Volume 5, Issue 9, September 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Wireless Body Area Network– A Study

Prameela.S, P. Ponmuthuramalingam
Department of Computer Science, Government Arts College,
Coimbatore, Tamil Nadu, India

Abstract—Wireless body area networks are the promising key areas in wireless sensor networks which are capable of collecting continuous real time health data of patients, process, aggregate, store and sent to centralized healthcare database. The data sent has to be accurate, reliable, confident and so secure data discovery and dissemination becomes vital .In this paper Wireless body area network data dissemination and security is analysed.

Keywords—WSN, WBAN, Data Dissemination, Security, Privacy.

I. INTRODUCTION

Wireless sensor network are spatially distributed autonomous devices, denoted as sensor nodes which are capable of sensing, computing, communicating with each other wirelessly. These sensor nodes are usually small, inexpensive, lightweight, and low power. Each sensor node is tightly constrained in computation capability, storage capacity, and energy consumption, a large number of these tiny devices can collaboratively execute complex tasks. Wireless sensor networks have varied applications in fields of environment monitoring, warfare, agriculture, and healthcare.

A. Overview of Wireless Body Area Networks

Wireless Body area network (WBAN) is a wireless network of wearable computing and implantable body sensor devices. A WBAN is a wireless network of tiny and smart sensors which are attached to or entrenched in a patient to monitor his physiological activities and actions [1]. These Wireless sensor Node (WSN) sensors gather related data from patients and communicate through the gateways which in turn perform data processing, aggregation and distributed storage and these data from all wireless Body area networks are sent to a centralized healthcare database. This is an effective way to gather and provide constant real-time health and movement related information of patients to medical staff [1] with security measures in data discovery and dissemination. Wireless body area networks mostly deployed in the medical centres. The difference between WBAN and WSNs are listed as follows:

1. *Deployment and Density:* WBAN nodes are either wearable or implantable in the human beings .Redundant nodes are not deployed in WBAN for coping up with the failure of nodes. In WSN more nodes are placed to cope up with node failures.
2. *Data Rate: W*BAN are used for registering human activities and actions. These activities sends data at periodic and at stable rates. In WSN the activities are event based and it may occur at irregular intervals.
3. *Mobility :* WBAN nodes are mobile while WSN nodes are stationery.
4. *Latency:*It necessary to maximize battery life of WSN as it is physically unreachable; replacement of batteries in WBAN nodes is comparatively easy.

There are several advantages in using WBANs which include

Flexibility: The sensors are used for monitoring of physiological readings which are propagated to nearby devices such as cell phone, laptop, Personal Digital Assistant (PDA) based on the needs of application being used.

Effectiveness and efficiency: The batteries used are low power consuming and they last long due to the low power consumption .These body sensors provide reliable and accurate data effectively.

Cost-effective: As more and more sensor is mass produced for medical environment they have become cost effective.

Biocompatibility: Biocompatibility is a must for implanted sensors and to also for some external sensors. It is not of much importance in WSN

Security: Security should be comparatively higher in WBAN as it deals with patient's information. Data loss is more significant.

Energy scavenging Source: Wind and solar energy are energy sources for WSN but in WBAN vibration caused due to movement in body and the heat generated by this motion are the sources of energy.

II. CHARACTERISTICS OF WBAN

A. Types of Nodes in a WBAN

Nodes in WBAN are an independent device. They are classified into different groups based on Functionality, Implementation and Role of the node

Table 1. Types of nodes in WBAN

Functionality	Personal device	Sensor	Actuator
Implementation	Implant node	Body surface node	External node
Role	coordinator	End nodes	Relay

1. Functionality: Personal Device (PD device which is called as Body gateway, sink, Body Control Unit (BCU) or PDA. It helps in collecting information from sensors and actuators and in interactions with other users. [3]. WBAN Sensors measure certain parameters like temperature, Blood Pressure in one's body. On responding to physical stimuli these nodes process data and provide information. [4], [5].On receiving data from the sensors the actuator interacts with the user and provides feedback by acting on the sensor data. [3].

2. Implementation within the body

Implant Node is planted in the human body, either immediately underneath the skin or inside the body tissue. Body Surface Node is either placed on the surface of the human body or 2 centimetres away from it. External Node are nodes not in contact with the human body and remains a few centimetres to 5 meters away from the human body. [6][7].

3.Role in Network

The coordinator node is like a gateway to the outside world, another WBAN, a trust centre or an access coordinator. This coordinator of a WBAN is the PDA, through which all other nodes communicate. The end nodes in WBANs are limited to performing their embedded application. The intermediate nodes are called relays. They have a parent node, possess a child node and relay messages.

B. Number of Nodes in a WBAN

According to the drafts of IEEE standards, the number of nodes in a WBAN is a few actuators or sensors communicating with a portable handset reaching up to tens to hundreds of actuators or sensors communicating with a gateway to the Internet. But in practice the actual number of nodes varies based on the application environment [2].

C. Topology of WBANS

The IEEE 802.15.6 working group has considered WBANs to operate in either a one-hop or two-hop star topology [3] .Two feasible types of data transmission exist. In the one-hop star topology transmission from the device to the coordinator and transmission from the coordinator to the device exists. In a multi-hop architecture nodes are connected to access points via other nodes

Standards used for WBAN Communication are

A. IEEE 802.15.1 (Bluetooth) Bluetooth has high bandwidth, low latency , used for short range up to 10metre communication with a data rate of is a short range 3 Mbps. Currently it supports mobile platforms . The disadvantage is that power consumptions in high.[4]
B. ZigBee the most commonly used standard is Zigbee .It can manage complex communications in low power devices Power consumption is low and data rate 250 kbps. It has the capability to handle complex communication in low power communication devices. Hardware support with encryption is featured by many ZigBee controllers to provide effective protection for communication in WBAN [4].
C. Medical Implant communication service (MICS) is designed especially for WBAN. It is short range communication with multi hop structure. Due to its very low power radiation it is suitable for heath monitoring systems[4]

D. Communication Architecture of WBANs

The communication architecture of WBANs can be separated into three different tiers as follows:

Tier-1: Intra-WBAN communication

Tier-2: Inter-WBAN communication

Tier-3: Beyond-WBAN communication

1.Tier-1: Intra-WBAN communication

Intra WBAN Communication shows the transmission range and the nodes interactions in and around the body. The processed data is passed on to Tier -2.

2. Tier-2: Inter-WBAN communication

This communication tier is between the PS and one or more access points (APs). The Access points are placed in order to handle emergency situations. It interconnects WBANs with various networks.

3. Tier-3: Beyond-WBAN Communication

The design of this communication tier is for use in metropolitan areas. A gateway such as a PDA can be used to bridge the connection between Tier-2 and this tier. However, the design of Tier-3 for com

III. PRINCIPLES OF WBAN

Wireless Body sensors Networks are used to automatically monitor physiological readings, which can be forwarded to a nearby processing device, referred to as the controller or base station, such as a smart phone, a wrist watch, a tablet PC, a laptop PC, or a robot, based on the application needs. Packets broadcast by the base station can be received by each body sensor through one or two hops.

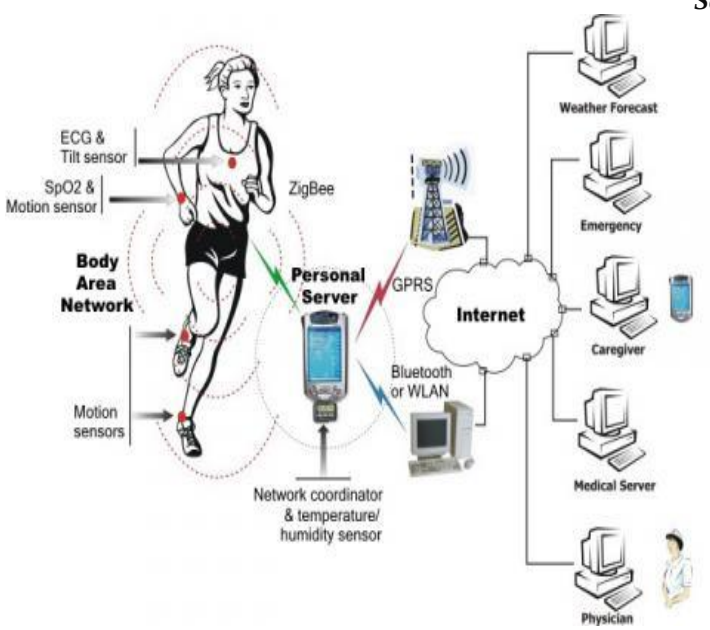

Fig 1. Architecture of Wireless body Area Network [16]

This two-tier architecture confirms the features of a WBAN such as communication, resource, deployment, density, and mobility characteristics as shown in the figure 1. Moreover, such a two-tier architecture is indispensable for increasing overall network capacity and scalability, reducing system complexity, prolonging network lifetime, and ensuring the security and privacy. With respect to disseminating data items, sensors of practical WBANs are at most three hops away from the base station.

IV. APPLICATIONS OF WBANS

WBANS have various applications in medical as well as Non-Medical field. In Medical field WBAN can be Wearable, Implantable or used for remotely controlling the medical devices. Wearable WBANS or On-body medical applications include monitoring of blood pressure, temperature, respiration, electro cardiogram, and On-body non-medical applications include evaluating soldier tiredness in battle field, monitoring forgotten things, a social network, ,sports training, stages of sleep, Asthma[10].Implantable or In-body applications include, monitoring and reconfiguration of pacemakers and implantable cardiac defibrillators, bladder function control , retinal implants. .Non-Medical WBAN are used in real time streaming, entertainment applications

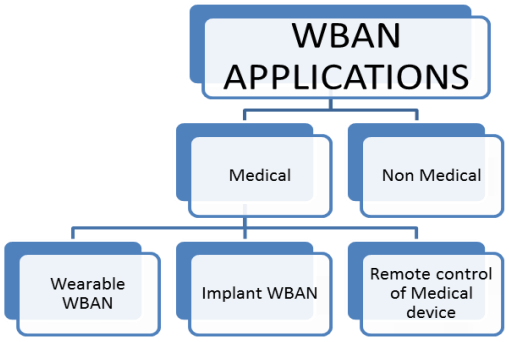

Fig 2. Applications of WBAN

Stages of the Wireless body sensor Network is as follows

In WBAN and other Functional WSN, each node has some common variables stored in the network. The data discovery and dissemination protocols get these variables from such nodes and then add, delete, modify them to maintain data consistency across the network [1].

A. Data Collection

Each data item contains a unique key to identify the variable (i.e., parameter or command) that it aims to update, and a value to reflect its freshness. In Drip, each data item is formatted as a three-tuple (key, version, data), in which key identifies uniquely the concerned variable, version indicates whether the data item is new (a larger version means a newer data), and data denotes the disseminated value for the concerned variable.

B. Data dissemination

A node needs to periodically broadcast a summary of its stored data, unless the same summary has been received recently. If a node receives an older summary from its neighbouring node, it will update the neighbouring node

with the latest summary. To save energy, when the data in all nodes are consistent, the broadcast interval is increased exponentially. However, when a node has new data, it will report more quickly, when new data are injected by the base station.

C. Data discovery and dissemination protocols

The Data discovery and dissemination protocol configures parameters or manages distribution of commands queries and distribute reliable and confident data through the wireless link. They are of two types Code dissemination protocols [9] are developed to efficiently distribute long messages into a network, enabling complete system reprogramming. On the other hand, data discovery and dissemination protocols are used to distribute short messages, such as several two-byte configuration parameters, Common uses of this kind of protocols include injecting small programs, commands, queries, and configuration parameters.

V. CHALLENGES IN WBAN

In practice, WBANs may be subject to malicious attacks from external attackers. By placing an intruder node or compromising a node of the WBAN, an adversary could possibly modify or replace the legitimate data being propagated in the WBAN. Furthermore, an adversary can reboot the whole network with wrong data data* by injecting a fake data item (key, version, data*) to the network where version is larger than all version numbers of the concerned variable stored on the body sensor nodes. Alternatively, the adversary can even erase an important variable identified by key from all sensor nodes by sending the data item (key, version, 0) using a data discovery and dissemination protocol, where version is a large enough number.

A. Security Challenges

Security is more critical Issue and highly prioritized in the Wireless body area network compared to traditional networks for data discovery and data dissemination. Types of attacks which can make system vulnerable either through external and internal attacks as follows

1. *Eavesdropping attack :*The disseminated data items are easily intercepted. Leakage of important information may lead to serious consequence. For example, if an adversary eavesdrop a small program, update, can attack the WBAN by exploiting potential bugs in the program update.
2. *Distributed Denial of service attack :* Adversaries can easily exploit this feature by launching Denial of service attacks to drain the resources of body sensor nodes from their intended functions. For example, an adversary can inject large volume of counterfeit data items to the WBAN, effectively exhausting the energy of body sensor nodes to process the bogus data items [10].
3. *Data inference :* It is process by which data is analysed in order to illegitimately gain knowledge about a subject or patient. Hence considerable effort is required to make the routing and data transmission secure in Wireless body area network while data dissemination.
4. *Confidentiality*: Ensuring protection of sensitive information without revealing to unauthorized third party.
5. *Authentication*: Sensor nodes and base stations should have the capacity to verify that the data sent and received are from trusted sender and not by an adversary who has tricked the legitimate nodes to accept false data as legitimate data [5].
6. *Integrity* : Integrity controls implies that the information are received without being intercepted and modified in the process.
7. *Freshness:* Data freshness means the messages are fresh and that they neither reused or nor redundant [6].
8. *Interoperability challenges*: WBAN systems should ensure seamless data transfer across standards such as Bluetooth, Zigbee etc. to promote information exchange, plug and play device interaction. Further, the systems should be scalable, ensure efficient migration across networks and offer uninterrupted connectivity. [15]
9. *Device Component Complexities*: The sensor nodes in WBAN should be of light weight, low in power consumption, easy to use, reconfigurable, tiny in size, and less complex. The storage devices need to facilitate remote storage and viewing of patient data as well as access to external processing and analysis tools.
10. *Data consistency challenges related data fusion (reliability*):Data has to be collected from patient nodes a, mobile devices should be analysed in fusion mode. The data of the patients which are available in fragments in various systems like laptops personal computers need to be aggregated. The medical staff attending should have the complete details about the patient or the quality of care given may degrade.
11. *Node Interference issue :* Throughout data transmission and discovery, the body sensors wireless links should reduce interference
12. *Constrained deployment:* The WBAN needs to be wearable, lightweight and non-intrusive [15]
13. *Consistent :* WBAN performance should be accurate and consistent from source to destination node. Sensor measurement, personal server, wireless links performance should be consistent, robust and also secure even in adverse environment.

B. Privacy Issues

Privacy is an important concern in wireless body area networks as the health related data of an individual is private in nature. First of all it necessary to obtain consent from patients in data transfer. The physicians, nurses and some

other clinical and technical staffs are the users of the data. In emergency situations, disasters or remote patient monitoring disclosure of information to save the patient life is unavoidable.

1. Users privacy can be protected by encrypting of messages.
[11].
2. Specific users should not be identified unless necessary.

C. Regulations and Laws

Regulations and acts for Protecting security and privacy varies greatly from country to country.

American Health Insurance Portability and Accountability Act of 1996 (HIPAA) [12] and the Health Information Technology for Economic and Clinical Health Act (HITECH) [13].

HIPAA standardizes many rules which are to be followed by medical staff. Complete security for administration, protecting of data becomes necessary.

Commercially obtaining and revealing, spiteful harming of patients information is severely punishable. Furthermore medical providers must guarantee that their system, and those of their business associates, ensures [14] the following:

- Patient's health information should not only be secure and confident but also in proper format.
- Protection against any breach in security, confidentiality and integrity.
- Only Authorised access to patient health information
- Further HIPAA regulates some other areas:
- Authenticated data users...
- Authorised user access to data.
- Level of Authorisation for sensitive data.
- Maintain integrity of data throughout life cycle of system.

VI. CONCLUSION

The characteristics, applications and challenges in Wireless body area networks are discussed in this paper. Security and privacy issues in data transfer has to be resolved, further the sensitive data collected by WBANs should be securely transferred through authenticated source to the authorized personnel for providing quick better and quality care to patient.

REFERENCES

[1] Daojing He, Sammy Chan, Yan Zhang,and Haomiao Yang,"Lightweight and Confidential Data Discovery and Dissemination for Wireless Body Area Networks", *IEEE Journal of Biomedical And Health Informatics*, Vol. 18, NO. 2, pp.440-448,March 2014.

[2] Samaneh Movassaghi, Mehran Abolhasan , Justin Lipman David Smith, Abbas Jamalipour, "Wireless Body Area Networks: A Survey", *IEEE Communications Surveys & Tutorials*,2013[3]

[3] R. Shah and M. Yarvis, "Characteristics of on-body 802.15.4 networks,"in *2nd IEEE Workshop on Wireless Mesh Networks (WiMesh)*,pp. 138 –139, Sept. 2006.

[4] Emil Jovanov, et al., Body Area Networks for Ubiquitous Healthcare Applications: Opportunities and Challenges", *J Med Syst*(2011) 35:1245-1254

[5] J Latr´e, B. Braem, I. Moerman, C. Blondia, and P. Demeester, "A survey on wireless body area networks," *Wirless Network*, vol. 17,pp. 1–18, Jan. 2011

[6] M. Hanson, H. Powell, A. Barth, K. Ringgenberg, B. Calhoun, J. Aylor,and J. Lach, "Body area sensor networks: Challenges and opportunities," *Computer*, vol. 42, pp. 58 –65, Jan. 2009.

[7] J. Xing and Y. Zhu, "A survey on body area network," in *5th Int.Conf.on Wireless Communications, Networking and Mobile Computing(WiCom '09)*, pp. 1 –4, Sept. 2009.

[8] C. Tachtatzis, F. Franco, D. Tracey, N. Timmons, and J. Morrison, "An energy analysis of IEEE 802.15.6 scheduled access modes," in *IEEEGLOBECOM Workshops (GC Wkshps)*, pp. 1270 –1275, Dec. 2010.

[9] D. He, S. Chan, S. Tang, and M. Guizani, "Secure data discovery and dissemination based on hash tree for wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 12, no. 9, pp. 4638–4646, Sep. 2013

[10] K. Malasri and LWang, "Design and implementation of a secure wireless mote-based medical sensor network," *Sensors*, vol. 9, no. 8, pp. 6273–6297, 2009.

[11] Office for Civil Rights, United State Department of Health and Human Services. Medical Privacy. National Standards of Protect the Privacy of Personal-Health-Information. Available online: http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html

[12] Health Information Technology for Economic and Clinical Health Act (HITECH). Available online: http://waysandmeans.house.gov/media/pdf/110/hit2.pdf

[13] Strong User Authentication and HIPAA: Cost-Effective Compliance with Federal Security Mandates. Available online: http://www.techrepublic.com/whitepapers/strong-user-authenticationand-hipaa-cost-effective-compliance-with-federal-security-mandates/2345053

[14] https://en.wikipedia.org/wiki/Body_Area_Network

[15] Shreyas S. Tote1 , Sameer M. Khupse and Kunal S. Bhutwani, Data Authentication in Wireless Body Area Network (WBAN) Using A Biometric-Based Security ,*IJREST* E-ISSN: 2349-7610 Vol., Special Issue-1, MARCH- 2015

