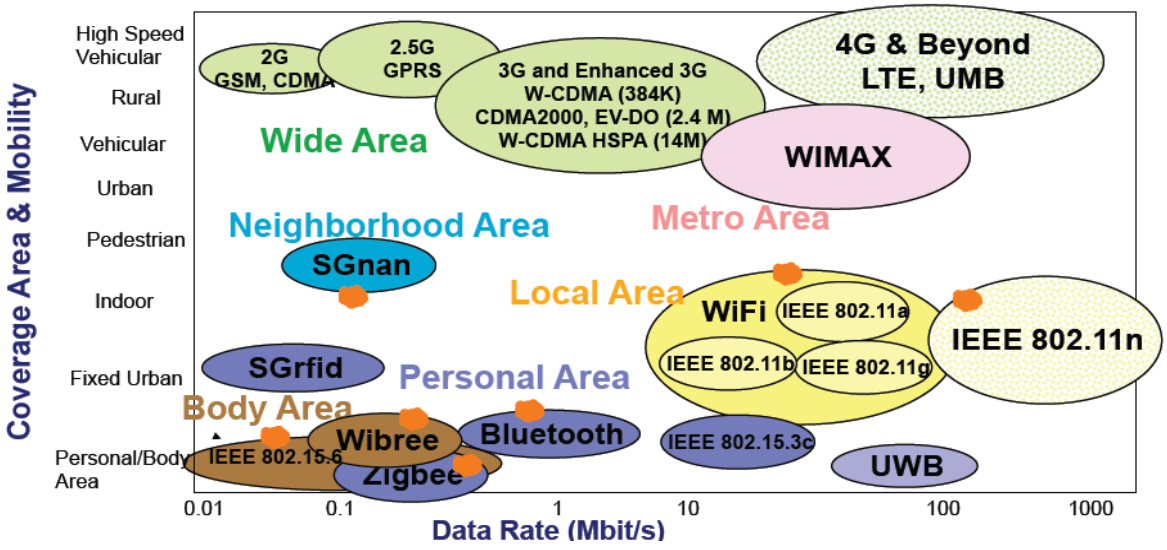
Report Title: WBAN Tutorial

Author: Rana Nazir

Abstract:

Our aim is to provide a tutorial to introduce WBAN and its working knowledge as well as architecture. We will address Emergency health issues and suggest how it can be improved [1].

Its most of the issues are inherit from wireless, as it is using the ISM band, shown in figure.



WBAN is RF based wireless networking technology that interconnects tiny nodes with sensors in, on, or around a human body [2].

A typical WBAN consists of a number of inexpensive, lightweight, miniature sensor platforms, each featuring one or more physiological sensors like [3]

Motion Sensors

ECG (Electrocardiograms)

Sp02

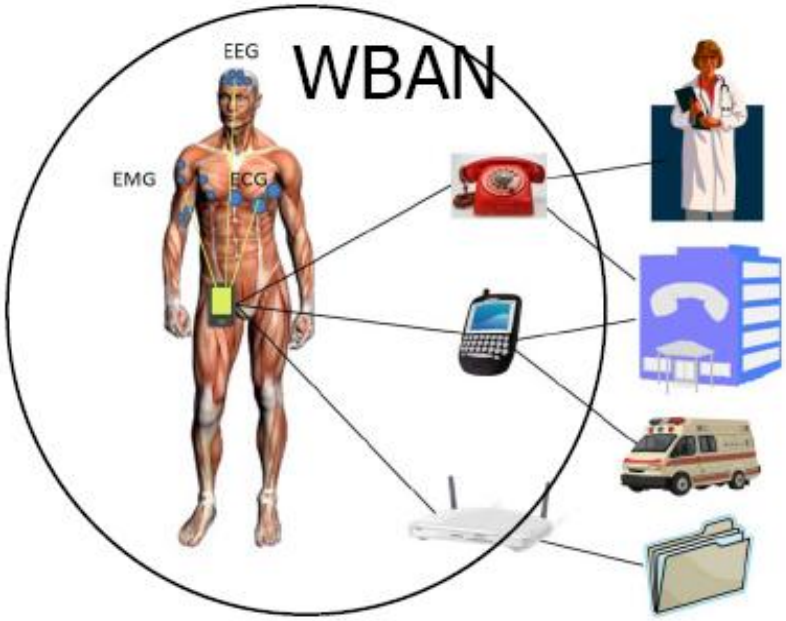
Breathing Sensors

Blood pressure

EMG (Electromyograms)

EEG(Electro-encephalograms)

Blood Glucose Sensors



1. INTRODUCTION

The increase in average lifespan and health cost in many developed nations are catalysts to innovation in health care. These factors along with the advances in miniaturization of electronic devices, sensing, battery and wireless communication technologies have led to the development of Wireless Body Area Networks (WBANs). WBANs consist of smart miniaturized devices (motes) that are able to sense, process and communicate. They are designed such that they can be worn or implanted, and monitor physiological signals and transmit these to specialized medical servers without much interference to the daily routine of the patient. [4] [5]

A WBAN consists of several sensors and possibly actuators equipped with a radio interface. Each WBAN has a sink or personal server such as a PDA, that receives all information from the sensors and provides an interface towards other networks or medical staff. Connecting health monitoring sensors wirelessly improves comfort for patients but induces a number of technical challenges like coping with mobility and the need for increased reliability [6].

An important requirement in WBANs is the energy efficiency of the system. The sensors placed on the body only have limited battery capacity or can scavenge only a limited amount of energy from their environment. Consequently, in order to increase the lifetime of the network, energy efficient measures needs to be taken. From that point of view, several researchers are developing low power sensors and radios. Another possibility is the design of optimized network protocols to lower the energy consumption while satisfying the other requirements [7].

A Wireless Body Area Network consists of small, intelligent devices attached on or implanted in the body which are capable of establishing a wireless communication link. These devices provide continuous health monitoring and real-time feedback to the user or medical personnel. Furthermore, the measurements can be recorded over a longer period of time, improving the quality of the measured data [3]. Generally speaking, two types of devices can be distinguished: sensors and actuators. The sensors are used to measure certain parameters of the human body, either externally or internally. Examples include measuring the heartbeat, body temperature or recording a prolonged electrocardiogram (ECG). The actuators (or actors) on the other hand take some specific actions according to the data they receive from the sensors or through interaction with the user. E.g., an actuator equipped with a built-in reservoir and pump administers the correct dose of insulin to give to diabetics based on the glucose level measurements. Interaction with the user or other persons is usually handled by a personal device, e.g. a PDA or a smart phone which acts as a sink for data of the wireless devices. In order to realize communication between these devices, techniques from Wireless Sensor Networks (WSNs) and ad hoc networks could be used. However, because of the typical properties of a WBAN, current protocols designed for these networks are not always well suited to support a WBAN.

2. WBAN ARCHITECTURE

The WBAN technology is the consequence of the existing WSN technology. A number of tiny wireless sensors, strategically placed on the human body, create a wireless body area network that can monitor various vital signs, providing real-time feedback to the user and medical personnel. In a WBAN, each medical sensor monitors different vital signs such as temperature, blood pressure, or ECG. The system consists of multiple sensor nodes that monitor body motion and heart activity, a network coordinator, and a personal server running on a personal digital assistant or a personal computer [8].

Figure 1 shows secure 3-level WBAN architecture for medical and non-medical applications. Level 1 contains in-body and on-body BAN Nodes (BNs) such as Electrocardiogram (ECG) – used to monitor electrical activity of heart, Oxygen saturation sensor (SpO2) –used to measure the level of oxygen, and Electromyography (EMG) – used to monitor muscle activity [9].

Level 2 contains a BAN Network Coordinator (BNC) that gathers patient's vital information from the BNs and communicates with the base-station. Level 3 contains a number of remote base-stations that keep patient's medical/non-medical records and provides relevant (diagnostic) recommendations. The traffic is categorized into on demand, emergency, and normal traffic. On-demand traffic is initiated by the BNC to acquire certain information. Emergency traffic is initiated by the BNs when they exceed a predefined threshold. Normal traffic is the data traffic in a normal condition with no time critical and on-demand events [11].

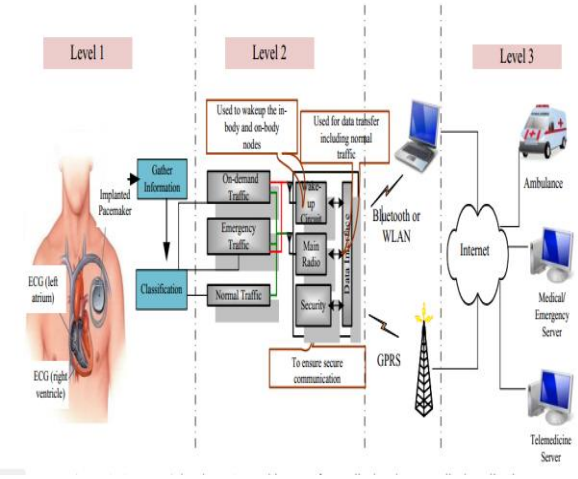


Figure 1: Secure 3-Level WBAN Architecture For Medical And Non-Medical Applications

The normal data is collected and processed by the BNC. The BNC contains a wakeup circuit, a main radio, and a security circuit, all of them connected to a data interface. The wakeup circuit is used to accommodate on-demand and emergency traffic. The security circuit is used to prevent malicious interaction with a WBAN [10], [14], [13].

3. Damage & Costs

1. **Other affecting:** There are many costs associated with denial-of-service attacks. Like an attacker target the server, when server down, it does not only effect the server but also other users and sites associated with that victim server [19].
2. **Bandwidth wastage:** Network resources are shared among many stations. Like bandwidth. If attacker launches DDoS attack it does not only affect the target because of wastage of bandwidth and that also slow down the activity of non-victim systems [21].
3. **Extra network channels:** To detect the attack users must use extra resources only to handle and prevent their system from such kind of attacks. Like emailing, making logs etc.
4. **Insurance& Bandwidth cost:** As in international market we pay per byte. In DoS attack case the traffic is very high from normal traffic and that also increases the bandwidth cost.

4. How to handle DoS

- **Protecting:** The first step should be protected in such kind of attack, protection mechanism should be installed by ISP, and there should be an agreement between ISP, an insurance policy. Most of the people do that after learning a lesson.
- **Detecting:** If you detect properly then you would be able to respond accurately. For detection, there should be proper check and balance on log system, traffic pattern, updated blacklist and all updated detection software. The attacker use different mechanism to launch the attack. So maybe detection not helps out in some kind of attacks [22].
- **Reacting:** Reaction step comes when there is no proper protection and detection mechanism. In that step there would some technical steps which are mostly implemented, are informing ISP, start backup system and moving data to the backup system, decreasing the incoming traffic, applying available data content filters on incoming traffic, redirecting traffic, shut downing after data is moved. [23]

5. Available Solutions

- The DoS attacks at the MAC layer discussed here are very common in the IEEE 802.11 standard networks.
- The attacker exploited mostly the non-implementation of the authentication method for management and control frames.
- Mostly available solutions are cryptographically protecting of management and control frames. In that method first step is finding the vulnerability on the basis of cryptography and then the possible solution to mitigate these attacks.
- IEEE made an amendment to the original standard IEEE 802.11 and releases a new standard 802.11w.It included the security features for management frames like data confidentiality, data origin authenticity, and replay protection [27].
- But for control frames, there are still no cryptographic protection schemes at the MAC layer. So control frames are still vulnerable to DoS attack. An attacker can easily exploit the control frame by spoofing them and then use for resource exhaustion.

- The de-authentication vulnerability, in particular, can be fixed by authenticating control frames explicitly [26].
- De-authentication flooding, in particular, can be mitigated by delaying the effect of requests.
- In RTS DoS attack, the network performance can be restored back by Reevaluate RTS Duration (RRD) technique [25].
- MAC address spoofing can be protected if there is incrimination mechanism implanted in firmware in each node. When a node sends its MAC address there would incrimination after next frame by sender node. Since firmware functionality of wireless card can't be changed by an attacker. The receiver will only accept and response such frames which have incremented MAC [24].

6. References

[1] Z. Haider, M. Saleem, and T. Jamal, "Analysis of Interference in Wireless", in Proc. of ArXiv, arXiv:1810.13164 [cs.NI], Oct. 2018.

[2] T. Jamal and P. Mendes, “Relay Selection Approaches for Wireless Cooperative Networks”, in Proc. of IEEE WiMob, Niagara Falls, Canada, Oct. 2010.

[3] T. Jamal, P. Mendes, and A. Zúquete, “Opportunistic Relay Selection for Wireless Cooperative Network”, in Proc. of IEEE IFIP NTMS, Istanbul Turkey, May 2012.

[4] T. Jamal and P. Mendes, “Cooperative relaying in user-centric networking under interference conditions”, in Proc. of IEEE Communications Magazine, vol. 52, no. 12, pp. 18–24, Dec 2014.

[5] P. Mendes, W. Moreira, T. Jamal, and Huiling Zhu, “Cooperative Networking in User-Centric Wireless Networks”, In: Aldini A., Bogliolo A. (eds) User-Centric Networking. Lecture Notes in Social Networks. Springer, Cham, ISBN 978-3-319- 05217-5, May 2014.

[6] T. Jamal, P. Mendes, and A. Zúquete, “Relayspot: A Framework for Opportunistic Cooperative Relaying”, in Proc. of IARIA ACCESS, Luxembourg, June 2011.

[7] T. Jamal, and SA Butt, "Malicious Node Analysis in MANETS", in Proc. of International Journal of Information Technology, PP. 1-9, Springer Publisher, Apr. 2018.

[8] T. Jamal, and P. Mendes, “COOPERATIVE RELAYING FOR DYNAMIC NETWORKS”, EU PATENT, (EP13182366.8), Aug. 2013.

[9] T. Jamal, and P. Mendes, “802.11 Medium Access Control In MiXiM”, in Proc. of Tech Rep. SITILabs-TR-13-02, University Lusófona, Lisbon Portugal, Mar. 2013.

[10] T Jamal, M Alam, and MM Umair, "Detection and Prevention Against RTS Attacks in Wireless LANs", in Proc. of IEEE C-CODE, Islamabad Pakistan, Mar. 2017.

[11] L. Lopes, T. Jamal, and P. Mendes, "Towards Implementing Cooperative Relaying", In Proc. of Technical Report COPE-TR-13-06, CopeLabs University Lusofona Portugal, Jan 2013.

[12] T. Jamal, P. Mendes, and A. Zúquete, “Interference-Aware Opportunistic Relay Selection”, In Proc. of ACM CoNEXT student workshop, Tokyo, Japan, Dec. 2011.

[13] T. Jamal, "Cooperative MAC for Wireless Network", In Proc. of 1st MAP Tele Workshop, Porto, Portugal, 2010.

[14] T. Jamal and P. Mendes, “Analysis of Hybrid Relaying in Cooperative WLAN”, In Proc. of IEEE IFIP Wireless Days (WD), Valencia, Spain, November 2013.

[15] T. Jamal, and P. Mendes, “Cooperative Relaying for Wireless Local Area Networks”, In: Ganchev I., Curado M., Kassler A. (eds) Wireless Networking for Moving Objects. Lecture Notes in Computer Science, vol 8611. Springer, Cham, (WiNeMo), Aug. 2014.

[16] T. Jamal, and SA Butt, “Cooperative Cloudlet for Pervasive Networks”, in Proc. of Asia Pacific Journal of Multidisciplinary Research, Vol. 5, No. 3, PP. 42-26, Aug 2017.

[17] T. Jamal, P. Mendes, and A. Zúquete, “Wireless Cooperative Relaying Based on Opportunistic Relay Selection”, in Proc. of International Journal on Advances in Networks and Services, Vol. 5, No. 2, PP. 116-127, Jun. 2012.

[18] SA Butt, and T. Jamal, “Frequent Change Request from User to Handle Cost on Project in Agile Model”, in Proc. of Asia Pacific Journal of Multidisciplinary Research 5 (2), 26-42, 2017.

[19] T. Jamal, and P. Amaral, “Flow Table Congestion in Software Defined Networks”, in Proc. of IARIA 12th ICDS, Rome Italy, Mar. 2018.

[20] R. Sofia, P. Mendes, W. Moreira, A. Ribeiro, S. Queiroz, A. Junior, T. Jamal, N. Chama, and L. Carvalho, “Upns: User Provided Networks, technical report: Living-Examples, Challenges, Advantages”, Tech. Rep. SITI-TR-11- 03, Research Unit in Informatics Systems and Technologies (SITI), University Lusofona, Lisbon Portugal, Mar. 2011.

[21] T. Jamal, and P. Mendes, “Cooperative Relaying in Wireless User-Centric Networks”, Book Chapter In: Aldini, A., Bogliolo, A. (eds.) User Centric Networking. Lecture Notes in Social Networks, Springer, Cham, pp. 171–195, 2014.

[22] T. Jamal, P. Mendes, and A. Zúquete, “Design and Performance of Wireless Cooperative Relaying”, PhD Thesis MAP-Tele, University of Aveiro, Oct. 2013.

[23] T. Jamal, P. Mendes, and A. Zuquete, “RelaySpot: Cooperative Wireless Relaying”, in Proc. of MAP-Tele Workshop, Aveiro, Portugal, May 2011.

[24] T. Jamal, and P. Mendes, “Cooperative Wireless Relaying, Key Factors for Relay Selection”, in Proc. of MAP-Tele Workshop, Porto, Portugal, Dec. 2009.

[25] SA Butt, and T. Jamal, “Study of Black Hole Attack in AODV”, in Proc. of International Journal of Future Generation Communication and Networking, Vol. 10, No.9, pp. 37-48, 2017.

[26] T. Jamal, and SA Butt, “Low-Energy Adaptive Clustering Hierarchy (LEACH) Enhancement for Military Security Operations”, In Proc. Of Journal of Basic and Applied Scientific Research, ISSN 2090-4304, 2017.

[27] T. Jamal, and P. Mendes, “RelaySpot, OMNET++ Module”, Software Simulator Extension In Proc. of COPE-SW-13-05, 2013.