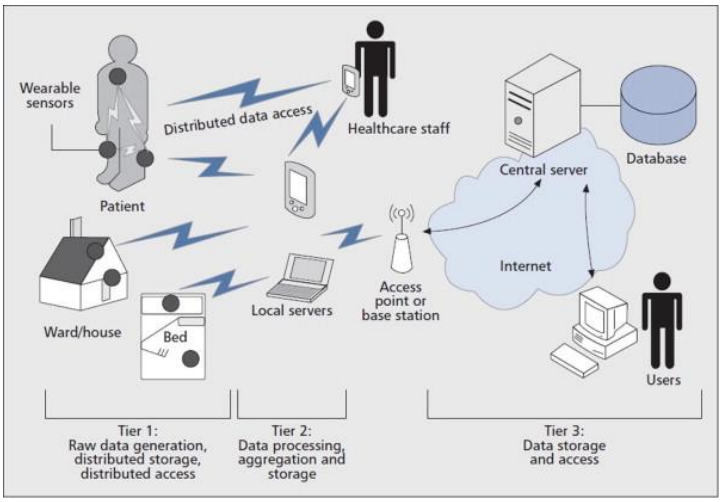

Fig1: Communication tiers in a WBAN

As information is shared about the patient's sensitive and private data in WBAN therefore, there are some security threats which are prone to such communication.

Literature Review

The other key areas in this regard are the energy efficiency and low computational cost with maximum functionality. Another algorithm, namely good neighbor was presented for WBAN's authentication in (Cai, Zeng, Chen, & Mohapatra, 2011). But due to unrealistic assumptions, that proposal's implementation is questionable. (Shi, Li, Yu, & Yuan, 2013) proposed a channel characteristics scheme for authentication which is based on non-cryptographic mechanisms very useful for small scale security level only. Recently basic cryptographic hash functions and symmetric cryptosystems are used for efficiency and lightweight (Gupta, Tripathi, & Sharma, 2020).

(Liu, Zhang, & Sun, 2016) presented anonymous based on comparatively low computational cost protocol which uses 1-step authentication. However, their protocol is improved by (X. Li et al., 2017) by dealing with the threats like DoS attack, verifier stolen information attack, key capturing attacking by impersonating the certificate less sign cryption's security protocol for data communication between BAN and server is presented in (F. Li & Hong, 2016). (Xiong, 2014) presented a CLPKC (certificate less public key cryptography), which is mainly used for verification.

(He, Zeadally, Kumar, & Lee, 2017) also used the same CLPKC but for WBANs. A group of verification and key-administration conventions based on hash-chains / ECC for boycott to realize shared confirmation along with secure transmission, the devices related to control data of patient and health experts is presented in (Shen et al., 2015). A lightweight key administration convention to set up an overall secure medium for an asset restricted hub along with farther substance regarding participation is proposed in (Abdmeziem & Tandjaoui, 2015). The main idea is to get rid of asset devouring security measures from the obliged hub to effective 3rd parties. Cryptographic key is used for security authentication.

Proposed Methodology

As four different attacks are described, therefore four different strategies are taken into consideration to solve the research problem. DoS attack has many gateways and variation but in order to improve the existing solution the involvement of extra database retrieval will be

avoided for initialization and authentication phase. New enhancement will filter the unauthorized requests and ban them from even penetrating the network. Same approach will also solve the problem of attack of stolen mobile device in order to have dual check.

The proposed idea for sensor node capture attack is to make it strong by including other parameters like time stamp, temporary id generation along with one time produced random number during authentication and linkage phase. Detail methodology's glimpses are presented below:

Insider attack is a malevolent attack carried by authorized person on a network or computer system. Moreover, these kinds of attacks are underrated because of less importance instead of external attacks. Therefore, by avoiding storing password or keys in external database which can be misuse by third party, this less preference given attack can be deal with.

In order to improve user authentication phase powered by resistance of various attacks and to compare the efficiency of the results, the properties regarding security of proposed protocol will be explained in detail, along with the proof by using broadly accepted BAN logic. The protocol presented will use the simple cryptographic primitives where Diffie–Hellman Algorithm will be used to bring simple but very strong cryptographic approach.

System Model

Network and threat models used for the proposed protocol are described below:

Network Model:

The IEEE 802.15.6 designed to define the WBAN communication standard based on star topology, where both sender (node/hub) and receiver (node/hub) use relay node. All this is mainly based on body / node movements.

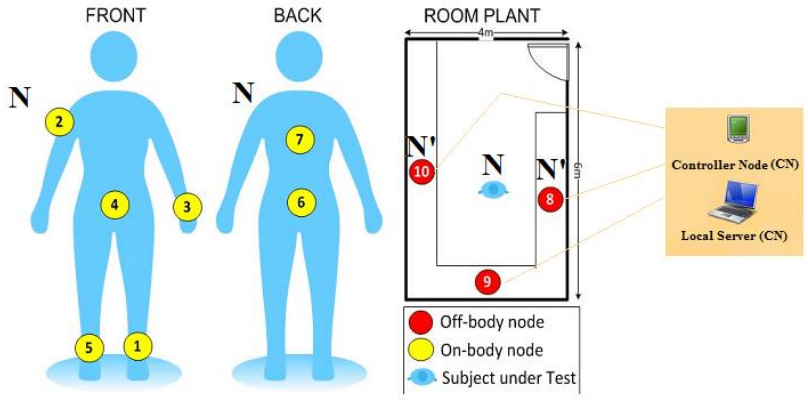

Fig 2: Domain of WBAN according to IEEE 802.15.6

Special purpose hand-held devices or modern smart phone or PC could be act like a hub. That's why the node used to be control should be better than the nodes which are used to sense and send data. Either the node will generate or start the data while other node can be used as relaying the data. The first node will be act like a secondary and the later as a primary. Now combination of primary and the hub is 2nd tier and the combination of secondary and the hub is 1st Tier setup.

Therefore, relation Controlling-Node (C-N) ← → Primary-Node (N) ← → Secondary-Node (N′) is the 2 – jump link between the secondary N′ node and the hub. As hub is attached with primary nodes, this is considered as the 2-tier architecture. Similarly in 2nd tier the corresponding primary and secondary nodes are interconnected.(Ibrahim, Kumari, Das, Wazid, & Odelu, 2016)

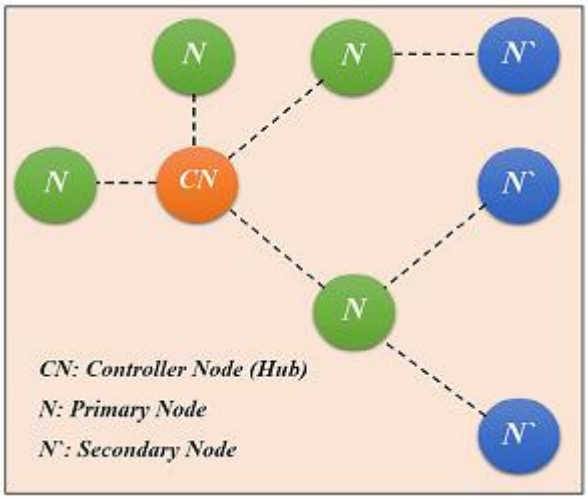

Fig 3: Types of Nodes

Threat Model

Following are basic features of the threats considered in its formation (Ibrahim et al., 2016):

- The node used to be act like a controller trusted and free of being compromised.
- The attacker can overhear all data transmission and can penetrate and play with the transmission.
- Due to barrier of expensiveness interference of the sensors on hardware level is not fortified which can lead to loss or theft of data.
- Considering WBAN's threat model as Dolev Yao model which represents an adversary who can eavesdrop, interfere or recreate data transmission channel in the network. It can only be stopped by measures taken by fundamentals of cryptography (Ibrahim et al., 2016).

Architecture of WBAN

Nowadays WBAN's icon is wearable sensory devices, using for multi purposes; ranging from health care applications to sports and warfare domain. In order to explain its architecture, there are three things should be kept in mind i.e. User (U), Network Manager (NM) and Application Server (AS). As in this study medical infrastructure is considered in mine therefore all discussion will circle around patient data transmission and safety (Xiong, 2014).

- U → It can be a patient or generally the user who use or wear the WBAN device.
- NM →: The NM is responsible for registering and authorizing.
- AS →: its authorized by NM which gives out related medical facility to the WBAN's user.

Network manager uses insecure channel and mutually authenticate based on pre-distributed parameters. Upon authentication on the side application server, network manager shared encrypted session key to swap sensitive information with medical service suppliers. Following picture describes it well. (Xiong, 2014)

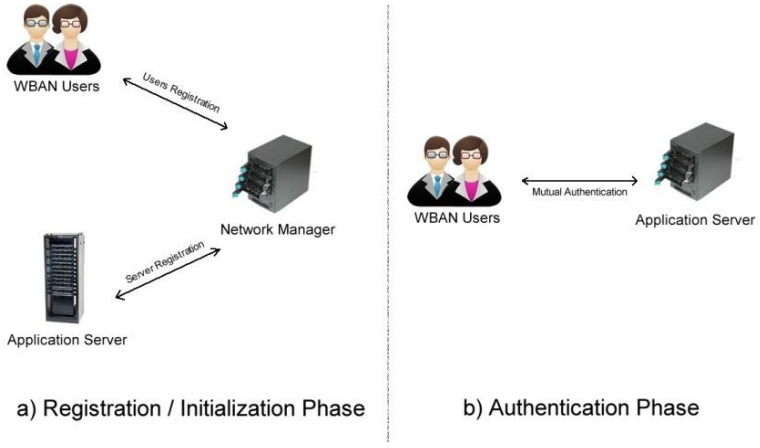

Fig 4: General processes of WBAN's authentication

Conclusion

Confidentiality and mutual authentication services are essential for WBANs. Therefore, the transmission needs be anonymous and un-linkable as well. By this study the some of the threats like DoS, sensor node capture attack, insider attack and the stolen mobile device attack are successfully incorporated in the existence scheme and verified by BAN logic. Generating own power will be the solution to the energy efficiency and for privacy / security new techniques or merging of different techniques would be the solution. But in such conditions the computational and time elapse factor should be kept in mind. Therefore, deffie helman's algorithm was used for low cost computational factor.

As far as medical data is concerned the primary goal is reliability and security of data. The sensor nodes should be able to transmit the medical data in a reliable and secure method. Therefore, using of timestamp and simple password technique were the other improvements made in the existing work.

References

Abdmeziem, M. R., & Tandjaoui, D. (2015). An end-to-end secure key management protocol for e-health applications. *Computers & Electrical Engineering, 44*, 184-197.

Al-Janabi, S., Al-Shourbaji, I., Shojafar, M., & Shamshirband, S. (2017). Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. *Egyptian Informatics Journal, 18*(2), 113-122.

Cai, L., Zeng, K., Chen, H., & Mohapatra, P. (2011). Good Neighbor: Ad-Hoc Authentication of Nearby Wireless Devices by Multiple Antenna Diversity. *NDSS Symposium*.

Chatterjee, S., Das, A. K., & Sing, J. K. (2014). A novel and efficient user access control scheme for wireless body area sensor networks. *Journal of King Saud University-Computer and Information Sciences, 26*(2), 181-201.

Gupta, A., Tripathi, M., & Sharma, A. (2020). A provably secure and efficient anonymous mutual authentication and key agreement protocol for wearable devices in WBAN. *Computer Communications, 160*, 311-325.

He, D., Zeadally, S., Kumar, N., & Lee, J.-H. (2017). Anonymous authentication for wireless body area networks with provable security. *IEEE Systems Journal, 11*(4), 2590-2601.

Ibrahim, M. H., Kumari, S., Das, A. K., Wazid, M., & Odelu, V. (2016). Secure anonymous mutual authentication for star two-tier wireless body area networks. *Computer methods and programs in biomedicine, 135*, 37-50.

Karulf, E. (2008). Body area networks (ban). *A survey paper written under guidance of Prof. Raj Jain*.

Li, F., & Hong, J. (2016). Efficient certificateless access control for wireless body area networks. *IEEE sensors journal, 16*(13), 5389-5396.

Li, X., Peng, J., Kumari, S., Wu, F., Karuppiah, M., & Choo, K.-K. R. (2017). An enhanced 1-round authentication protocol for wireless body area networks with user anonymity. *Computers & Electrical Engineering, 61*, 238-249.

Liu, J., Zhang, L., & Sun, R. (2016). 1-RAAP: An efficient 1-round anonymous authentication protocol for wireless body area networks. *Sensors, 16*(5), 728.

Shen, J., Tan, H., Moh, S., Chung, I., Liu, Q., & Sun, X. (2015). Enhanced secure sensor association and key management in wireless body area networks. *Journal of Communications and Networks, 17*(5), 453-462.

Shi, L., Li, M., Yu, S., & Yuan, J. (2013). BANA: body area network authentication exploiting channel characteristics. *IEEE Journal on selected Areas in Communications, 31*(9), 1803-1816.

Toorani, M. (2015). *On vulnerabilities of the security association in the IEEE 802.15. 6 standard.* Paper presented at the International Conference on Financial Cryptography and Data Security.

Xiong, H. (2014). Cost-effective scalable and anonymous certificateless remote authentication protocol. *IEEE Transactions on Information Forensics and Security, 9*(12), 2327-2339.