IJRSET OCTOBER 2018 Volume 5, Issue 10 Pages: 1-6

ISSN 2394-739X

International Journal for Research in Science Engineering and Technology

# A SURVEY ON BODY AREA NETWORK IN MOBILE HEALTH SYSTEM

[1] J. Monica Rebecca [2] Dr. A. Marimuthu,
[1, 2] Department of Computer Science,
[1, 2] Government Arts College,
[1, 2] Coimbatore, India.

**ABSTRACT-** The Body Area Network (BAN) technology is one of the core technologies of developments in healthcare system, where a patient can be monitored using a collection of tiny-powered and lightweight wireless sensor nodes. However, development of this new technology in healthcare applications without considering security makes patient privacy vulnerable. In this article, at first we address the several security requirements in WBAN based modern healthcare system. Then, we propose a secure Robust and Efficient Authentication Scheme based healthcare system using WBAN - HealthCare, which can efficiently accomplish those requirements. And then we used Anonymous Authentication Protocol for Authorized user selection in WBAN. Random Key Pre-distribution (RKP) secure key management Scheme for Secure Communication.

**Keyword- [**Healthcare, Authentication, WBAN, Random Key Pre-distribution (RKP).]

## 1. INTRODUCTION

A Body Area Network (BAN), also referred to as a Wireless Body Area Network (WBAN) or A Body Sensor Network (BSN) or A Medical Body Area Network (MBAN), is a wireless network of wearable computing devices. BAN devices may be embedded inside the body, implants, may be surface-mounted on the body in a fixed position Wearable technology or may be accompanied devices which humans can carry in different positions, in clothes pockets, by hand or in various bags.Whilst there is a trend towards the miniaturization of devices, in particular, networks consisting of several miniaturized body sensor units (BSUs) together with a single body central unit (BCU).Larger decimeter (tab and pad) sized smart devices, accompanied devices, still play an important role in terms of acting as a data hub, data gateway and providing a user interface to view and manage BAN applications, insitu. The development of WBAN technology started around 1995 around the idea of using wireless personal area network (WPAN) technologies to implement communications on, near, and around the human body. About six years later, the term "BAN" came to refer to systems where communication is entirely within, on, and in the immediate proximity of a human body. A WBAN system can use WPAN wireless technologies as gateways to reach longer ranges. Through gateway devices, it is possible to connect the wearable devices on the human body to the internet. This way, medical professionals can access patient data online using the internet independent of the patient location.

BAN technology is still an emerging technology, and as such it has a very short history. BAN technology emerges as the natural byproduct of existing sensor network technology and biomedical engineering. Professor Guang-Zhong Yang was the first person to formally define the phrase "Body Sensor Network" (BSN) with publication of his book Body Sensor Networks in 2006. BSN technology represents the lower bound of power and bandwidth from the BAN use case scenarios. However, BAN technology is quite flexible and there are many potential uses for BAN technology in addition to

BSNs. Some of the more common use cases for BAN technology are:

- Body Sensor Networks (BSN)
- Sports and Fitness Monitoring
- Wireless Audio
- Mobile Device Integration
- Personal Video Devices

## 2. BODY AREA NETWORK APPLICATIONS

### 2. Applications in Healthcare

As previously mentioned, BANs have grown as a refinement of BSN. As such, BSN remain the most thought out applications of BAN.

### 2.1 Managed Body Sensor Networks

A managed body sensor network (MBSN) is defined as a system where the third party makes decisions based the data collected from one or many BSN. We will discuss Mobile Health and CodeBlue, two managed BSN that are are approaching development of managed BSN from two different perspectives.

In 2003, two researchers from the University of Twenty published a paper entitled "Continuous monitoring of vital constants for mobile users: the Mobile Health approach." The paper described the increasing demand of resources placed on the medical community, the rising costs of in-patient care, and the relative lack of out-patient monitoring. The paper defined "extra-BAN communication" (EBAN) as communication between a BAN and another network. The solution paper provided was Mobile Health, a BSN with EBAN connectivity to a 2.5/3G networks to provide out-patient monitoring of patients vital signs. Through this infrastructure the Mobile Health designers were able to provide sensor information to qualified medical professionals, where multiple patient's data could be monitored in an aggregate form.

### 2.2 Autonomous Body Sensor Networks

Autonomous body sensor networks (ABSN) and MBSN share the same goals, but they accomplish them in different ways. While a MBSN will relies on reading sensor information and delivering it to a third party for decision making and intervention, ABSN take a more proactive approach. ABSN introduce actuators in addition to the sensors to allow the BSN to effect change on the user's body. In addition to the actuators, ABSN contain more intelligent sensors that contain enough intelligence to complete their own tasks independently.

Human++ is a project developed in Belgium that aims to bring ABSN to the mainstream. The design of Human++ is relatively simple, any node in the mesh-network are able to talk to any other node in the network. There is a predefined "central" node that is designated for all EBAN communication. The central node also publishes information on any services that the ABSN provides external access to.

### 3. Challenges Associated with BAN

**Data Quality**: Data generated and collected through BANs can play a key role in the patient care process. It is essential that the quality of this data is of a high standard to ensure that the decisions made are based on the best information possible [16]

**Data Management**: As BANs generate large volumes of data, the need to manage and maintain these datasets is of utmost importance.[17][18]

**Sensor Validation**: Pervasive sensing devices are subject to inherent communication and hardware constraints including unreliable wired/wireless network links, interference and limited power reserves. This may result in erroneous datasets being transmitted back to the end user. It is of the utmost importance especially within a healthcare domain that all sensor readings are validated. This helps to reduce false alarm generation and to identify possible weaknesses within the hardware and software design.[19]

**Data Consistency**: Data residing on multiple mobile devices and wireless patient notes need to be collected and analyzed in a seamless fashion. Within body area networks, vital patient datasets may be fragmented over a number of nodes and across a number of networked PCs or Laptops. If a medical practitioner′s mobile device does not contain all known information then the quality of patient care may degrade.[20]

**Security**: Considerable effort would be required to make WBAN transmission secure and accurate. It would have to be made sure that the patient ‘'secure‘' data is only derived from each patient's dedicated WBAN system and is not mixed up with other patient's data. Further, the data generated from WBAN should have secure and limited access. Although security is a high

priority in most networks, little study has been done in this area for WBANs. As WBANs are resource-constrained in terms of power, memory, communication rate and computational capability, security solutions proposed for other networks may not be applicable to WBANs. Confidentiality, authentication, integrity, and freshness of data together with availability and secure management are the security requirements in WBAN. The IEEE 802.15.6 standard, which is latest standard for WBAN, tried to provide security in WBAN. However, it has several security problems.[21]

**Interoperability**: WBAN systems would have to ensure seamless data transfer across standards such as Bluetooth, ZigBee etc. to promote information exchange, plug and play device interaction. Further, the systems would have to be scalable, ensure efficient migration across networks and offer uninterrupted connectivity.

**System devices**: The sensors used in WBAN would have to be low on complexity, small in form factor, light in weight, power efficient, easy to use and reconfigurable. Further, the storage devices need to facilitate remote storage and viewing of patient data as well as access to external processing and analysis tools via the Internet.

**Invasion of privacy**: People might consider the WBAN technology as a potential threat to freedom, if the applications go beyond "secure" medical usage. Social acceptance would be key to this technology finding a wider application.

**Interference**: The wireless link used for body sensors should reduce the interference and increase the coexistence of sensor node devices with other network devices available in the environment. This is especially important for large scale implementation of WBAN systems.[9][22]

**Cost**: Today's consumers expect low cost health monitoring solutions which provide high functionality. WBAN implementations will need to be cost optimized to be appealing alternatives to health conscious consumers.

**Constant monitoring**: Users may require different levels of monitoring, for example those at risk of cardiac ischemia may want their WBANs to function constantly, while others at risk of falls may only need WBANs to monitor them while they are walking or moving. The level of monitoring influences the amount of energy required and the life cycle of the BAN before the energy source is depleted.

**Constrained deployment**: The WBAN needs to be wearable, lightweight and non-intrusive. It should not alter or encumber the user's daily activities. The technology should ultimately be transparent to the user i.e., it should perform its monitoring tasks without the user realizing it.

The most critical objective of this paper was to address the few security necessities in BAN based present day medicinal services framework. At first we address the few security necessities in WBAN based current medicinal services framework. At that point, we propose a safe Robust and Efficient Authentication Scheme based medicinal services framework utilizing WBAN - HealthCare, which can effectively achieve those prerequisites. And afterward we utilized Anonymous Authentication Protocol for Authorized client choice in WBAN. Irregular Key Pre-appropriation (RKP) secure key administration Scheme for Secure Communication.These sensors gather the physiological parameters and forward them to an organizer called Local Processing Unit (LPU), which can be a convenient gadget, for example, PDA, PDA and so forth.should be accurate and calibrated, even when the WBAN is switched off and switched on again.[23] The wireless links should be robust and work under various user environments.

BAN technology is still emerging and there are a lot of problems left to solve. Setting aside ethical issues like privacy, there are still plenty of technical challenges that we must overcome before BAN will become an effective solution. The BAN draft submissions have defined solutions for a lot of the basic wireless network protocols, but there is still a large amount of research that must be done to effectively propagate a signal in and around the human body. The last challenge BAN technology faces is actually a problem of Human-Computer Interaction (HCI) and how to make the technology usable.

## 3. BAN – LITERATURE REVIEW

This research provides the various methodologies implemented to BAN reflective thinks with reference to opinion and behavior using BAN techniques. The Mobile-Health (M-Health) system has been envisioned as a promising approach to improving healthcare quality and save

lives in the aging society. In this section, we present significant research carried out in Mobile-Health (M-Health) system for reflective thinks. “SAGE: A strong privacy-preserving scheme against global eavesdropping for eHealthsystems,” X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, IN [3] eHealth framework is imagined as a promising way to deal with enhancing social insurance through data innovation, where security and protection are urgent for its prosperity and large scale arrangement. In this paper, we propose a solid security safeguarding Scheme against Global Eavesdropping, named SAGE, for eHealth frameworks. The proposed SAGE can accomplish the substance situated protection as well as the relevant security against a solid worldwide foe. Broad investigation exhibits the viability and practicability of the proposed plot.

, “SPOC: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency,” R. Lu, X. Lin, and X. Shen, In [4] the inescapability of PDAs and the development of remote body sensor systems (BSNs), versatile Healthcare (m-Healthcare), which broadens the activity of Healthcare supplier into an unavoidable domain for better wellbeing observing, has pulled in extensive intrigue as of late. Be that as it may, the twist of m-Healthcare still faces numerous difficulties including data security and protection safeguarding. In this paper, we propose a protected and security safeguarding shrewd processing structure, called SPOC, for m-Healthcare crisis. With SPOC, advanced mobile phone assets including figuring force and vitality can be artfully assembled to process the registering escalated individual wellbeing data (PHI) amid m-Healthcare crisis with insignificant security divulgence. In particular, to use the PHI protection revelation and the high unwavering quality of PHI process and transmission in m-Healthcare crisis, we present an effective client driven security get to control in SPOC structure, which depends on a trait based access control and another security saving scalar item calculation (PPSPC) strategy, and enables a medicinal client to choose who can take an interest in the shrewd registering to help with handling his staggering PHI information. Nitty gritty security examination demonstrates that the proposed SPOC system can effectively accomplish client driven protection get to control in m-Healthcare crisis. Likewise, execution assessments by means of broad reproductions exhibit the SPOC's adequacy in term of giving high-solid PHI process and transmission while limiting the protection exposure amid m-Healthcare crisis., “Energy-Spectrum Efficiency Tradeoff for Video Streaming over Mobile Ad Hoc Networks”L. Zhou, R. Q. Hu, Y. Qian, and H-H Chen.In [5]this work, we examine the properties of vitality productivity (EE) and range effectiveness (SE) for video gushing over portable impromptu systems by building up a vitality range mindful planning (ESAS) plot. To depict a pragmatic portable situation, we utilize an arbitrary walk versatility display, in which every hub can pick its portability bearing and speed haphazardly and freely. Through thorough examination and broad reenactments, we exhibit that the hub portability is gainful to EE however not to SE. The commitments of this work are twofold: 1) We propose an ESAS conspire with a dynamic transmission extend, which essentially outflanks the past least twisting video planning for terms of joint EE and SE execution; 2) We determine an achievable EE-SE tradeoff go and a tight upper/bring down bound concerning vitality range effectiveness file for different hub speeds. We trust that this work sheds experiences on the basic outline rules on building a vitality and range effective portable video transmission framework.,

“Enabling Device-to-Device Communications Underlying Cellular Networks: Challenges and Research Aspects,L. Wei, R. Q. Hu, Y. Qian, and G. Wu In [6]Gadget to-gadget correspondence underlying a cell organize is a promising innovation in future remote systems to enhance arrange limit and client encounter. While D2D correspondence can possibly enhance remote framework ghostly and vitality effectiveness because of the closeness of correspondence parties and higher range reuse increase, enormous work is as yet progressing to transform the promising innovation into a reality. This article examines D2D specialized difficulties and in addition gauges advance and imperative research viewpoints that empower D2D interchanges underlying cell systems. The key research regions tended to incorporate impedance administration, multihop D2D interchanges, and D2D correspondences in heterogeneous systems. While empowering D2D interchanges underlying cell systems, D2D cor-

respondences can utilize either cell downlink or cell uplink assets. The two asset sharing modes will make distinctive obstruction situations. The execution assessment on D2D correspondences underlying cell arranges under these two unique situations is given. “Opportunities and challenges: Security ineHealth,” Bell Labs Technical JournalS. Sabnis, and D. Charles, In [7] e Health is the exchange of wellbeing assets and human services by electronic means, and is empowered by interchanges innovation through broad data sharing and joint effort. Given the touchy idea of medicinal data, and human services experts' high level of reliance on solid records, issues of uprightness, security, protection, and classification are of specific essentialness, and in this way security must be plainly and successfully tended to by eHealth applications. This letter features the difficulties, drivers, and institutionalization activities for security, consistence, and interoperability in wellbeing related exercises did over separation by methods for data correspondence innovations. © 2012 Alcatel-Lucent.

## CONCLUSION

The most critical objective of this paper was to address the few security necessities in BAN based present day medicinal services framework. At first we address the few security necessities in WBAN based current medicinal services framework. At that point, we propose a safe Robust and Efficient Authentication Scheme based medicinal services framework utilizing WBAN - HealthCare, which can effectively achieve those prerequisites. And afterward we utilized Anonymous Authentication Protocol for Authorized client choice in WBAN. Irregular Key Pre-appropriation (RKP) secure key administration Scheme for Secure Communication.These sensors gather the physiological parameters and forward them to an organizer called Local Processing Unit (LPU), which can be a convenient gadget, for example, PDA, PDA and so forth.

## REFERENCES

[1] United Nations, World Population Prospects: The 2004 Revision Population Database, Population Division, 2004.

[2] S. Harper, Ageing societies: Myths, challenges and opportunities, Hodder Arnold, 2006.

[3] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, “SAGE: A strong Privacy-preserving scheme against global eavesdropping for eHealth Systems,” IEEE Journal on Selected Areas in Communications, vol. 27, No. 4, pp. 365-377, 2009.

[4] R. Lu, X. Lin, and X. Shen, “SPOC: A secure and privacy-preserving Opportunistic computing framework for mobile-healthcare emergency,” IEEE Transaction on Parallel and Distributed Systems, vol. 24, no. 3, pp. 614-624, 2013.

[5] L. Zhou, R. Q. Hu, Y. Qian, and H-H Chen, “Energy-Spectrum Efficiency Tradeoff for Video Streaming over Mobile Ad Hoc Networks,” IEEE Journal on Selected Areas in Communications, vol. 31, no. 5, pp. 981- 991, 2013.

[6] L. Wei, R. Q. Hu, Y. Qian, and G. Wu, “Enabling Device-to-Device Communications Underlying Cellular Networks: Challenges and Research Aspects,” IEEE Communications, vol.52, no.6, pp. 90-96, 2014.

[7] S. Sabnis, and D. Charles, “Opportunities and challenges: Security in E Health,” Bell Labs Technical Journal, vol. 17, no. 3, pp. 105-112, 2012.

[8] A. Sawand, S. Djahel, Z. Zhang, and F. Nait-Abdesselam, “Toward Energy-efficient and trustworthy eHealth monitoring system,” China Communications, vol. 12, no. 1, pp. 46-65, 2015.

[9] L. Guo, C. Zhang, J. Sun, Member, and Y. Fang, “A privacy-preserving attribute-based authentication system for mobile health networks,” IEEE Transactions on Mobile Computing, vol. 13, no. 9, pp. 1927-1941, 2014.

[10] X. Liang, R. Lu, L. Chen, X. Lin, and X. Shen, “PEC: A privacy preserving Emergency call scheme for mobile healthcare social networks,” Journal of Communications and Networks, vol. 13, no. 2, pp. 102-112, 2011.

[11] X. Liang, X. Li, M. Barua, L. Chen, R. Lu, X.(Sherman) Shen, and H. Y. Luo, “Enable Pervasive Healthcare through Continuous Remote Health Monitoring,” IEEE Wireless Communications, vol. 19, no. 6, pp. 10-18, 2012.

[12] G. Tormo, F. Marmol, J. Girao, and G. Perez, “Identity management in Privacy we trust: Bridging the trust gap in eHealth environments,” IEEE Security and Privacy, vol. 11, no. 6, pp. 34-41, 2013.

[13] A. G. Frangopoulos, J. Gialelis1, and D. Serpanosl, "Imposing Holistic Privacy and Data Security on Person Centric eHealth Monitoring Infrastructures," 12th IEEE International Conference on e-Health Networking Applications and Services (Healthcom), 2010.
[14] M. Barua, R. Lu, and X. Shen, "SPS: Secure personal health information Sharing with patient-centric access control in cloud computing," IEEE Global Communications Conference, pp. 647-652, 2013.
[15] H. F. Ji, W. B. Han, and L. Zhao, "Certificate less generalized signcryption,"
Cryptology ePrint Archive, Report 2010/204.
[16] O'Donoghue, J., Herbert, J. and Sammon, D., 2008, June. Patient sensors: A data quality perspective. In International Conference on Smart Homes and Health Telematics (pp. 54–61). Springer, Berlin, Heid berg, https://link.springer.com/chapter/10.1007/978-3-540-69916-3_7
[17] O'Donoghue, John; Herbert, John (1 October 2012). "Data Management within mHealth Environments: Patient Sensors, Mobile Devices, and Databases". J. Data and Information Quality.
[18] Lai, D. , Begg, R.K. and Palaniswami, M. eds, Healthcare Sensor Networks: Challenges towards practical implementation, ISBN 978-1-4398-2181-7, 2011
[19]Donoghue, J., Herbert, J., Fensli, R. and Dineen, S., 2006, October. Sensor validation within a pervasive medical environment. In Sensors, 2006. 5th IEEE Conference on (pp. 972–975).
IEEE. http://ieeexplore.ieee.org/abstract/document/4178781/
[20] O'Donoghue, J., Herbert, J. and Salerno-Kennedy, R., 2006, October. Data consistency within a pervasive medical environment. In Sensors, 2006. 5th IEEE Conference on (pp. 968–971).
IEEE. http://ieeexplore.ieee.org/abstract/document/4178780/
[21] Toorani, Mohsen (2015). "On Vulnerabilities of the Security Association in the IEEE 802.15.6 Standard". Financial Cryptography and Data Security. Lecture Notes in Computer Science. 8976. pp. 245–260. ArXiv:1501.02601
[22] Garcia P., "A Methodology for the Deployment of Sensor Networks", IEEE Transactions on Knowledge and Data Engineering, vol. 11, no. 4, December 2011
[23] P. Kushwah, and S. Lai, "Efficient generalized signcryption schemes," Cryptology ePrint Archive, Report 2010/346. http://eprint.iacr.org (2010).
[24] C. Zhou, W. Zhou, and X. Dong, "Provable certificate less generalized Signcryption scheme," Design, Codes and Cryptography, 71: 331-346, 2014.
[25] W. Shi, N. Kumar, P. Gong, and Z. Zhang, "Cryptanalysis and Improvement of a certificate less signcryption scheme without bilinear Pairing," Frontiers of Computer Science, vol. 8, no. 4, pp. 656-666, 2014.
[26] S. Rahman, M. Masud, C. Adams, K. El-Khatib, H. Mouftah, and E. Okamoto, "Cryptographic security models for eHealth P2P database Management systems network," IEEE Annual International Conference On Privacy, Security and Trust, 2011.
[27] M. Ahmed, M. Ahamad, and T. Jaiswal, "Augmenting security and Accountability within the eHealth Exchange," IBM Journal of Research And Development, vol. 58, no. 1, 8:1-8:11, 2014.
[28] S. Al-Riyami, and K. Paterson, "Certificateless public key cryptography," Advances in Cryptology-Asiacrypt2003, Lecture Notes in Computer Science, Springer-Verlag 2894: 452-473, 2003.
[29] M. Bellare, and P. Rogaway, "Random Oracles are Practical: a Paradigm For Designing Efficient Protocols," ACM CCCS, pp. 62-73, 1993.
[30] "Exercise and walking is great for the alzheimer's and Dementiapatient's physical and emotional health," http://freealzheimerssupport.com/wordpress/2010/06/exercise-and walking/, June 2010.

## AUTHOR'S BIOGRAPHIES

**First Author**
J. Monica Rebecca B.Sc., M.Sc.,
PursuingM.Phil.In Department of Computer Science, Government Arts College, Coimbatore-641 018
**Second Author**
Dr.A.Marimuthu M.C.A., M.Phil., PhD.,
Associate Professor, Department of Computer Science,
Government Arts College (Autonomous),
Coimbatore – 641 018.
Years of working experience and specialized in Computer Networks and Security.