IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

AN OVERVIEW OF BSN AND ITS SECURITY

Krupali Dilipbhai Panchal

Assistant Professor

Department of Computer Applications, Faculty of Science

The Maharaja Sayajirao University of Baroda

Vadodara, Gujarat, India

ABSTRACT

In the world of technology, one of the most recent exciting developments is Body Sensor Networks. This BSN allows for the constant monitoring of a variety of bodily functions through the use of implantable, wearable, and portable sensors. User's sensitive information such as the identity, their medical history can be compromised if they are transmitted over an insecure or untrustworthy network. This study provides an overview of the Body Sensor Networks and possible security threats could possible.

Keywords: BSN, Body Sensor Network, Wearable devices, BSN security

INTRODUCTION

Healthcare service is essential for the well-being of all age people for personal care, nursing, life threatening illness, health consulting, and contingency help. Around the world, in almost countries the major burning issue is in healthcare service where there is the lack of workforce and funding for the services. Health issues are majorly seen to the elderly people but it has been extended to youth and children due to the ultimate change in earthly climate and today's lifestyle. In this scenario, the adequate medical workforce and healthcare infrastructure should be there for continuous monitoring the health condition. From the standpoint of the ordinary medical workforce, a wireless body sensor network can be a great an emerging solution for health monitoring.

Originally the term "body sensor network" refers to a subset of the broader category of "wireless sensor network" designed specifically for physical contact uses. To monitor a person's current physical health, wireless body sensor networks are a promising technology. They are able to do remote monitoring in a variety of circumstances to deliver the concerned medical professionals physiological data. Primarily body sensor devices were designed for healthcare sector to continuous monitor the patient's health and record the vital information. The heart patient can be monitored remotely by the medical staff from anywhere if the patient is using body sensor network devices having ECG sensor. Likewise any other chronic disease can be monitored using these devices with different sensors. Nowadays some wearable devices like smart watch are available in the market with some basic sensors which can monitor heart rate, SpO2, blood pressure, etc. By wearing these kinds of devices, a person can monitor the health condition of its own and the gateway device will also send this information to the server also. So in the case of any emergence person can get the medical treatment.

One of the previous difficulties with wearable sensing or wearable computing was the development of a wearable sensor network. With the advent of recent wireless technologies with efficient protocols, the idea of a body sensor network (BSN) may allow for the continuous supply of low-cost healthcare. Wearable sensor nodes are the building blocks of a body-area network. Each sensor has the ability to take physiological readings, process them, and transmit the results to the server of concerning medical officer. There are gateway devices, such as smart phones, that send the sensed data to the BSN server.

The mechanism for transmitting the sensed data is the antenna components built into the sensor nodes enable wireless transfer of data to a device worn or implanted on the body. The gateway device such as PDA or a computer system revolves around to handles all interactions.

SYSTEM ARCHITECTURE

The body sensor network devices are the devices which can be implanted on the body, or user can wear them and the centre devices which send the sensed data to the BSN server. The devices which are used to be in physical contact with the body will constantly monitor the health of the user and transmit the sensed data to the gateway device acting as a centre device. This centre device should be connected with Internet to send the sensed data to the server from where it will be transmitted to the concerning medical staff such as a doctor.

There are mainly three tiers of body sensor network systems.

1. At the first prior level intelligent sensors or nodes can only relay information to and receive commands from a parent device.
2. A second-tier device, like a private server, is a device that can be smart PDA, smart phone or desktop computer. There is two-way communication between the sensors and the second-level devices for transmission of the sensed data.
3. The third stage involves sending the data to a distributed set of remote servers. Each tier is an individual, complex subsystem that uses internal hierarchy to maximise effectiveness, portability, safety, and cost savings.

The body sensor network (BSN) is a significant category of devices that tightly couples lightweight embedded processors and communication systems to the human body. Information gleaned from data collected in users' natural environments can be incredibly valuable for medical care providers, and clinicians, researchers. The authorised medical staff can track the development of a disease, spot its earliest signs, or just gauge the health of the user with this data. A major challenge for widespread deployment of body sensor network is organizing and maintaining a massive amount of sensed and transmitting data. An approach to data mining motivated by methods from the study of text and natural language processing are being developed to deal with this challenge. The method relies on motion transcripts, a string of characters used to represent sensor readings. The complexity of the data can be greatly reduced by using transcripts, but the original shape and structure of the physiological signals are preserved. Specifically, the data-mining method exploits the signal's structure by analyzing its signature transitions.

TOPOLOGIES AND PROTOCOLS

Topologies: The configuration of network devices including the transmission media and the access points can be described by the network physical topology. These topologies can also describe the protocols used by the nodes to transmit the data among each other. Whereas the network logical topology describes how the data will be transmitted between the transmitting nodes. From the reference model OSI, defining the physical topology is the combined responsibility of physical layer and logical layer; in the reference model TCP/IP, link layer is responsible for the same. For the logical topology the network layer is responsible in both of the reference models. Regarding latency, robustness, capacity, and the complexity of data routing and processing, each topology has features and drawbacks.

Only two devices are needed for the simplest star topology architecture. One device can be master controller, oversees the network of peripheral devices. Slave devices are the periphery nodes constrained to conversing to their masters. Slaves cannot directly communicate with one another; rather, they must relay all messages through the master. In this topology the master controller device will act as a centre device which will control all other slave devices.
This topology works as a peer-to-peer network where any two devices within range of one another can exchange data. Multi-hop networking protocols allow data packets to be sent from one network node to another.

There is always only one path between each given pair of devices in a tree topology, which makes it a specific example of a multi-hop mesh network where root node, parent node and child node will be there. In this network topology, the root will be initiating node. To allow other devices to join the network, the root node can accept a new device as its "child" node. Nodes and their child nodes are all identifiable to the devices in a network. Through its hierarchical structure, this network architecture simplifies routing.
In this topology there can be any combination of two or more differing network topologies. The advantages of both the single-hop star topology and the multi-hop mesh topology can be found in a hybrid star-mesh network.

Protocols: Protocols are set of rules for communication in network. The protocols define how the data will be transmitted among the connecting nodes. The Institute of Electrical and Electronics Engineers (IEEE) had defined some standards for wireless networks. IEEE 802.11 standard specifies the set of MAC and PHY protocols to implement the wireless LAN for communication in different frequencies. Basically this standard was for WiFi network working for PCs, or PDAs. IEEE 802.15 standards are used to define the Bluetooth technology, a personal area network which can be operable in a small range of area. This standard is generally used in body area network to connect the node with the gateway with less power consumption. IEEE 802.15.4 standard is a standard for low cost, low data rate wireless personal area network. Zigbee is a suite of high level communication protocol based in IEEE 802.15.4 standard. Zigbee is used to create a small

personal area network for home automation, medical devices or any small scale projects which require wireless connection.

IEEE had defined the IEEE 802.15.6 standard for short range wireless transmission. The data rates offered up to 10 Mbps to satisfy the healthcare services. The personal area networks do not support the combination of low power, data rate, non interference, Quality of Service and reliability. The IEEE 802.15.6 standard has different security levels. These levels will be selected as per the requirement of an application. Level 0 is used for insecure data transmission with no security checks. At the level 1 of the standard authentication will be performed but no checks for data integrity. Level 2 is the highest level of security where all security measures are available.

SECURITY

In the body sensor network, sensed information regarding a person will be transmitted using a gateway over the internet across the world. The chances of sniffing or capturing the data and alteration of sniffed or captured data are highly possible. The security feature of body sensor network must have to be ensuring the access of sensitive data of a person by the authorized healthcare professionals. It must have to be mandatory to keep the person's identity and health records secure while they are under observation. The possible threats or attack can be active or passive. The intruder can compromise the patient's health by stealing their sensitive medical data.

Some of the possible threats in body sensor network can be any of the following:

1. Data diddling: An intruder can change any piece of sensed data of any patient during or before transmitting to the dedicated server. This alteration can cause a critical situation by having misinterpreting information regarding patient's health which can lead to the crucial stage of health.
2. Impersonation: An intruder can act as a body sensor network node where he can send misinterpreting information of actual patient. In this attack, there is a possibility of impersonation by an intruder for a medical representative or any of medical staff which can prescribe any medical treatment that might not be suggested to that patient.
3. Data exfiltration: An intruder or an attacker can get the access of the system of authorized user and can steal or delete the medical records or history of any patient. An attacker can misuse this stolen information, sell them over the internet or cause any critical damage to the patient.

Some of the possible solutions for the above mentioned threats can be:

1. Data breach is a crucial threat and to prevent this, on the gateway side and server side, some universal data coding system should be there to mark the sensitive data as original information sent by the intended sending device. On the side of medical or hospital, the authenticate person must have to keep a track of patient's health information and have to examine it to identify the breaches. All endpoints of body sensor network must have to be secured.
2. At all the points, authentication in a secure manner should be there to avoid impersonation. So an intruder can be identified who intends to attack. In case of any change in device or any replacement, all data must have to be coded with secure algorithms. Some protocols also should be used to secure the transmission of sensitive information.
3. The security applications like firewall, antivirus or anti spyware should have to be implemented on the server and gateway side. The data which is in transmission should be in encrypted form, the only person having the decryption method can access it.
4. The medical staff should be trained enough to understand the actual data or to identify the authenticate source of the data. Intrusion detection and prevention system (IDPS) can also be a good solution to prevent intrusion threats. The network or device access should be limited to authorized users only. The third party cannot use any of the devices in any situation. If it is required in critical condition and in the unavailability of the authorized user, another alternative should be there to avoid unavoidable impacts.

The patient's medical information is at a risk of being stolen or any alteration. To maintain data confidentiality, integrity and availability different security measures must have to be implemented in body sensor network. This can be done by data encryption with a secret key which also have to be in encrypted form using the different algorithm. Data authentication should be mandatory for the transmission so the receiver can make sure about the trusted source. Even each data packet that is transmitting over a network must have a unique time stamp to prevent an intruder from reusing data. The combination of encryption, authentication and secure routing is required to keep information far away from the intruder.

Body sensor network devices have a crucial challenge of limited power and limited data storage capacity. The gateway devices handle the authentication and firewall securities. The body sensor network devices require a physical security to prevent from steal or tampering. Only authorized and skilled staff should handle the health monitoring devices, and the patient must have to be strongly advised against any inherent risks.

CONCLUSION

With the extent benefit of constant health monitoring some limitations are also crucial aspects of body sensor networks. The power optimization, battery life performance of the device, reliability, usability and data security are the major limitations of body sensor networks. Researchers and the medical experts are collaboratively devoting their time and energy to overcome from these limitations. For persistent availability and data integrity in a BSN context, a low-weight, energy-efficient, and highly secure authentication mechanism is required. As the gateway node has abundant processing, memory, communication, and power capabilities, the majority of the cognitive work is performed by the gateway.

REFERENCES

[1] J.I. Bangash, A.H. Abdullah, M.H. Anisi and A.W. Khan, "A survey of routing protocols in wireless body sensor networks", Sensors, vol. 14, no. 1, pp. 1322-1357, 2014.

[2] S. Warren, E. Jovanov, `The need for rules of engagement applied to wireless body area networks', Proceedings Of the 3rd IEEE Consumer Communications and Networking Conference, (CCNC), (2006); Las Vegas, Nevada, pp. 979-983.

[3] 802.15.6-2012 – IEEE Standard for local and metropolitan area networks – Part 15.6: Wireless Body Area Networks.

[4] S. Movassaghi, M. Abolhasan, and J. Lipman, `A Review of Routing Protocols in Wireless Body Area Networks', Journal of Networks (2013), Vol. 8, No.3, pp. 559-575.

[5] D. Djenouri and I. Balasingham, `New QoS and Geographical Routing in Wireless Biomedical Sensor Networks', Proceedings of 6th International Conference on Broadband Communications, Networks, and Systems (2009) September 14-16; Madrid, Spain, pp. 1–8.

[6] M. A. Razzaque, C.S. Hong, and S. Lee, `Data-Centric Multiobjective QoS-Aware Routing Protocol for Body Sensor Networks', Sensors (2011), Vol. 11, No.1, pp. 917-937..

[7] "World population prospects: the 2015 revision key findings and advance tables", Working Paper No. ESA/P/Wp, pp. 241, 2015.

[8] S. Ullah, H. Higgins, B. Braem, B. Latre, C. Blondia, I. Moerman, et al., "A comprehensive survey of wireless body area networks", Journal of medical systems, vol. 36, no. 3, pp. 1065-1094, 2012.

[9] R. Cavallari, F. Martelli, R. Rosini, C. Buratti and R. Verdone, "A survey on wireless body area networks: technologies and design challenges", IEEE Communications Surveys & Tutorials, vol. 16, no. 3, pp. 1635-1657, 2014.

[10] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith and A. Jamalipour, "Wireless body area networks: A survey", IEEE Communications Surveys & Tutorials, vol. 16, no. 3, pp. 1658-1686, 2014.

[11] "IEEE 802.15.6 Regulation Subcommittee Report" (doc. IEEE P802.15–08–0034–12-0006).

[12] A. Bag and M.A. Bassiouni, "Energy efficient thermal aware routing algorithms for embedded biomedical sensor networks", 2006 IEEE International Conference on Mobile Ad Hoc and Sensor Systems, pp. 604-609, 2006, October.

[13] A. Bag and M.A. Bassiouni, "Routing algorithm for network of homogeneous and id-less biomedical sensor nodes (RAIN)", Sensors Applications Symposium 2008. SAS 2008. IEEE, pp. 68-73, 2008, February.

[14] M.M. Monowar and F. Bajaber, "On designing thermal-aware localized QoS routing nrotocol for in-vivo sensor nodes in wireless body area networks", Sensors, vol. 15, no. 6, pp. 14016-14044, 2015.

[15] Cleophas D.K Mutepfe, Clement Nyirenda, "Comparative Analysis of MAC Protocols in a Mobility Aware Wireless Body Area Network", 2018 Open Innovations Conference (OI), pp.8-12, 2018.

[16] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao and V. C. Leung, `Body Area Networks: A Survey', Mobile Network Applications (2011), Vol. 16, No.2, pp.171-193.

[17] M. Patel, and W. Jainfeng, `Applications, challenges, and prospective in emerging body area networking technologies', IEEE Wireless Communications (2010), Vol.17, No. 1, pp. 80-88.

[18] B. Latr , B. Braem, I. Moerman , C. Blondia, E. Reusens, W. Joseph and P. Demeester, `A lowdelay protocol for multihop wireless body area networks', Proceedings of Mobiquitous (2007) August; Philadelphia, pp. 1-8.

[19] Liu Jingwei , Zhang Zonghua, Sun Rong and Kyung Sup kwak, `An Efficient Certificateless Remote Anonymous Authentication Scheme for Wireless Body Area Networks', Proceedings of IEEE International Conference on Communications(ICC) (2012) June 10-15; Ottawa, ON, pp. 3404-3408

[20] 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

[21] Mathur, S., Miller, R., Varshavsky, A., Trappe, W., & Mandayam, N. (2011). Proximate: Proximity-based secure pairing using ambient wireless signals. In Proceedings of the 9th International Conference on Mobile Systems, Applications, and Services (pp. 211–224).

[22] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3690007/ A Survey of Body Sensor Networks - PMC (nih.gov)

[23] Singh, K., Muthukkumarasamy, V. (2007). "Authenticated key establishment protocols for a home health care system. In Proceedings of 3rd International Conference on Intelligent Sensors, Sensor Networks and Information (ISSNIP'07) (pp. 353–358).

[24] Z. Khan, S. Sivakumar, W. Phillips and B. Robertson, `QPRD: QoS-Aware Peering Routing Protocol for Delay Sensitive Data in Hospital Body Area Network Communication', Proceedings of 7th International IEEE Conference on Broadband, Wireless Computing, Communication and Applications (BWCCA) (2012) November 12-14; Victoria, BC, Canada, pp. 178–185.

[25] Z. Khan, S. Sivakumar, W. Phillips, and B. Robertson, `A QoS-aware Routing Protocol for Reliability Sensitive Data in Hospital Body Area Networks', Procedia Computer Science (2013), Vol. 19, pp. 171- 179