A SURVEY ON SECURITY ISSUES AND WEARABLE SENSORS IN WIRELESS BODY AREA NETWORK FOR HEALTHCARE SYSTEM

IBRAHIM ABDULAI SAWANEH[1], IBRAHIM SANKOH[2], DAVID KANUME KOROMA[3]

[1]Department of Computer Science Director of Academic Affairs - Institute of Advanced Management and technology-Sierra Leone
[2]Department of Networking & Telecommunication Head of Department - Institute of Advanced Management and technology-Sierra Leone
[3]Department of Mining & Petroleum Management Vice Principal - Institute of Advanced Management and technology-Sierra Leone
E-MAIL: ciddiisawaneh@yahoo.com/ciddiisawaneh@iamtech.edu.sl, Ibrahimsankoh2006@yahoo.com, Ibrahimsankoh2006@yahoo.com

Abstract:

Several works have been done in recently geared towards improving and maintaining the aging world population from chronic diseases due to our numerous activities. Researchers actively working in various fields (medical, academic, military, and industry). This survey report focuses on developing and implementing wireless body area network technology (WBAN) in healthcare systems. Body area network (BAN) technology establishes a system which monitors patient health status using tiny wireless sensors devices placed in or around the human body that aids medical professionals, and the patients with easy and convenience of operation and mobility. However, this technology faces peculiar challenges in designing and implementing, such as security vital for any system, privacy concern for everybody because it holds our data and must maintain high secrecy, power failure, sensor validation versus system compatibility, data consistency, cost and many others. Moreover, the survey suggests ways to improve and maintain the dependability of WBAN.

Keywords:

Wireless Body Area Network; Body Sensor Network; ECC; DES; BNC

1. Introduction

The field of computer science nowadays has become an attractive discipline with the advent of big data "extremely large data sets that may be analyzed computationally to reveal patterns, trends, and associations, including human behavior and interactions".

The increase in human population with diverse needs posed numerous problems as results of man's persistent interference with nature leading to chronic diseases, increase healthcare cost, less trained and qualified medical personnel in third world nations like Sierra Leone prompting researchers to find an alternative measure that will withstand those challenges as opposed by the traditional systems.

BAN is a communication platform of lightweighted and inexpensive gadgets mostly based on wireless technology [1-4]· Wireless body area network is a communication domain which monitors and maintains patient wellbeing condition. It consists of tiny biosensor buried in human skill, or placed on the body surface, or enclosed in mobile devices placed near or around the human body and may extend beyond human monitoring. It is implemented in several systems such as medicine, transportation, infrastructure, security apparatus, etc. [5] The Bluetooth and ZigBee infrastructure is the global requirement for wireless wearable biosensor [6]. BAN requires biosensors and accelerometers in identifying patients' location via a communication channel to transmit essential signs to medical practitioners.

It is designed to build gainful healthcare systems for less developed nations with poor medical infrastructure and less skilled medical practitioners. A wireless physiological data monitoring system uses communication link to transmit real time vital sign from wearable biomedical sensor gadgets to central network coordinator. The wireless gadgets deployed by patient collect physiological health signs and transmit the data to doctors in real time. WBAN systems have several merits over traditional healthcare systems. WBAN helps it users to stay at home for minor issue thereby reducing frequent hospitalization routine, and visit only when major health problem occurs reducing medication cost. This helps doctors attend to fewer patients with greater care daily and further diminish overcrowding

978-1-5386-1010-7/17/$31.00 ©2017 IEEE

in hospitals. For natural disaster, these systems transmit accident remotely to wellbeing experts for emergency response system thereby saving people's lives.

Physiological/biological sensors continuously check patient's fundamental signs and\or ecological factors. They are gifted in gathering, processing, aggregating, storing and conveying the data to central networking coordinator for additional calculation. An analysis of privacy and security challenges and possible solutions caregiver's environments, and technologies dealing with large data set are encouraged. The survey concludes with the challenges and future directions towards WBANs in healthcare systems. This Paper evaluates possible solutions to related works for proper security maintainability in medical applications. The survey evaluate possible clarifications for security enhancement in WBANs, and offer prospective opportunity.

2. Security and Privacy Requirements in WBANS

Security and Privacy of patient's vital parameters are two essential tools for secure WBAN security platform. Transmitting data via internet which is prune to attack should be done via a secure channel to maintain and protect patient related data from malicious users. Data security in the context of WBAN means protecting patient related data from vicious elements and unwanted actions of illegal users during and after transmission [7]. Whilst data privacy (or data protection), are steps and processes implemented to ensure data isn't being used or accessed by unauthorized individuals or parties. Privacy concern in medication application arises as a result of confidential patient records collected and store on medical servers, if reveal to unlawful users creates devastating problems. It arises from sources to name but few:

- ✓ Medical records
- ✓ Physiological/biological heritage
- ✓ Privacy breach
- ✓ Geographical locations and records
- ✓ Communication companies
- ✓ Governmental agencies

There are several security requirements such as data confidentiality, data availability, data reliability, data authentication, dependability, access control, accountability, non-repudiation, etc which are imminent in WBAN. Confidentiality is fundamental in protecting patient medical records against unlawful individual or party. Disclosure of such detail information create traumatic and devastating effects on patients. Data reliability ensures no alteration is made to patient medical data in transit, using digital signature, hash function and/ or using two factors authentication techniques via personal mobile number as second layer of security for properly securing medical records in WBAN.

2.1. Challenges for Enhancing Privacy and Security in WBAN

The distinctiveness of an application is needed to develop vigorous security mechanism, which defends the system from imminent security threats. Fundamental security rationales in WBAN are vividly stated below [8].

2.1.1. Data Confidentiality

It is paramount to protect healthcare records from unauthorized individuals, entities, or actions. The prospect of eavesdropping sensitive information transmitted via internet by an adversary should be discouraged to secure patient medical records. Using digital signature, hash function keys, two factors authentication method to encrypt health records over a secure channel renders data confidentiality.

2.1.2. Data Authentication

Medical and non-medical systems need data authentication. The body apparatus has to confirm whether the data is transmitted by trusted sensor or by an adversary. Symmetric platform can be used in WBAN to accomplish data authentication. This technique shares the secret key to compute Message Authentication Code (MAC) for all data.

2.1.3. Data Reliability

Healthcare records collected from several patients should be accurate, complete and consistent. Data reliability is of great significance, because it is used to identify and track patients as they move from one level of care to another. Data are used to validate the individuality to guarantee that patients are medication and maintains billing activity. Data reliability is achieved through data authentication protocols, ensuring that received data are not altered by an adversary. Digital signature stops an adversary of replaying old messages thereby increasing data reliability.

2.1.4. Secure Management

BNC assigns key in WBAN to attain encryption and decryption, it ensures secure management. The BNC adds and removes the WBAN in a secure behavior in the case of connection and disconnection [9]. Furthermore, BANs produce huge amount of data, and therefore, the need to manage and maintain these datasets is of paramount significance [10].

2.1.5. Availability

With the existence of big data analytics, doctors can easy fetch patient's information. This ease of access can be cracked by an adversary in disabling the ECG mode. This may lead to critical situation such as loss of life. Patient's data should be available at all times since this network carry highly sensitive data and possibly life-saving information. Most significantly, patient data is backup on secured servers to preserve the system running if an adversary manipulates the patient data [11].

2.1.6. Encryption

Encryption is the most competent way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt the message providing confidentiality for well-being healthcare system. It utilizes some algorithms such as Data Encryption Standard (DES), Advance Data Encryption Standard (ADES), Elliptic Curve Cryptography (ECC), and RSA algorithm to provide data confidentiality.

2.1.7. Data Security

Data security in WBAN is the protection of well-being data from an adversary or unauthorized users securely stored and transmitted over WBAN. The IEEE 802.15.16 standard, the latest standard for WBAN, tried to provide security in WBAN. However, it has several security problems [13].

2.1.8. Data Privacy

Data privacy for WBAN is the practice whereby unauthorized users are denied access and determines the type of well-being data to be shared with third parties. It uses non-cryptographic designs to protect privacy.

2.1.9. Interferences

Interference hinders WBAN as it collides with other wireless networks operating in the same domain. Therefore, the biosensors should be capable of coexisting among other networks thereby lessen interference on sensor nodes. It is pertinent because of the emergency for big data in WBAN applications [12-13]. Interference can degrade signal or cause system to fail.

2.1.10. Shared resource problem

Wireless band is a limited resource shared with all hubs within its transmitters. Bandwidth distribution is a complex task for large scale network with multiple users. Therefore, collision is often visible, but user-in-the-loop (UIL) is an alternative to future solution in WBAN.

2.1.11. Unknown node dilemma

In some wireless links, identifying sensor node is difficult from wireless access point (AP), though it doesn't stops other sinks from communicating with the AP. This creates dilemma in scheming media access control for WBAN.

2.1.12. Secure Data Localization

Localization is paramount to WBAN implementation. Security and privacy are the basic requirements for WBAN application. WBAN often results to diversity of unfavorable conditions (interference), affecting localization performance.

2.1.13. Data Freshness

Data integrity and confidentiality can only be guaranteed if data freshness methods are used. Adversary manipulative capability in replaying old messages to create confusion for WBAN coordinator. Data freshness assures data is not reused with frames in order. Two types of data freshness are: *strong freshness* guarantees delay with frame ordering, and *weak freshness* provides no guarantee in terms of delay. Strong freshness is necessary in synchronization while data is being communicated to WBAN coordinator, and whereas weak freshness is necessary for WBAN nodes with low-duty cycle.

2.1.14. Packet Alteration

An adversary can alter a packet while in transmission resulting to security breach. The adversary simply intercepts the packet, modify and send it to the intended destination.

Other security prerequisites (confidentiality, integrity & authentication) at all levels of WBAN as in below:

- **Efficiency**

Energy sustainability is an essential feature of a WBAN's design and implementation as a result of the limited capabilities of sensors. The constant monitoring requirements of a WBAN can be stalled by the regular energy reduction even though the sensors are rechargeable. Therefore an improve energy system is needed for safe communication in WBAN.

- **Usability**

The performance of the WBAN should be useable. The Sensor capacity should be accurate and well calibrated even when the system is logout and logon again [14]. The wireless links should be vigorous and work under various user environments.

- **Cost**

WBAN in the 21st century requires low health monitoring cost with high functionality by it users. WBAN designs motivation need to be reduce in cost to be a likable alternatives to mindful health clients.

- **Deployment Constrained**

The WBAN needs to be wearable, trivial and non intrusive. It should not change or impede the user's daily activities. The technology should eventually be crystal clear to the user i.e., it should perform its monitoring tasks without the user realizing it.

Table 1 the General Differences between Wban and Wsn

	WBAN	WSN
Deployment	The quantity of nodes used by the user depends on different factors. (i.e.: on human body or hidden under clothing). Devices are only added when they are needed for use. WBAN does not employ redundant nodes.	WSN is used in areas that are not easily reached by operators allowing additional nodes to be placed to complement possible failures in nodes.
Density	WBAN is not node-dense	
Data Rate	WBAN normally happen in an intermittent and steady rate.	WSN is deployed for supervising event-based which occurs at uneven.
Mobility	WSN permits users to have their freedom of movement without any restriction.	WSN here the sensor nodes are habitually viewed as fixed.
Latency	Batteries in the devices are easily removed and replaced which is vital to energy utilization.	Here the sensor Nodes cannot be reached sometimes after deployment which makes higher latency pivotal in maximizing battery life duration.

The above table illustrates the difference between WBAN and WSN which is a communication system between the humans and computers via wearable devices.

3. Discussion and Conclusion Remark

3.1. Discussion

Referring to the above literatures, biometric system [15-16], attribute based encryption (ABE) and the elliptical curve cryptography (ECC) has emerged as a powerful tools in key establishment and authentication of body sensor nodes. This method uses measurement of physiological characteristics of the body itself as an important parameter in a symmetric key management system. It is more secure than most techniques but reduces the transmission speed of the patient health data due to its complexity. Furthermore, the proposed schemes have not adequately addressed the security issues. Therefore, it is incumbent upon researchers to design a sustainable and low cost WBAN with flexible cryptographic algorithms along side with renewable energy source for an efficient use of the WBAN in the healthcare system.

3.2. Conclusion Remark

The WBAN is a vital phenomenon in modern day healthcare sector with huge benefits of improved technology that will change people's standard of living. Due to the improvement in technologies in the 21st century, is sometime difficult to protect and maintain Patient Health Data because of the actions of an adversary or unauthorized users over the internet posing a security threat and privacy in WBANs. With the continuing modernizations of biosensors, improving the batteries durability, acting as integrated sensors and aggregators, envisage to see WBAN as an efficient technology capable of taking care of the aging world population with more secure, dependable and efficient WBANs.

Acknowledgment

The author would like to thank Prof Paul Kamara, and Dr. Michael N. Wundah from the Institute of Advanced Management and Technology, Freetown Sierra Leone for their support and encouragement.

References

[1] Developing wireless body area networks standard .

[2] Sana Ullah, Henry Higgins, Bart Braem, Benoit Latre, Chris Blondia, Ingrid Moerman, Shahnaz Saleem, Ziaur Rahman and Kyung Sup Kwak, A Comprehensive Survey of Wireless Body Area Networks: On PHY, MAC, and Network Layers Solutions, Journal of Medical Systems (Springer), 2010.

[3] Chen, Min; Gonzalez, Sergio; Vasilakos, Athanasios; Cao, Huasong; Leung, Victor (2010). "Body Area Networks: A Survey" (PDF). Mobile Networks and Applications (MONET) (Springer Netherlands) 16(2):1–23.

[4] Movassaghi, Samaneh; Abolhasan, Mehran; Lipman, Justin; Smith, David; Jamalipour, Abbas (2014). "Wireless Body Area Networks: A Survey". IEEE Communications Surveys and Tutorials (IEEE).

[5] Poslad, Stefan (2009). Ubiquitous Computing Smart Devices, Smart Environment and Smart Interaction.

[6] IEEE P802.15.6-2012 Standard for Wireless Body Area Networks.

[7] G. Virone, A. Wood, L. Selavo, Q. Cao, L. Fang, T. Doan, Z. He, and J.A. Stankovic. An Advanced Wireless Sensor Network for Health Monitoring. In proceeding of the Trans-disciplinary Conference on Distributed Diagnosis and Home Healthcare (D2H2), April 2006.

[8] Summers, G. (2004). Data and databases. In: Koehne, H Developing Databases with Access: Nelson Australia Pty Limited. p4-5.

[9] Shahnaz Saleem, Sana Ullah, Hyeong Seon Yoo, "On the Security Issues in Wireless Body Area Networks", International Journal of Digital Content Technology and its Applications, Vol 3, No 3, Sept 2009.

[10] "Data Management Within mHealth Environments: Patient Sensors, Mobile Devices, and Databases" J. Data and Information Quality.

[11] Shahnaz Saleem, Sana Ullah and Kyung Sup Kwak, "A Study of IEEE 802.15.4 Security Framework for Wireless Body Area Networks", Sensors, vol-11, pp-1383-1395, 2011.

[12] On the vulnerabilities of the Security Association in the IEEE 802.15.6 Standard Proceedings of the 1st Workshop on Wearable Security and Privacy (Wearable '15), 2015.

[13] "Implementation of Wireless Body Area Networks for Healthcare systems". Sensors and Actuators.

[14] Garcia P., "A Methodology for the Deployment of Sensor Networks", IEEE Transactions on Knowledge and Data Engineering, vol. 11, no. 4, December 2011.

[15] C.C.Y Poon, et al. (2006, April) A novel Biometrics Method to Secure Wireless Body Area Sensor Networks for Telemedicine and M- Health. IEEE Communications Magazine.

[16] F.M. Bui and D. Hatzinakos, "Biometric Methods for Secure Communications in Body Sensor Networks: Resource-Efficient Key Management and Signal-Level Data Scrambling, " EURASIP Journal on Advances in Signal Processing, vol. 8, pp.1-16, 2008 .