SAVONIA

Body Area Network, Standardization, Analysis and Application

Olufemi Ekundayo

Bachelor’s Thesis

Degree Programme in Information Technology

___. ___. ______ ________________________________

Valitse kohde.

SAVONIA-AMMATTIKORKEAKOULU

OPINNÄYTETYÖ
Tiivistelmä

Koulutusala	Tekniikan ja liikenteen ala
Koulutusohjelma	Degree Programme in Information Technology
Työn tekijä(t)	Ekunday Olufemi Adeola
Työn nimi	Body Area Networks; Standardization, Analysis and Application
Päiväys	28 February 2013
Sivumäärä/Liitteet	
Ohjaaja(t)	Mr. Arto Toppinen, Principal Lecturer
Toimeksiantaja/Yhteistyökumppani(t)	University of Eastern Finland

Tiivistelmä

WBAN (Wireless Body Area Network) on sisätiloissa tai ihmiskehon välittömässä läheisyydessä käytettävä lyhyen kantaman langaton tiedonsiirtotapa. Se soveltuu sekä lääketieteellisiin että ei-lääketieteellisiin sovelluksiin. Yleisimmin sitä käytetään lääketieteessä potilaan reaaliaikaisessa diagnosoinnissa. Olemassa olevat lyhyen kantaman tiedonsiirtoteknologiat, kuten Bluetooth, Bluetooth Low Energy (BLE), ZigBee ja Wi-Fi olisivat olleet soveltuvia teknologioita WBAN:lle. Ne ovat kuitenkin suunniteltuja eri käyttötarkoituksiin. Niitä ei ole optimoitu vähäisen virrankulutuksen käyttötarpeisiin, joka on yksi tärkein perusta WBAN-teknologialla. Siksi uusi standardointi WBAN:lle on tarpeellinen.

Tämä opinnäytetyö perehtyy WBAN-teknologiaan ja kuinka ihmiskeho voi lähettää langatonta signaalia, ja siten auttaa potilaan diagnosoinnissa. Opinnäytetyössä selitetään miten eri ihmiskehon asennot vaikuttavat ulostulosignaaliin, ja erityisesti mikä käytännössä vaikuttaa ulostulosignaaliin ihmiskehosta.

Avainsanat
Body Area Networks (BAN), Medical Implant Communication Services (MICS), IEEE802.15.6.

SAVONIA UNIVERSITY OF APPLIED SCIENCES

THESIS
Abstract

Field of Study Technology, Communication and Transport			
Degree Programme Degree Programme in Information Technology			
Author(s) Ekundayo Olufemi Adeola			
Title of Thesis Body Area Networks; Standardization, Analysis and Application			
Date	28 February 2013	Pages/Appendices	
Supervisor(s) Mr. Arto Toppinen, Principal Lecturer			
Client Organisation/Partners University of Eastern Finland			

Abstract

In view of the ever aging society, the increasing world poplulation and the continuous outburst of new epidemics, the need for medical attention is needed like never before. The purpose of this thesis was to study and analyse the new IEEE802.15.6 Body Area Network, and how this technology could help safe lives in the medical world. In this thesis, the Ambu Neuroline 700 single patient surface electrode was used for this analysis. The electrode was connected to the signal generator, and then connected to the human body, and through the human body, it was then connected to the signal analyzer. Through this study, it was observed that the signals generated from a human body are mainly affected by the state of being of the person. Though the position of the person, and the fact that a person is moving or not, may also have a very little effect. The main factor affecting the signal generated from a human body is the state of being of the persons mind, whether he or she is anxious, or scared

Keywords

Body Area Networks (BAN), Medical Implant Communication Services (MICS), IEEE802.15.6.

ACKNOWLEDGMENT

Firstly I will like to thank Mr. Arto Toppinen my supervisor and Mr Iiro Jantunen for their help and support, this work wouldn’t have been completed without your help, so thank you very much. Also special thanks to my parents Mr. & Mrs. Ekundayo. Thank you both for supporting me financially, morally and in every other ways you have supported me throughout my studies. Special thanks also to my brothers and sisters, Bukuola, Arinola and Babatunde Ekundayo, you guys are great. Also my friends Kenneth Irabor Otabor, Adewala Akinfaderin, Okeowo Monisola, and most especially James Oluwatosin. Thank you all for your continuous support and encouragement, I really appreciate your efforts.

This work would not have been complete if not for the help of Mikko S. Niskanen and Adedji Olumuyiwa. You both made your body available for experimental purpose, I really appreciate your sacrifice, Thank you.

TABLE OF CONTENTS

LIITTEET

1. INTRODUCTION

This thesis explains the new short range wireless technology IEEE802.15.6 Body Area Network (BAN). The thesis will be divided into 7 sections, each section describing some very important aspect of the new technology. This thesis will mainly focus on how BAN could be used medically.

Section 2 discusses the short range wireless technologies in general. Bluetooth and ZigBee will also be discussed in this section, because of their similarities with BAN. In addition both of these technologies are used for medical purposes.

Section 3 will discuss BAN standardization and the task group responsible for it standardization. It will also discuss the reason why BAN is a better technology for medical applications and its power consumption.

Section 4 will explain BAN network topology. This section will discuss the MAC sublayer of BAN. This section will also discuss the security structure of BAN.

Section 5 will discuss the physical layer specification of BAN. It includes: Narrowband (NB) PHY, Ultra Wideband (UWB) PHY, and Human Body Communication (HBC).This sections talks about the channels of operation of BAN, as well as other PHY properties of BAN.

Section 6 explains the results of the experiments in this thesis, and the results from another research. It explains how the human body reacts to electrical signal, and how the change in the position of a person could also have an effect on the output signal. Section 7 is a summary of the whole thesis.

2. INTRODUCTION TO WIRELESS NETWORKS

Over the years, the world population has been increasing rapidly and hence there is an increase in the amount of patients needing medical attention. Due to the nature of today's world economy, the government could not meet the budget of each sector including the medical sector. The medical sector have been suffering from limited resources needed for acquiring as many qualified medical practitioners as needed in the hospitals to allow for a smooth operation of every section in the hospital. So in order to meet the increasing demands for need of medical attention, the scientist and engineering need to intervene.

Wireless technology has been a major part of today's world for sometime, It has brought great changes in the way humans communicate between themselves. Wireless technology enables ubiquitous networking for anyone, at any time, and anywhere. The IEEE 802 is the standard committee responsible for the standardization of different wireless technologies. This committee was established in February 1980 hence the number 802. The services and protocols were simplified to just the last two layer of the seven layers OSI model which includes:
The Application, Presentation, Session, Transport, Network, Data link and the Physical layer, but the IEE 802 committee work is only limited to Data link and Physical layer. Data link was further spitted into two sub-layers by the IEEE 802 and these include: LLC Sub-layer, MAC Sub-layer. (Wikipedia 12.102012)

Though the IEEE 802 is responsible for all technologies involving Local Area Networks and Metropolitan Area Networks, it also creates smaller committees within itself for the standardization of each technology and they refer to these smaller committees as Work Group (WG), or Task Group (TG). Each task group is responsible for the standardization of each technology, they define the PHY layer and MAC specifications for the particular technology they are working on. There have been different task groups over the years, and new task groups are setup to address the need of a particular wireless technology. Table 1 lists the different task groups that have been setup over the years, and a short description of their task. (Ryuji, K., Kiyoshi, H., Li, H., & Kenichi, T.. 2008).

TABLE 1. IEEE 802 Task Groups and there Task. (Wikipedia 2012)

Name	Description	Note
IEEE 802.1	Bridging (networking) and Network Management	
IEEE 802.2	LLC	inactive
IEEE 802.3	Ethernet	
IEEE 802.4	Token bus	disbanded
IEEE 802.5	Defines the MAC layer for a Token Ring	inactive
IEEE 802.6	MANs (DQDB)	disbanded
IEEE 802.7	Broadband LAN using Coaxial Cable	disbanded
IEEE 802.8	Fiber Optic TAG	disbanded
IEEE 802.9	Integrated Services LAN (ISLAN or isoEthernet)	disbanded
IEEE 802.10	Interoperable LAN Security	disbanded
IEEE 802.11 a/b/g/n	Wireless LAN (WLAN) & Mesh (Wi-Fi certification)	
IEEE 802.12	100BaseVG	disbanded
IEEE 802.13	Unused	
IEEE 802.14	Cable modems	disbanded
IEEE 802.15	Wireless PAN	
IEEE 802.15.1	Bluetooth certification	
IEEE 802.15.2	IEEE 802.15 and IEEE 802.11 coexistence	
IEEE 802.15.3	High-Rate wireless PAN	
IEEE 802.15.4	Low-Rate wireless PAN (e.g., ZigBee, WirelessHART, MiWi, etc.)	
IEEE 802.15.5	Mesh networking for WPAN	
IEEE 802.15.6	Body area network)	
IEEE 802.16	Broadband Wireless Access (WiMAX certification)	
IEEE 802.16.1	Local Multipoint Distribution Service	
IEEE 802.17	Resilient packet ring	
IEEE 802.18	Radio Regulatory TAG	

IEEE 802.19	Coexistence TAG	
IEEE 802.20	Mobile Broadband Wireless Access	
IEEE 802.21	Media Independent Handoff	
IEEE 802.22	Wireless Regional Area Network	
IEEE 802.23	Emergency Services Working Group	
IEEE 802.24	Smart Grid TAG	New (November, 2012)
IEEE 802.25	Omni-Range Area Network	Not yet ratified

Table 1 sows that each task group was formed for a particular task, each task is unique and hence it needed special attention. The following examples are some of the technologies taken into consideration.

2.1 Bluetooth

Bluetooth is a proprietary open wireless technology standard, ad hoc, terrestrial wireless standard for short range communication. It can also be referred to as a short range wireless communications standards, that defines the data link layer and the application layer to support both voice and data applications. It was proposed to be a low cost, low power, radio based replacement for cable. It range of communication ranges from 1metre to about 100meters depending on the class of the device been used. Bluetooth operates in the globally-unlicensed 2.4GHz ISM-band. (Tjensvold J. M. 2007).

Bluetooth deploys its frequency hopping across the entire band, so as for it to comply with the regulations that guide the use of the ISM band. It uses 79 carriers of about 1MHz bandwidth each to perform the hopping. It allows that every packet is transmitted on a newly chosen frequency, in about 65µs per carrier. This technology has been optimized to allow for large amounts of uncoordinated communication to take place in the same area. Unlike most other ad hoc technologies where all units in ranges use the same channels, Bluetooth allows for independents channels, with each channel serving a limited numbers of users. This was made possible by the use of the Frequency-Hop Spread Spectrum (FHSS) technique. The signal is spread on a large frequency range but only a small bandwidth is occupied instantaneously, avoiding most of the potential interferences in the ISM band. (Matheus, K., Zurbes, S., Taori, R., & Magnusson. 2003) (Maulin, P., & Jianfeng, W 2010)

2.2 ZigBee

ZigBee is a very similar technology to Bluetooth. It is an IEEE802.15.4 short range wireless standard, which operates in the 868MHz, 915MHz, and 2.4GHz, ISM band. It is optimized for industrial sensors, smart grids, and low-duty cycle operation for sensing devices. It has been used lately in medical applications. This is the closest short range wireless technology to BAN in terms of its medical applications. (Tjensvold J. M. 2007) (Maulin P., et al. 2010)

2.3 Body Area Networks IEEE802.15.6

All of these above mentioned technologies seem like a very good and competent technology to be implemented in BAN. But just like these technologies where designed for some particular reasons, with some certain specifications, to fulfil some certain needs. BAN will also be designed in this manner. The IEE802.15.6 task group also put into considerations some of the properties of the pervious short range wireless technology and how they could be implemented into this new technology: (Anuj, B., & Ariton, X. 2011)

- Bluetooth technology was optimized for voice link.
- ZigBee is optimized for industrial smart grids, etc
- While Wi-Fi is optimized for data network.

Also these already existing short range wireless standards carry significant overhead. Most importantly when these technologies where designed, the task group responsible for these technologies did not have any other applications in mind, they designed the technology for its own optimum used to serve the reason it had been designed. Though most of these technologies might have a lot in common and hence the thought of making just little modifications to these already existing technologies, and then they would serve perfectly for BAN applications might come to mind. But these might work fine to an extent, it cannot work to the optimal, it would only be a short term solution. Considering all the requirements for BAN, none of the already existing short range wireless technology would serve as permanent solution to BAN. (Anuj, B., et al. 2011)

3. BAN STANDARDIZATION

Body Area Networks, BAN is defined as a communication technology which is optimized for low power consumption. It is able to operate either inside a human's body, on a human's body, or in close vicinity of the human body. Figure 1 shows an example of BAN used medically, though its application is not limited to medical application alone. (Anuj, B., et al 2011)

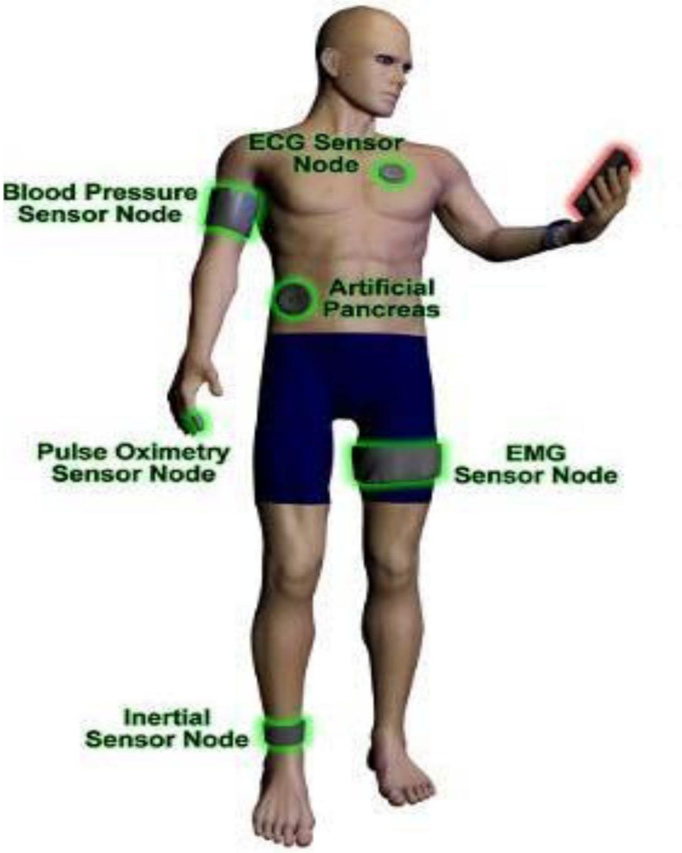

FIGURE1. Example of Medical BAN (Anuj, B., et al 2011)

As shown in Figure 1, the sensor could be place in any part of the human body, whether it's the chest, the arm, or the thigh. The sensor can also work effectively when placed inside the human body.

Vital information is being collected from a patient continuously and this information is being sent to a monitoring device for further analysis. This really helps to monitor the patient all the time, and whenever the data being read by the monitoring devices signifies any problem with the patient being monitored, an alert is sent to the doctor requesting that a patient needs urgent medical attention. This technology could help save a lot of lives. Unlike the traditional routine in the hospitals, whereby nurses check on each patient couple of times in a day, in this case all patients are being monitored at all times with the help of BAN. BAN could also be used to monitor and help patients with disabilities. (Monto´ n, E., Hernandez, J. F., Blasco, J. M., Herve´, T., Micallef, J., Grech, I., Brincat, A. & Traver, V. 2008) (Schmitt, L., Falck, T., Wartena, F., & Simons. 2007). (Otto, C., Milenkovic A., Sanders C., & Jovanov, E.. 2006).

3.1. BAN Application

BAN application is not only limited to medical applications alone, it also has non-medical applications like gaming, data file transfer, social networking applications as shown in Figure 2. Though BAN is mainly optimized for medical applications, but it is still a short range wireless technology and it can perform most the function as most of the already existing technology could. (Kwak K. S.,, Ullah, S., & Ullah, N. 2010)

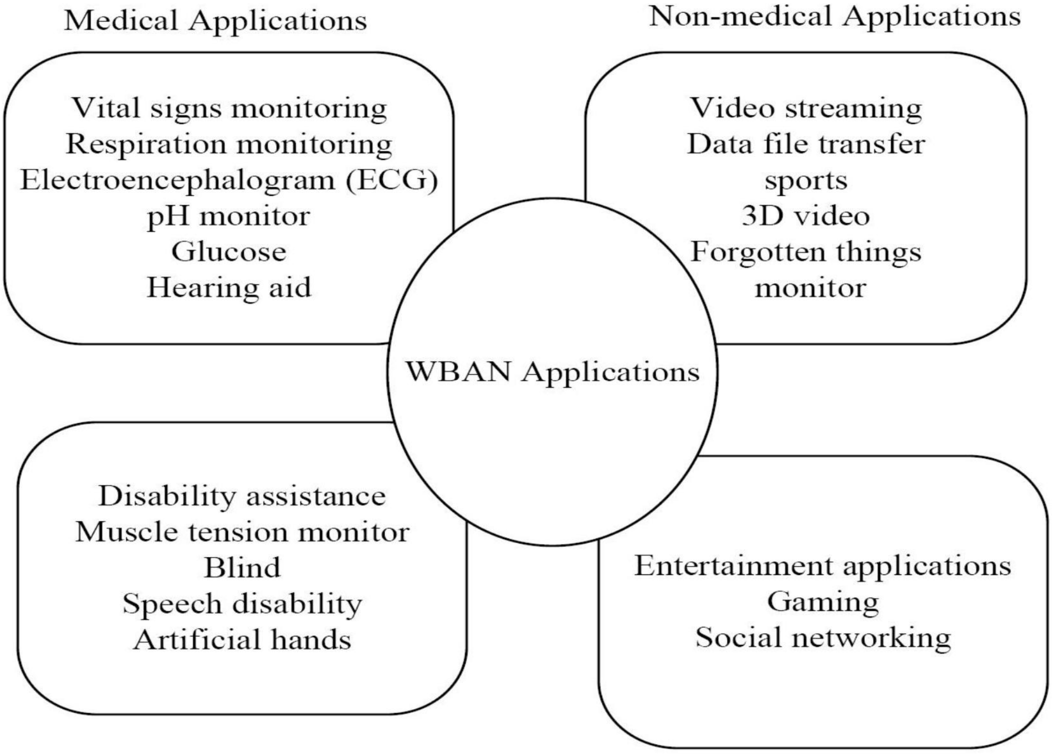

FIGURE 2 BAN Applications (Kwak, K.S., et al 2010)

3.2. BAN Standardization Task Group

The standardization task group for BAN was setup in December 2007. The task group was mainly focus on the medical application part of the technology, though there are some other members of the group who are also working on the non-medical part of the technology. It is most likely that both the medical and non-medical application of BAN would be able to support same PHY, but due to the requirements involves for medical application, the security, QoS, and the MAC who be different for both applications. Table 2 shows some characteristics of BAN as compared with some other IEEE802.15 wireless standards. (Li, H., Takizawa, K., & Ryuji, K. 2008)

TABLE 2. BAN Standard as compared to other 802.15 Wireless Standards (Ryuji, K., et al 2008)

Characteristics	IEEE802.15 Standards	BAN
Configuration	15.3, 15.4, MAC	Single Scalable MAC with reliable delivery.
Power Consumption	Averagely Low Power Consumption	Very low power consumption.
Power Source	Conventional power source.	Compatible with body energy scavenge operation.
Requirements (QoS)	Low Latency	Guaranteed and reliable response to external stimuli
Frequency band	ISM	MICS, ISM, WMT
Channel	Air	Air, Around human

		body, Inside human body.
Safety for human body	Not required	Required e.g. SAR

As shown in Table 2, due to the medical application of BAN, it has a different frequency band (Medical Implant Communication Service (MICS) Band), as compared to the other IEEE802.15 standards. One very important characteristics of BAN is its safety to human body, and this have a very high priority in this wireless technology. This is because it has to comply with the MICS frequency band. As a result of this, parameters like Specific Absorption Ratio (SAR) need to be taken very seriously.

3.3. BAN Task Group Responsibilities

Wireless technologies such as Bluetooth, Wi-Fi and ZigBee achieve so much success due to their standardization. That is because standardization will help to bring down the cost of BAN enabled devices. Standardization helps bring down the cost by exploiting economics, scale, and it also allows for interoperability and seamless user experiences. It help to free consumers from being vendor dependent, that is with standardized technology, consumers could always chose from different manufacturers, that is best suited for their needs. (Maulin, P., et al 2010)

The factors that really affect the success of a technology in the consumer market are, cost, interoperability, and user convenience. Because what will be point of having a device whose price is very cheap but too complicated or sophisticated to use, or vice versa. Most people would rather do with the cheaper devices that could serve almost the same function. The Task Group responsible for the standardization of BAN (IEEE802.15.6 Task Group) is therefore developing a standard encompassing PHY and MAC layer for BAN. This standard that is being developed is expected to consume very low power as well as fill the gap in the data rate vs. peak power graph. This is shown in Figure 3. (Ryuji, K., et al 2008)

3.4. Power Consumption

Technological advances in lower power RF will help to significantly lower the peak power consumption, in the process this could bring to reality small low-cost disposable sensor. Because some other technologies likes Bluetooth, and ZigBee have already so much success in the consumer market and are also being used already for medical purposes, there is much doubt as to whether the new IEE802.15.6 standard could outperform these already established standards. (Anuj, B., et al 2011)

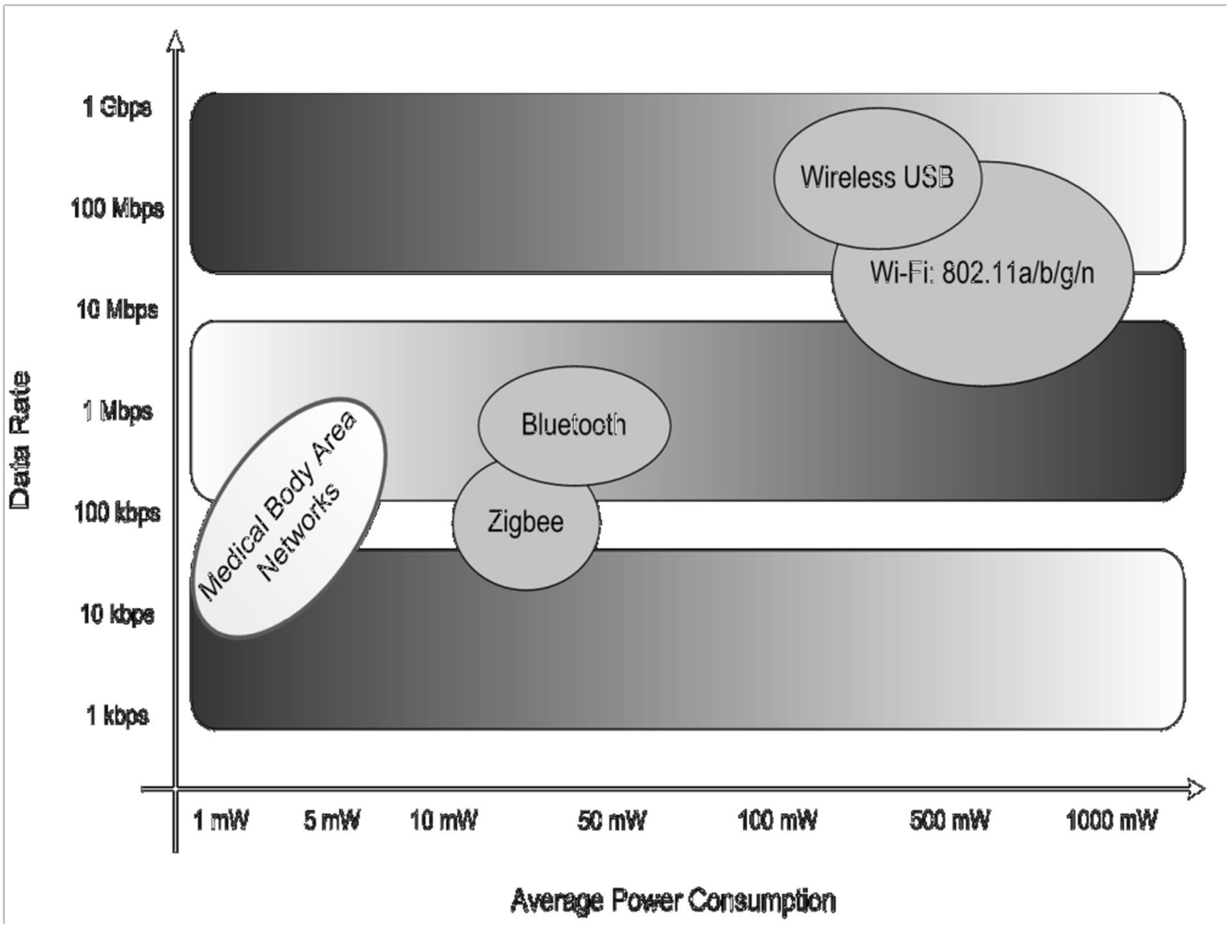

FIGURE 3. Target Position of BAN (Anuj, B., et al 2011)

4. NETWORK TOPOLOGY

In BAN topology the nodes and hubs are arranged in logical sets. There is usually only one hub in a BAN, but the numbers of nodes in a BAN ranges from 0 to mMaxBANSize. In a one-hop star BAN topology, exchange of frame occurs directly between hubs and nodes. While in a two-hop star BAN topology, exchange of frames occurs via a relay-capable node. Figure 4 shows a One-hob star BAN topology: H represents Hob while N represents Node. (IEEE Computer Society 2012)

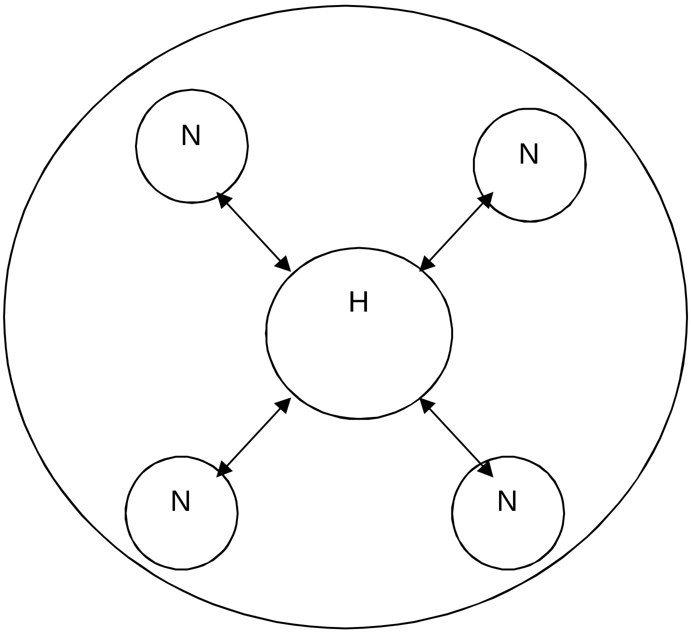

FIGURE 4 One-Hop Star BAN Network Topology (IEEE Computer Society 2012)

The hubs and nodes are partitioned internally into a physical (PHY) layer and a medium access control (MAC) sublayer. This is in accordance with the IEEE 802 committee reference model. As specified in this standard, the hub and node communicate directly in the PHY layer and MAC sublayer. At any given time, both the PHY layer and the MAC sublayer of a hub or a node are to use only one channel. Message security takes place at the MAC sublayer, while security key generations occur inside or outside the MAC sublayer. Within a hub or a node, through the MAC service access point (SAP) situated just above the MAC sublayer, MAC provides its services to the MAC client, also the PHY through the PHY SAP provides its service to the MAC located between them. The MAC client on transmission passes the MAC service data units (MSDUs) to the MAC sublayer through the MAC SAP. Also through the PHY SAP, the MAC sublayer passes MAC frames which could also be prefers to as MAC Protocol data units (MPDUs) to the PHY layer. On reception, the PHY layer via the PHY SAP passes MAC frames to the MAC sublayer, and also through the MAC SAP the MAC sublayer passes MSDUs to the MAC client. (IEEE Computer Society 2012)

4.1. MAC and Security

The main application of BAN is to support life saving medical application, therefore safety, security and reliability are very important features of BAN as well as its energy efficiency. Since BAN is also a form of short range wireless technology, data could also be transmitted via the air. In a place like hospital ward, or hospital elevators where there could be multiple BAN devices close to each other, there is need for a very robust MAC protocol for the BANs to coexist harmoniously without interference with each other. In case of heavy interference due to presence of multiple BANs devices, there is a need for a quick switch to a more quite channel in this kind of situation, for this reason, an adaptive frequency agility and channel migration protocol need to be developed. There is also a need for a well-developed and efficient duty cycling method in other to minimize the power consumption without having to compromise the QoS. (IEEE Computer Society 2012).

The human body structure/positions is another very important factor to be considered in the design of BAN. The human body changes frequently and this affect the position of the nodes in or around the body. Hence there are always changes in the topology and density. For instance when one is sleeping, standing, sitting down or walking, these are different human body positions. Because of these changes in positions there are also equal changes in the topology and density. Hence the MAC protocol should be able to cope and quickly adjust itself with these changes. Because BAN is mainly optimized for its medical application, unlike in some other short range wireless technologies. Its first priority should be to guarantee delivery of alarming messages in cases of emergency situations for real time vital monitoring. This very important feature should be prioritized in BAN. For instance in the configuration of voice traffic on a Cisco IP telephone, voice command is configured with a 0-priority. This is because the Cisco IP telephone is optimized for voice application. Though other applications are also allowed, but whenever there is voice traffic, the channel makes sure it abandons everything else and allows for any easy, efficient and very fast passage of the voice traffic and this is because of the priority configured for the voice traffics. This kind of protocol also needs to be enabled in all BANs devices, to give priority to guarantee the delivery of alarming messages. (IEEE Computer Society 2012).

4.1.1. Beacon mode with beacon superframe boundaries

In this mode, except if it is prohibited by the regulation or in active case, beacons are transmitted in each beacon period by the hubs. In this mode, the superframe structure of the IEEE802.15.6 is divided into seven phases namely: Exclusive Access Phase 1 (EAP1), Random Access Phase 1 (RAP1), Type I/II Phase, Exclusive Access Phase 2 (EAP2), Random Access Phase 2 (RAP 2), Type I/II Phase, and finally Contention Access Phase (CAP), as shown in the Figure 5. (IEEE Computer Society 2012) (Kyung Sup Kwak et al 2010).

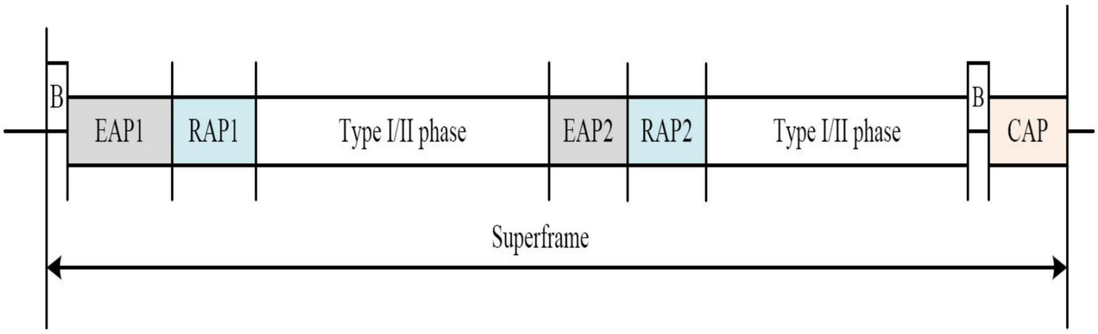

FIGURE 5 Superframe Structure (Kwak, K. S., et al 2010)

The seven phases are logically divided into performing certain functions: The EAP1 &EAP2 reserved for highest priority traffic such as reporting emergency events. The RAP1, RAP2 and CAP, are reserved for regular traffic, while the Type I/11 Phases are allocated for downlink and uplink allocation intervals, bilink allocation intervals and finally delay bilink allocation intervals. Polling is used for allocation of resources in Type I/II phases. Any of the periods could be disabled by setting the duration length to zero. (Kwak, K. S., et al 2010)

4.1.2. Non-Beacon mode with superframe boundaries

The entire superframe duration in this case is covered by either a Type I or a Type II access phase. It has to be one of the two, but it is never both. (IEEE Computer Society 2012).

4.1.3. Non-Beacon Mode without superfraeme boundaries

Only unscheduled Type II polled allocation is provided in this mode. The hub may also support contented access methods, in this mode. (IEEE Computer Society 2012).

4.2. Security

The dependability of a technology depends mostly on how secure the technology is, and this also applies to BAN. But most especially because BAN will be mostly used for medical purposes, security of this technology is of a very high priority. Medical information of a patient is very confidential information shared between only the doctor and the patient and no third party is involved. Bridge to this clause on the side of a medical practitioner could lead to a very big law suit, and it could also leads to the death of a patient if this falls into the wrong hands. Because of the importance of a very strong security for BAN, and the fact that most of the security mode of the already existing short range wireless technology has already been broken, it is therefore of utmost important to have a self-contained, low overhead, but very strong security solution for this technology. Figure 6 shows the generalized security structure of BAN. (Maulin Patel et al 2010) (Kwak, K. S., et al 2010).

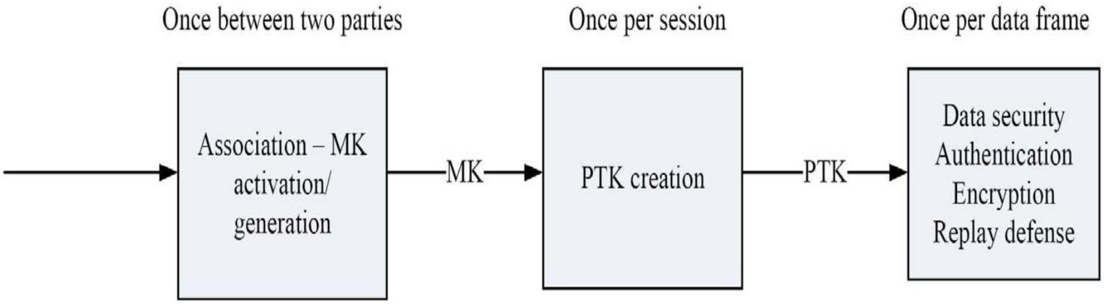

FIGURE 6 Security Structure of BAN (Kwak, K. S., et al. 2010)

In BAN, the security usually starts with the two communicating parties, the hub and the node, negotiating which of the securities best suites them. So when the desired security has been selected, this sets off a security association between the hub and node thereby activating a pre-shared or generating a new shared master key (MK). The security association protocols are discussed below. (IEEE Computer Society 2012).

4.2.1. Master Key Pre-shared association

In this kind of security protocol, before the hub and the node both parties involved in this communication run the MK pre-shared association protocol so as to activate their pre-shared MK for the creation of their Pairwise Temporal Key (PTK). Both the node and hub each have already a secret pre-shared Master key (MK), and this is mainly to keep third parties from the possession of this secret MK. (IEEE Computer Society 2012).

The node sends the first security association frame to the hub. This helps to initiate the security association process to run the MK pre-shared association protocol. Upon receiving the frame, the hub send the second security association frame to the node, indicating whether to join or abort the security association process. If the hub is aborting the security association, when the node receives the second security association frame indicating the aborting of the security association, it then aborts its current security procedure. But depending on the security suite selector the hub used in aborting the association, maybe due to temporary lack of resources, the node may choose to initiate a new security association process. But in the case whereby the hub is accepting to join the security association procedure, the hub thereby will activate the pre-shared MK as its shared MK with the node, completing the security association process while treating the node true identity unauthenticated. The node also on receiving this will activate its own pre-shared MK, the one they both shared, thereby treating the hub's true identity unauthenticated and thereby completing the security association process. Then the node proceeds to create PTK with the hub, and based on the pre-shared MK, they could both thereby perform a mutual authentication of each other. (IEEE Computer Society 2012).

4.2.2. Unauthenticated association

In this kind of security protocol, the two communicating parties the hub and the node requires no authentication credentials before running the unauthenticated association protocol, to generate their shared MK in order to create their PTK. The node initiates the association security protocol, like in the case of Master key pre-shared association. So when the hub receives the first security association frame sent by the node, the hub reply's by sending a second security association frame, indicating whether to accept the invitation to join in the association, or whether not to join the association. So the hub sends to the node a second security association frame. The hub sends a message either accepting to join the security association thereby setting the MK_KMAC field of the security association data to MK_KMAC_2, or to abort the security association, thereby setting the MK_KMAC field to 0. (IEEE Computer Society 2012).

When the node receives the second security association frame from the hub, suggesting that it would not be joining the association, the hub terminate the security association process. But depending on the suite selector the hub used in sending the message would determine if the node will re-initiate another association or not. If the hub aborted the security associate process with a different security suite selector, this indicates that it doesn't have enough resources at the moment, then in this case the node could initiate another security association process. But in the case when the security association procedure was not aborted, after the node has received a second security association frame from the hub with the MK_KMAC field set to MK_KMAC_2. Then the node will send the third security association frame of the procedure to the hub, setting the MK_KMAC field to MK_KMAC_3. When the third security association frame has been sent successfully the node then compute their shared MK treating the hub's true identity as unauthenticated but the association procedure as completed. The hub also does the same to the node after it has received the third security association frame. (IEEE Computer Society 2012).

4.2.3. Public Key Hidden Association

In this kind of security association procedure, both the hub and the node shall have a secret transfer of the node's public key to the hub, typically through an out-of-band channel. Prior to running the public key hidden association protocol to generate their shared MK for their PTK creation, and they do this while trying to keep the third parties from impersonation attack. (IEEE Computer Society 2012).

The node initiates the security association procedure by transmitting the first security association frame of the procedure to the hub, thereby indicating in the frame the selected security suite. The hub on receiving the first security association frame from the node, it replays by transmitting the second security association frame of the procedure. This security frame transmitted by the hub would determine if the hub is accepting the security association or aborting the association. To accept and continue the security association, the hub would set the MK_KMAC field of the security association data to MK_KMAC_2. Therefore when the node receives the second security association frame with the MK_KMAC field set to MK_KMAC_2, it then send the third security association frame of the procedure, setting the MK_KMAC field of the security association to mk_kmac_3. After the third frame has been successfully sent, the node would compute the shared the MK treating the hub's true identity as authenticated and the associated procedure as completed. The hub upon receiving the third frame having MK_KMAC field set to MK_KMAC_3, the hub also does the same as the node. (IEEE Computer Society 2012).

4.2.4. Password Authentication Association

In this kind of security association procedure, both the hub and the node will have a secret shared password. Prior to running the password authenticated association protocol in order to generate their shared MK for the creation of their PTK. While trying to keep the third parties away from processing the secret password so as to prevent impersonation attacks. The node initiates this procedure by first sending the first security association frame of the procedure to the hub, indicating in the frame its selected security suite. (IEEE Computer Society 2012).

The hub upon receiving the first security association frame, sends the second security associated frame indicating whether it will be accepting or aborting the security association. If the hub is aborting the security association due to temporary lack of resources, it sends the second security association frame with a different security suite selector. When the node receives this frame, it aborts the procedure and may re-initiate the security association later. But if the hub sends the second security association frame with the MK_KMAC field set to KM_KMAC_2, the node continues with the security association by sending the third security association frame of the procedure setting the MK_KMAC field of the security association data to MK_KMAC_3. When the third security association frame has been successfully sent, the node then compute the shared MK, treating the hub’s true identity as authenticated and the association procedure as complete. The node also does likewise upon successfully receiving the third security association frame from the node with the MK_KMAC field set to MK_KMAC_3. (IEEE Computer Society 2012).

4.2.5. Display Authentication Association

In this kind of security association procedure, both the hub and the node before running the display authentication association protocol shall each have a 5-digit decimal number. So that they could generate their shared MK for the creation of their PTK, while also trying to prevent attacks from third parties. (IEEE Computer Society 2012).

The node initiates this security association by first sending to the hub the first security association frame of the procedure. The hub upon receiving the frame sent by the node, would respond by sending the second security association frame of the procedure. This frame will indicate if the hub is accepting the security association or aborting the association, the node would indicate this by the selected security suite the hub use in sending the frame. Therefore when the node receives the second security association frame sent by the node, indicating that it is aborting the security association, the node will abort the current security association procedure. Though it may re-initiate another security association procedure. If the hub aborted the procedure with a different security suite selector, which may suggest that, the hob is temporarily out of resources. (IEEE Computer Society 2012).

The node could resume the procedure if it receives another frame from the hub with the MK_KMAC field set to MK_KMAC_3. In this case the node would treat the second security frame that was received earlier as a frame sent by an impersonator or a third party. But in the case whereby the second security frame received by the node the MK_KMAC field was set to MK_KMAC_2, the node in this case will send the third security association frame of the procedure setting the MK_KMAC field to KM_KMAC_3. Upon successfully sending the third security association frame, the node would display it 5-digit decimal number. The hub also upon verifying that the third security association key sent by the node is valid, it then display it’s 5-digit decimal number. If they both display the same 5-digit decimal number, they will both be informed through their respective user interfaces that their mutual authentication has succeeded. But if they both display different 5-digit decimal numbers, they both each would be informed that their mutual authentication has failed. After they both have been informed that their mutual authentication has been successful, they both then compute the shared MK, treating their association procedure as completed. (IEEE Computer Society 2012).

4.3. Security Dissociation

The dissociation procedure could be initiated by either of the two communicating parties, the hub or the node. The procedure nullifies the existing security association between both parties, and also their shared MK and PTK. Either the hub or the node, depending on which is initiating the dissociation procedure send a security dissociation frame setting the DA_KMAC field of the frame payload to *DA_KMAC.* The receiver could either be the hub or the node depending on who is initiating the dissociation procedure. When it receives the security dissociation frame, it erases the MK and the PTK from its internal storage and the sender does likewise after successfully sending the security dissociation frame. (IEEE Computer Society 2012).

5. PHYSICAL (PHY) LAYER SPECIFICATION OF BAN

Body Area Network BAN, supports three different physical layers namely: Narrowband (NB) PHY, Ultra Wideband (UWB) PHY, and Human Body Communication (HBC). (IEEE Computer Society 2012).

5.1. Narrowband (NB) PHY

The Narrowband, NB PHY is responsible for the activation and deactivation of the radio transceiver, clear channel assessment (CCA) within the current channel and finally for data transmission and reception. Figure 7 shows the Physical Protocol Data Unit (PPDU) structure of NB PHY. The PPDU frame of the NB PHY contains a Physical Layer Convergence Procedure (PLCP) preamble, a PLCP header, and a PHY Service Data Unit (PSDU) as shown in Figure 7. (IEEE Computer Society 2012) (Kwak, K. S., et al. 2010)

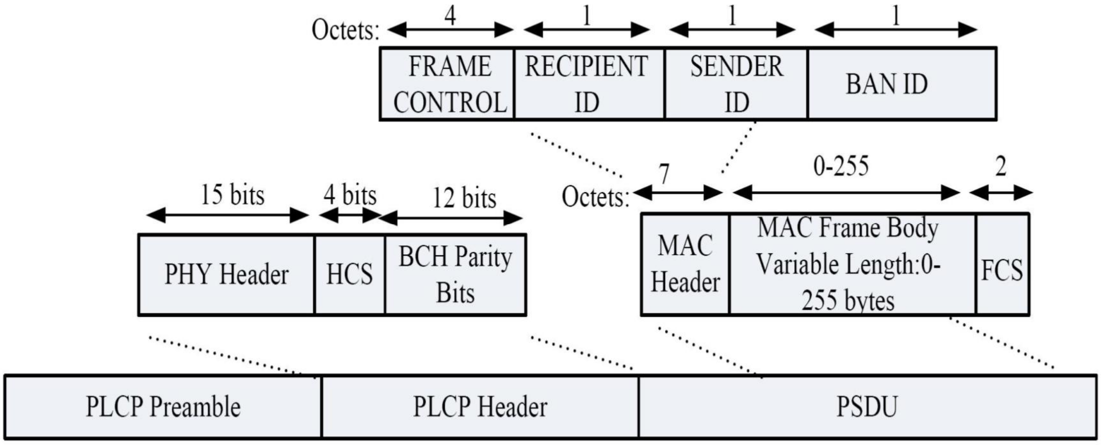

FIGURE 7; Narrowband PPDU Structure (Kwak, K. S., et al. 2010)

The PLCP preamble helps the receiver during timing synchronization and carrier-offset recovery. The PLCP header’s main purpose is to carry the necessary information about the PHY parameters to aid in the decoding of the PSDU at the receiver. The PLCP header could be further broken down into a RATE field, a LENGTH field, a BURST MODE field, a SCRAMBLER SEED field, reserved bits, a header check sequence (HCS), and finally BCH parity bits. The BCH parity bits helps in enhancing the robustness of the PLCP

header. The PLCP header is transmitted after PLCP preamble using the given header data rate in the operating frequency band. The PSDU is the third component of the NB PHY PPDU, it is formed by joining the MAC header together with the MAC frame body and frame check sequence (FCS). The PSDU is transmitted after the PLCP header using any of the available data rates in the operating frequency band. Table 3 shows the summary of frequency band that BAN devices should be able to support for transmission and reception.
(Choi, B., Kim, B., Lee, S., Wang, K., Kim, Y., & Chung, D. 2010).

TABLE 3 Modulation Parameters for PLCP Header and PSDU (Kwak, K. S., et al 2010).

Frequency Band	Packet Component	Modulation	Symbol Rate (Kbps)	Code Rate BCH (n,k)	Information Data Rate (Kbps)
402 – 405 MHz	PLCP Header	π/2-DBPSK	187.5	31.19	57.5
	PSDU	π/2-DBPSK	187.5	63.51	75.9
	PSDU	π/4-DQPSK	187.5	63.51	303.6
420 – 450 MHz	PLCP Header	GMSK	187.5	31,19	57.5
	PSDU	GMSK	187.5	63,51	75.9
	PSDU	GMSK	187.5	63,51	151.8
863 - 870 MHz	PLCP Header	π/2-DBPSK	250	31.19	76.6
	PSDU	π/2-DBPSK	250	63.51	101.2
	PSDU	π/4-DQPSK	250	63.51	404.8
902 - 928 MHz	PLCP Header	π/2-DBPSK	300	31.19	91.9
	PSDU	π/2-DBPSK	300	63.51	121.4
	PSDU	π/2-DBPSK	300	63.51	485.7
950 – 956 MHz	PLCP Header	π/2-DBPSK	250	31.19	76.6

	PSDU	π/2-DBPSK	250	63.51	101.2
	PSDU	π/2-DQPSK	250	63.51	404.8
2360–2400/ 2400–2483.5 MHz	PLCP Header	π/2-DBPSK	600	31.19	91.9
	PSDU	π/2-DBPSK	600	63.51	121.4
	PSDU	π/2-DBPSK	600	63.51	485.7

From Table 3, we could see that NB PHY standard uses Differential Binary Phase-shift Keying (DBPSK), Differential Quadrature Phase-shift Keying (DQPSK), Differential 8-Phase-shift Keying (D8PSK), and finally Gaussian minimum shift Keying (GMSK). All these modulation techniques are employed in this standard

5.1.1. PLCP Preamble

In order to aid the receiver in the packet detection, timing synchronization and carrier-offset recovery, prior to the PLCP header a preamble need to be added. Due to the several networks operating on adjacent channels, there is need to lessen the amount of false alarm. The two uniquely defined preambles helps in this regards. Preambles are formed by joining a length-63m- sequence with a 010101010101101101101101101 extension sequence. The length of the preamble is 90 bits. Both the former sequence and the latter sequence can be used in implementing various functions. The former sequence helps in implementing packet detection, coarse-timing synchronization, and carrier-offset recovery, and the latter sequence helps in implementing fine-timing synchronization. (IEEE Computer Society 2012).

5.1.2. PLCP Header

PLCP Header main purpose is to carry the necessary information about the PHY parameters, to aid in the decoding of the PSDU at the receiver. It is added after the PLCP preamble, and it is 31 bits long. Figure 8 and 9 shows the BCH coding scheme for PLCP header construction and also how the PLCP header is constructed for transmission respectively.

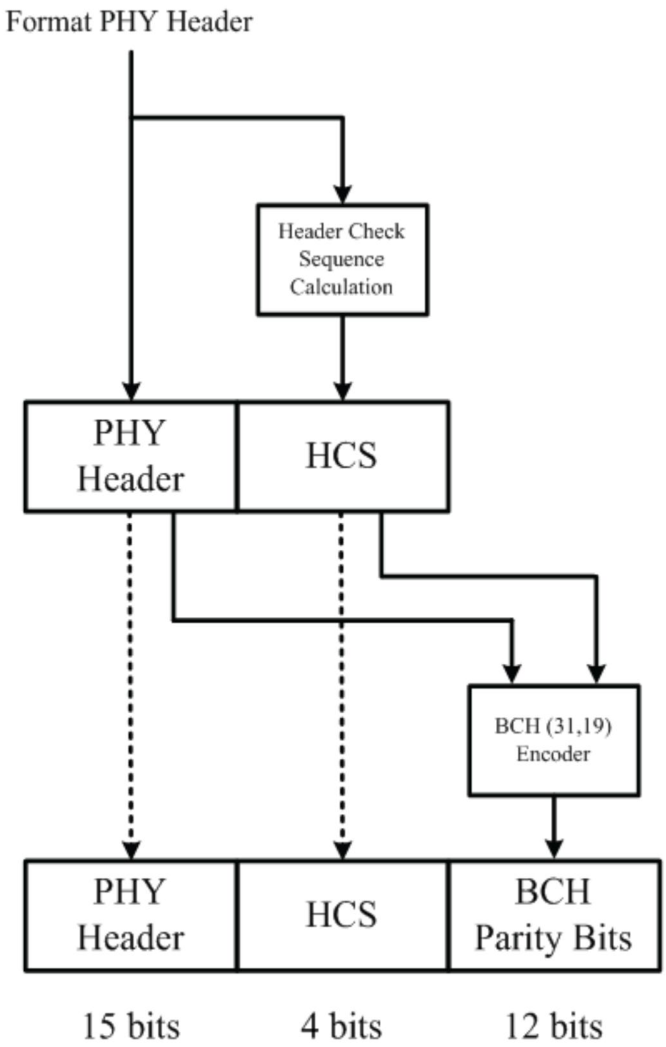

FIGURE 8 BCH Coding Scheme for PLCP Header Construction (Choi, B., et al 2010)

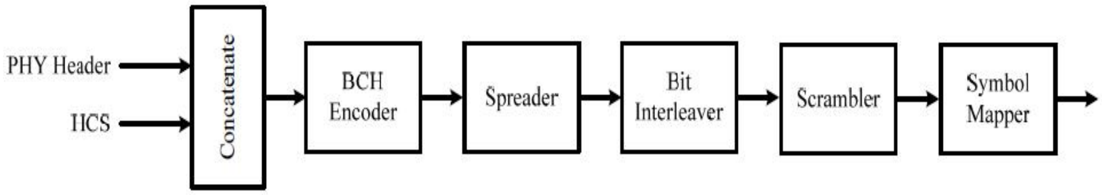

FIGURE 9 PLCP Transmission Block diagram (IEEE Computer Society 2012 P. 178)

5.1.3. PHY Header

The length of the MAC frame body, data rate of the MAC frame body, as well as the information as regards whether the next packet is being sent in a burst mode, are contained in the PHY header. As shown in Figure 8, the PHY header field consists of 15 bits ranging from 0-14. Figure 10 shows how the 15 bits are defined for their particular purposes.

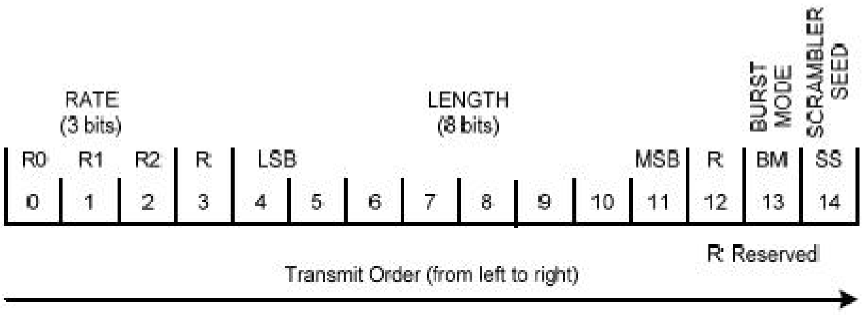

FIGURE 10 PHY Header bit assignment (IEEE Computer Society Std 802.15.6. P. 179)

Figure 10 shows that most of the bits are assigned. The various assignments of the bits are listed below: (IEEE Computer Society 2012).

i. Bit 0-2: They encode the rate field, which carries the information as regards the type of modulation, information as regards the data rate, the pulse shaping, coding rate, as well as the spreading factor used to transmit the PSDU.

ii. Bit 4-11: They encode the LENGTH field, with the LSB being the first to be sent.

iii. Bit 13: It encode regardless of the packet being transmitted in the burst mode or not.

iv. Bit 14: It encodes the scrambler seed.

v. Bit 3, 12: These two bits are unassigned and therefore are set to zero. But because BAN is a new technology which standardization is still in progress, it very reasonable to assume that these bits are reserve for future use.

5.1.4. HCS and BCH

The Header check sequence main function is to protect the PHY header, while the BCH helps to enhance it robustness. The BCH does this with the help of the BCH encoder. (IEEE Computer Society 2012).

5.1.5. PSDU

PSDU is another major component of the PPDU, which has already been described above. Figure 11 shows how PSDU comes about transmission. (IEEE Computer Society 2012).

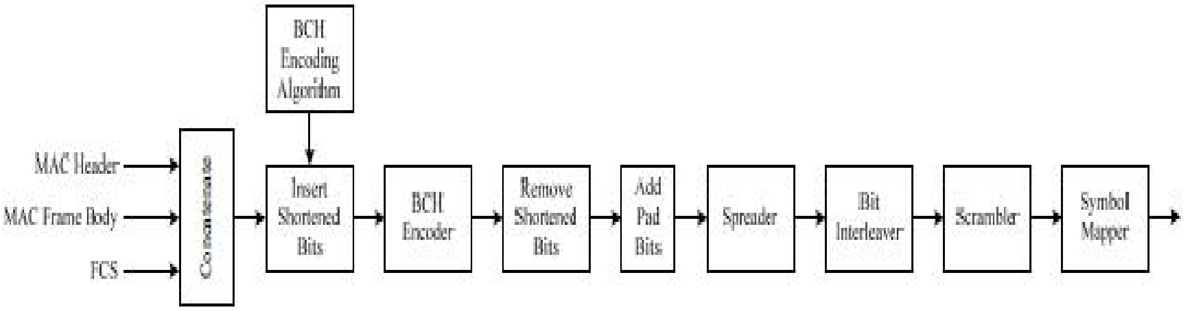

FIGURE 11 Block diagram of PSDU construction for transmission (IEEE Computer Society 2012 P. 181)

5.2. Ultra Wide-band (UWB) PHY

Ultra wide-band, UWB PHY offers robust communication and precise self-location of sensor nodes for BAN technology. It also provides a very good platform for implementation opportunities for high performance, and ultra low power operation. With the help of the physical layer convergence protocol (PLCP), UWB provides the MAC layer with a data interface. Namely below are the three layers of functionalities provided by the UWB PHY: (IEEE Computer Society 2012) (Lee, C., Kim Jaehwan., Lee, H. S., & Kim Jaeyoung. 2009.)

i. Activation and deactivation of the radio transceivers.

ii. With the help of the PLCP, and by connecting the Synchronization header (SHR), the Physical layer header (PHR) and the Physical layer service data unit (PSDU) together respectively. The PHY layer protocol data unit (PPDU) is well constructed, and also for the sake of wireless medium transmission, the PPDU bits are converted into RF signals.

iii. As mentioned above, the UWB PHY offers the precise location of the sensor node for BAN. It does this with the help of a Clear Channel Assessment (CCA).

5.2.1. UWB PHY Channels

UWB PHY has two modes of operation namely: The Default mode otherwise called the Low band and secondly the High band QoS mode also called the high band mode. The UWB PHY consists of 11 channels, the first three channels (Channel 1 – 3) are meant for operations in the low band mode, while the last eight channels (Channel 4 – 11) are reserved for high QoS mode operation. There are two channels regarded as mandatory channels: Channel 2 and Channel 7, both of which have a bandwidth of 499.2MHz like the rest of the channels, but their central frequencies are 3993.6MHz and 7987.2MHz respectively. It is mandatory for a UWB device to support at least one of the two mandatory channels, as shown in Table 4. Its low interference to other devices and because the signal power levels are in the order of those used in the Medical Implant Communications Services (MICS) band. It helps to provide a safe power level for the human body. Beacuse this technology is mostly focused on its medical applications. (Kwak, K. S., et al 2010).

TABLE 4. Showing UWB PHY operating frequency band. (Davenport, D. P. 21)

Band group	Channel number	Central frequency (MHz)	Bandwidth (MHz)	Channel attribute
Low band	1	3494.4	499.2	Optional
	2	3993.6	499.2	Mandatory
	3	4492.8	499.2	Optional
High band	4	6489.6	499.2	Optional
	5	6988.8	499.2	Optional
	6	7488.0	499.2	Optional
	7	7987.2	499.2	Mandatory
	8	8486.4	499.2	Optional
	9	8985.6	499.2	Optional
	10	9484.8	499.2	Optional
	11	9984.0	499.2	Optional

5.2.2. UWB PHY Frame Format

As already mentioned earlier, the UWB PHY frame format otherwise known as the Physical Layer Protocol Data Unit (PPDU) is constructed by the PLCP by connecting together the SHR, PLDU and the PSDU. This is illustrated in Figure 12. (Kwak, K. S., et al 2010)

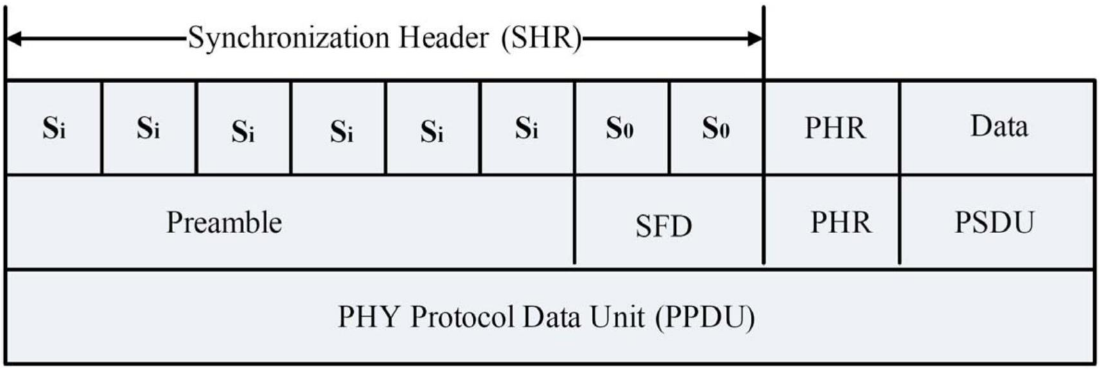

FIGURE 12 UWB PHY Frame Format (Kwak, K. S., et al 2010)

5.3. Human Body Communication (HBC)

The HBC PHY covers the entire protocol for BAN which includes: packet structure, modulation, preamble/SFD, etc. It uses the Electrostatics Field Communication (EFC). HBC operates in two frequency band 16MHz and 27MHz. The 27MHz operating frequency is accepted in Europe, while in the USA, Japan, Korea and most other part of the world both operating frequencies are accepted. The HBC PHY PPDC structure is made up of the Preambles, the start frame delimiter (SFD), the PHY header, and the PSDU. These are shown in the Figure 13. (Kwak, K. S., et al 2010).

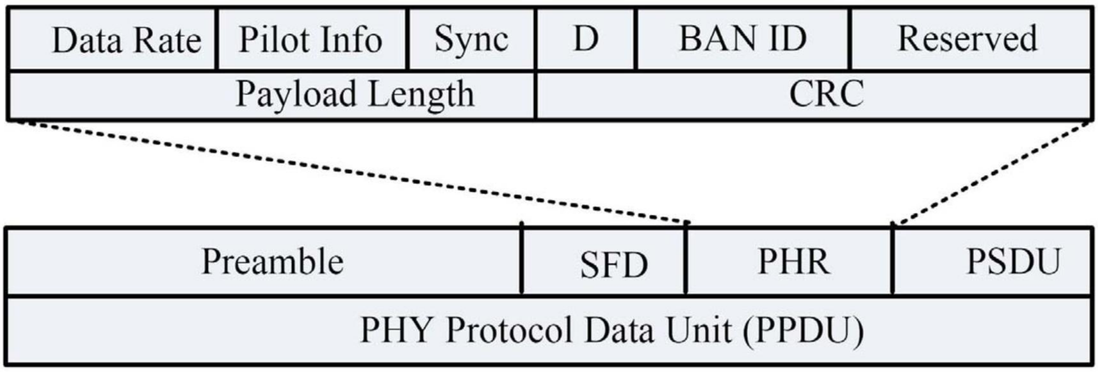

FIGURE 13 HBC PPDU Structure (Kwak, K. S. et al 2010).

Human body communication (HBC) can be categorized into two categories, depending on whether it is operated from inside or outside of the human body: Wearable BAN and Implant BAN. (Ryuji K., et al 2008).

5.3.1. Wearable BAN

Wearable BAN can be used for both Medical and non-medical applications. It could operate in close vicinity of the human body, as well as when it is attached to the human body. Figure 14 shows an example of a wearable BAN. Using an Ambu Neuroline 700 single patient surface electrode, the electrodes are connected from the signal generator to the human body, then from the human body to the signal analyzer. In this scenario, the signals generated from the signal generator, flows through the human body and it is been transmitted to the signal analyzer. In this case the human body serves as a wired medium for signal transmission. (Ryuji K. et al 2008).

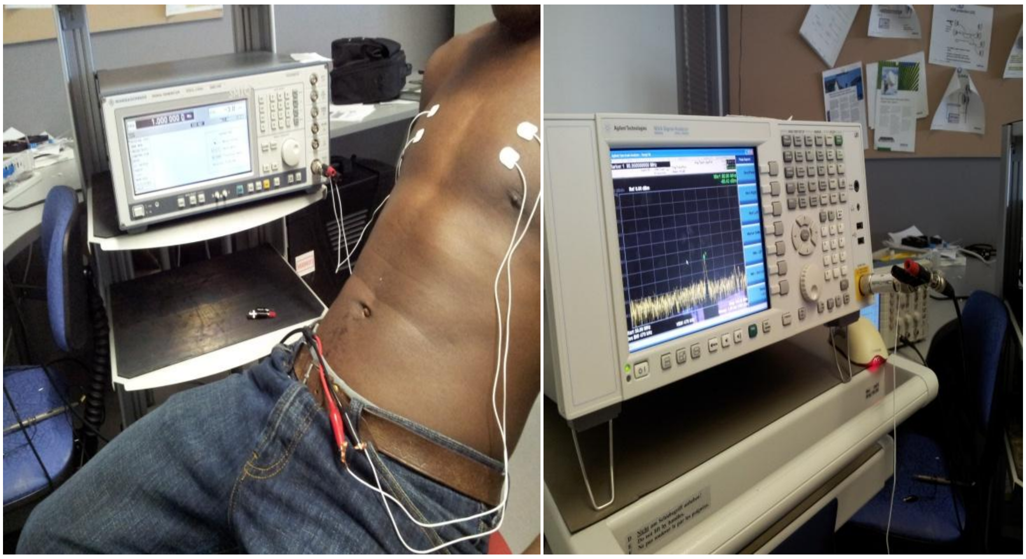

FIGURE 14 Wearable BAN (Ekundayo 2012)

This process is best suited for medical purposes, because of the wired medium, there would be less concern for interference. Because the patient would be continually connected to the devices, real time vital signals of the patient will be sent to the doctor or nurses via a wireless medium through the signal analyzer. This method is very reliable.

It is also possible to send the signals from the human body wirelessly. While the human body is connected to the signal generator, an antenna is connected to the signal analyzer. The human body transmit the signal wirelessly and the antenna receives the signal. This method is more reliable when there is only one device transmitting in the close proximity of the patient, else the antenna would be receiving more signals which are not related to the patient and this could be disastrous for the patient.

5.3.2. Implant BAN

Implant BAN is mainly considered for only medical purposes. They are in compliance with the MICS band standard. It is very reasonable to suggest that Implant band should be supported by separate PHY. While Wearable BAN operate in close proximity of the human body, with the possibility of causing little or no harm to the human body. In the case of a malfunction in the technically properties of the device, and besides they can be easily disconnected if the need arises. Implant BAN on the other hand could be much more harmful is this regards, because they are already inserted in the human body, they can't be easily removed, hence they should be subjected to much more restriction. (Ryuji, K., et al 2008).

Another very important factor to consider in Implant BAN is the SAR, though it is very important for both, Implant BAN need to be much more restricted in this area. Implant BAN is not another form of MicroChip or VeriChip Implantation, though both might have some similarities base on the fact that they are restricted to the MICS Band. But unlike implanted microchip, implant BAN is only concern with the health issues of a patient. It sends vital signals from the inside of the patient in form of electrical signal, which are being recorded on the signal analyzer and the result are sent to the doctor or nurse, and it alarms in case of a medical emergency. It provides a real time update on a patient. (Ryuji K., et al 2008) (Moshaddique, A. A., Liu, j., Ullah, S., Kwak, K. S.. 2011).

6. RESEARCH ON SIGNAL TRANSFER

The aim of this test was to see how the position and the state of the human body affect the output signal that is being recorded in the signal analyzer. Using the Ambu Neuroline 700 single patient surface electrode as shown in the Figure 14, two pairs of electrodes were connected to 2 parts of the human body, with one of the pairs connected to the signal generator and the other pair to the signal analyser. The electrical signal generated from the signal generator passes through the electrode connected to it, then through the human body and it comes out from the electrode at the other end, then into the signal analyzer. This is a simple test on how the human body could serve as a medium for transfer of electrical signals. Figure 15 and16 show the diagram of the signal generator and the signal analyzer.

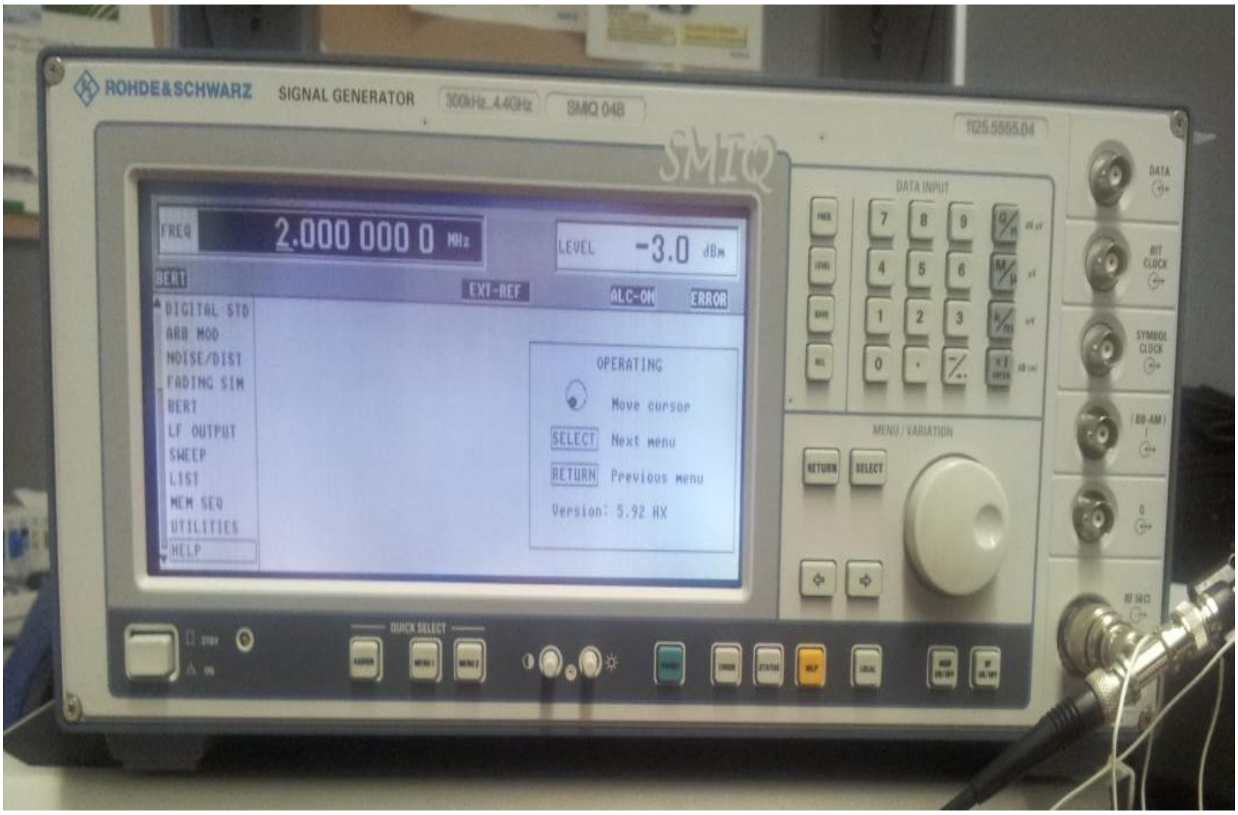

FIGURE 15 Rohde & Schwarz Signal Generator (Ekundayo 2012)

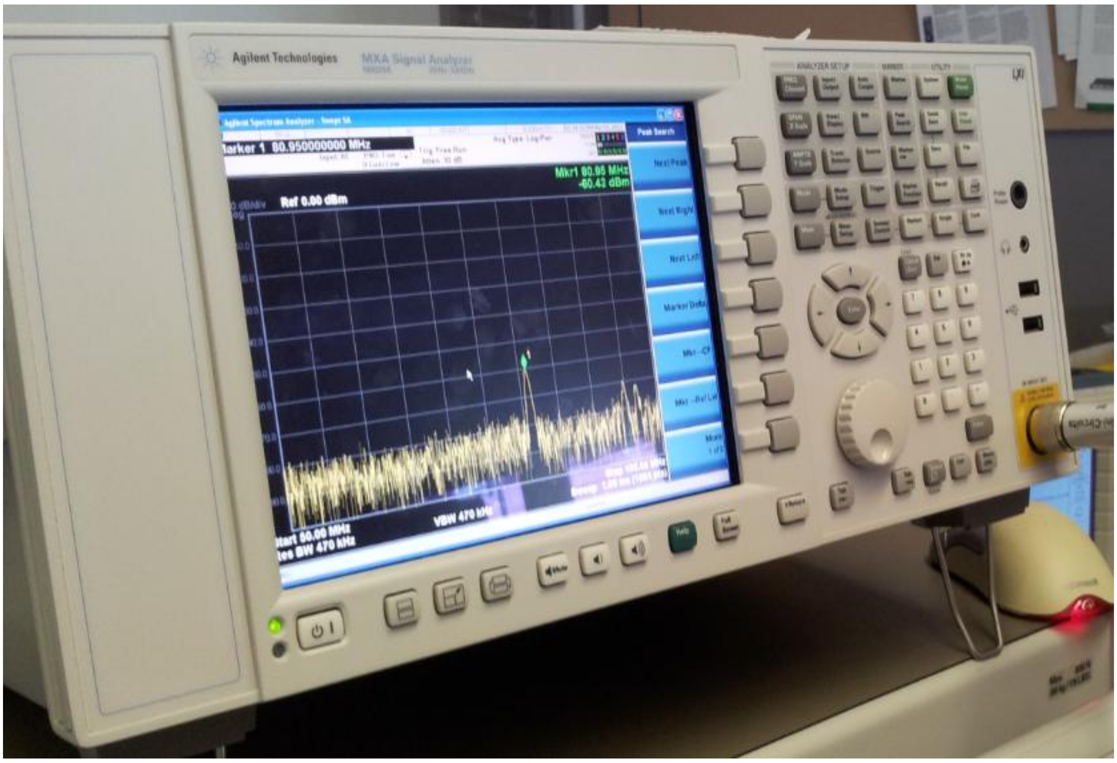

FIGURE 16 Agilent Technologies MXA Signal Analyzer (Ekundayo 2012)

Becuase this technology would be applied on patients in hospital, it is very important to know how the different parts of the human body could affect the flow of the electrical signals being sent from the signal generator. It is very most important to know how the state of the person would affect the output signal. Because this is what will really help the doctors and nurses to know what exactly is wrong with the patient, when the patient needs medical emergency and so on. Figures 17 to 20 shows the output signals in minus decibel (-db) values, and the input signal in Mega Hertz (MHz).

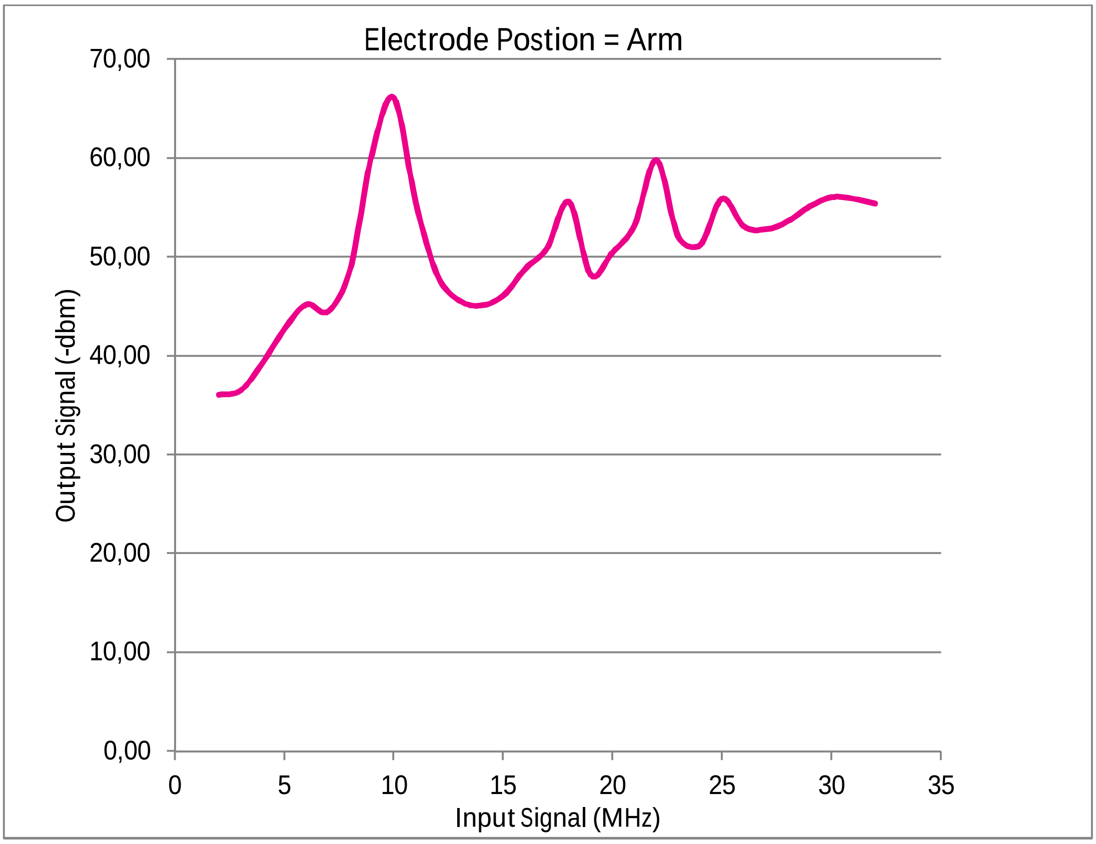

FIGURE 17 Output Signal when connected to the arm (Ekundayo 2012)

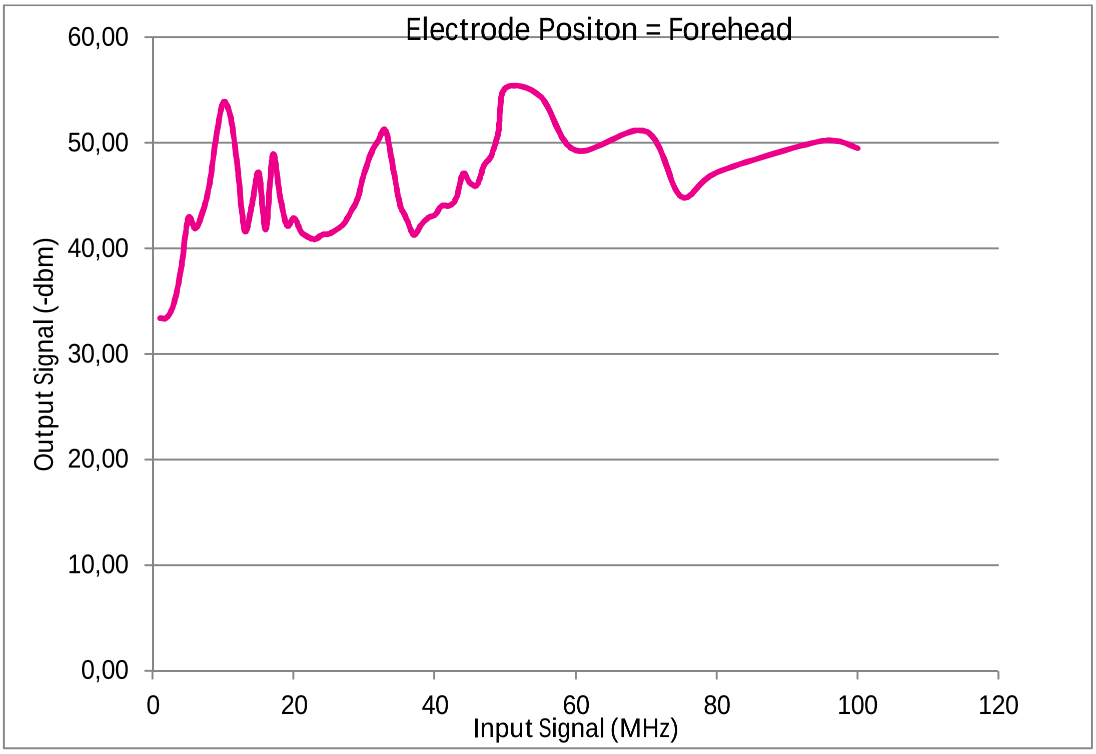

FIGURE 18 Output Signal when connected to the forehead (Ekundayo 2012)

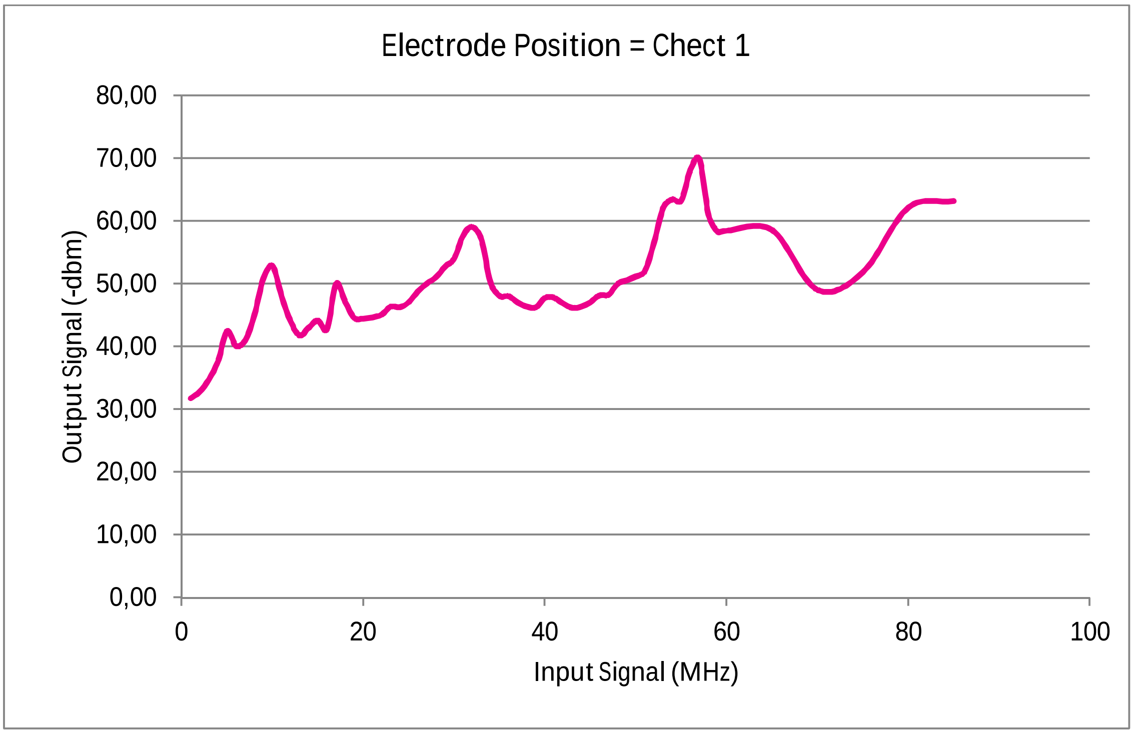

FIGURE 19 Output Signal when connected to the chest (Ekundayo 2012)

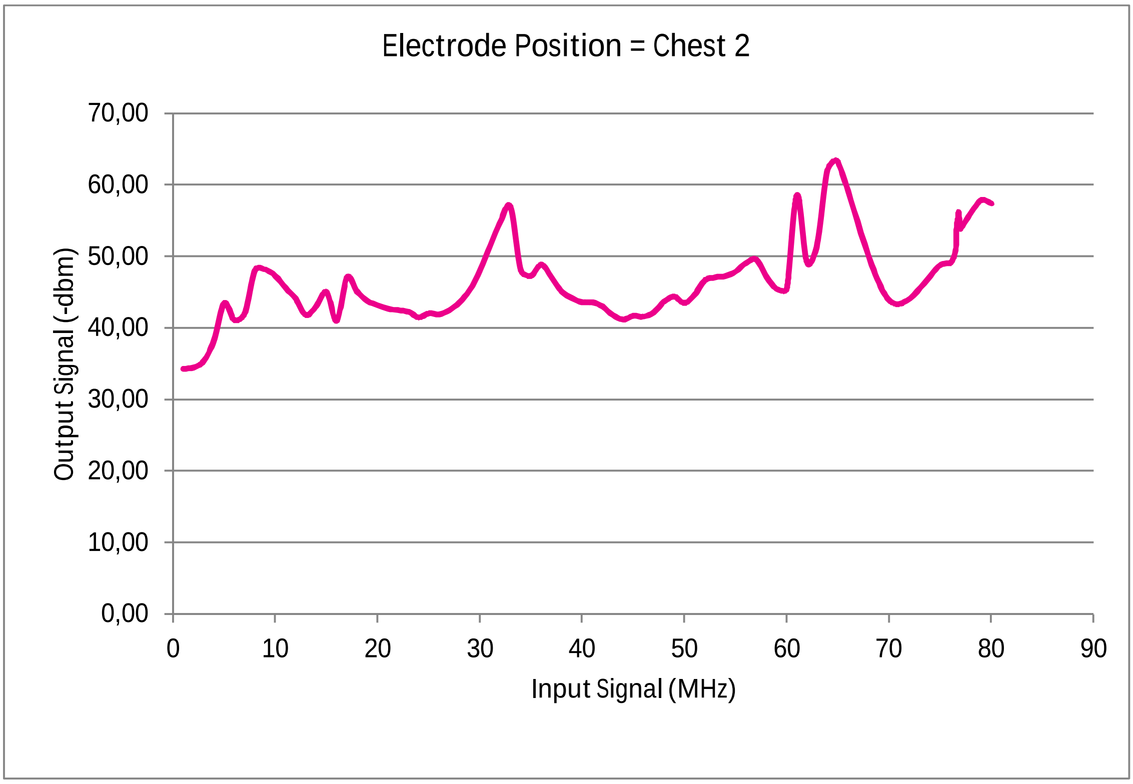

FIGURE 20 Output Signal when connected to the chest (Ekundayo 2012)

Figures 17 to 20 show that the SAR at different point in the human body varies, reason for this could be explain with further research into this technology. But we could see clearly that with increase in the input signal the human body react accordingly to this changes. The results shows a sinuosidal pattern, with a change in the input signal there is a corresponding change in the signal coming out from the body. But one very important point to consider in when comparing both graps when the electrodes was placed on the chest Figure 19 and 20.

This was a very interesting part of the testing process, several readings were taking on the same a person, while the person is sitting, standing or lying down very relaxed. After a while another set of readings where taken on the same person, but this time after I told the person that I will be sending some very high electric current into his body, and that he should try to remain still. But because news like that will normally create some fear or anxiety in the person, and despite the fact that the person is still trying to look relaxed as he was earlier. But inside he is not, I knew this because of the output signal I was getting from the signal analyzer. There was a very large difference in the output signal, when you compare the result to when the person was truely relaxed, without any fear or anxiety and when the person isn't or even pretending to be relaxed.

This could be easily applied on a sick patient in the hospital, the sensor attached to the body of the patient would be sending to the doctor or the nurse signals as regards his temperature, blood pressure, and some other physiological and important data needed for the patient to stay alive. When there is any abnormallty in the data being sent, this could trigger an alarm thereby calling for urgent medical attention. Patient could easily tell lies to the doctors or nurses and they do this all the time, but they can't tell lies to a sensor connected to them or working in close vicinity of them.

7. CONCLUSION

BAN will save a lot of lives, it will save time for the doctors and nurses, it will provide real time patient information to the office or home of the doctors and nurses and it will also help the hospital to run more smoothly.

With the world population growing massively every day, and different epidemics outburst every day, hence there are a lot of sick people in the hospitals today with not enough doctors and nurses to attend to all at the same time. But there is always someone in urgent need of medical treatment compared to the other patients, and with this technology it is easy to know who it is, thereby helping to save the life that was more in danger. It is a very secured technology, and it would not allow any third person interference.

Though ZigBee has been used for some medical applications, BAN is more equipped for this purpose, compares to any other short range wireless technology. It was designed with this in mind. As it was explained in this thesis in section 3, BAN consumes very low power. Section 4 showed how robust this technology is, and it is a much more secured technology, which makes it a much better technology compared to the already existing ones. This thesis also explained how the human body reacts to electrical signals. As well as how a person’s state of being could affect the output signal, coming out of a person’s body to the signal analyser.

This technology has a future in the medical world, though it might take some time before it breaks into the market, but when it does, it will continue to spread. There are not any companies actively producing devices operating on this technology yet, because its standardization is still in progress. Further research on the behaviour of the electrical signals sent into the human body, and some of it physical properties, is worth studying more. This technology will be part of the future of the world healthcare system.

References

Anuj, B., & Ariton, X. 2011. *An Overview of IEEE 802.15.6.* [Electronic file]. Systems and Applications R&D Center Texas Instruments, Dallas. BWRC Wireless Sensor Workshop. [accessed on 03.02.2012]. Available from: http://cutler.eecs.berkeley.edu/php/pubs/pubs.php/1749/overview%20of%20tg6%20-%20final%20-%20batra.pdf.

Choi, B., Kim, B., Lee, S., Wang, K., Kim, Y., & Chung, D. 2010. *Narrowband Physical Layer design for WBAN system*. [Electronic file]. School of Information and Communication Engineering, INHA University Incheon Korea. [accessed on 13.08.2012]. Available from: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5635680.

Choi, J., Kang, H., & Choi, Y. 2008*. A Study on the Wireless Body Area Network Applications and Channel Models.* [Electronic file]. Dept. of Information Technology Eng., Graduate School, Mokwon University. [accessed on 03.09.2012]. Available from: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4734219.

Davenport, D., Hernandez, M., Lewis, D., Huan-Bang, L., McPartland, R., Omeni, O. C., Jin-Meng H., & Astrin, A. 2011*. IEEE 802.15.6 Tutorial.* [Electronic file]. IEEE Computer Society. [accessed on 04.10.2012]. Available from: https://mentor.ieee.org/802.15/documents?is_group=0006.

IEEE Std 802.15.6. 2012. *IEEE Standard for Local and metropolitan area networks Part 15.6: Wireless Body Area Networks.* [Electronic file]. IEEE Computer Society. [accessed on 11.09.2012]. Available from: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6161600.

Kwak K. S.,, Ullah, S., & Ullah, N. 2010. *An Overview of IEEE 802.15.6 Standard*. [Electronic file]. UWB-ITRC Center, Inha University, Incheon, South Korea. [accessed on 1.09.2012]. Available from: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5702867.

Lee, C., Kim Jaehwan., Lee, H. S., & Kim Jaeyoung. 2009*. Physical Layer Designs for WBAN Systems in IEEE 802.15.6 Proposals.* [Electronic file]. IT Convergence Technology Research Laboratory Electronics and Telecommunications Research Institute, Korea. [accessed on 13.11.2012]. Available from: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5341123.

Li, H., Takizawa, K., & Ryuji, K. 2008. *Trends and Standardization of Body Area Network (BAN) for Medical Healthcare*. [Electronic file]. Yokohama National University. [accessed on 27.09.2012]. Available from: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4753792.

Matheus, K., Zurbes, S., Taori, R., & Magnusson, S. 2003. *Fundamental Properties of Ad-Hoc Networks Like Bluetooth: A Radio Network Perspective.* [Electronic file]. Ericsson Eurolab Germany, Ericsson Eurolab Netherlands, Ericsson Radio Systems Stockholm Sweden. [accessed on 03.09.2012]. Available from: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1286184.

Maulin, P., & Jianfeng, W. 2010. *APPLICATIONS, CHALLENGES, AND PROSPECTIVE IN EMERGING BODY AREA NETWORKING TECHNOLOGIES.* [Electronic file]. Philips Research North America. [accessed on 03.08.2012]. Available from: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5416354.

Monto´ n, E., Hernandez, J. F., Blasco, J. M., Herve´, T., Micallef, J., Grech, I., Brincat, A. & Traver, V. 2008. *Body area network for wireless patient monitoring.* [Electronic file]. IET Communication. [accessed on 18.10.2012].

Available from: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4479515.

Moshaddique, A. A., Liu, j., Ullah, S., Kwak, K. S.. 2011. *A Power Efficient MAC Protocol for Implant Device Communication in Wireless Body Area Networks.* [Electronic file]. Graduate School of IT and telecommunications, Inha University, South Korea. [accessed on 10.10.2012]. Available from: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5766358.

Otto, C., Milenkovic A., Sanders C., & Jovanov, E. 2006. *SYSTEM ARCHITECTURE OF A WIRELESS BODY AREA SENSOR NETWORK FOR UBIQUITOUS HEALTH MONITORING.* [Electronic file]. University of Alabama in Huntsville. Journal of Mobile Multimedia, Vol. 1, No.4 (2006). [accessed on 03.09.2012]. Available from: http://www.eng.uah.edu/~jovanov/papers/coamej_jmm06.pdf.

Porras, J., Hiirsalmi, P., Valtaoja, A. 2004. *Peer-to-peer Communication Approach for a Mobile Environment.* [Electronic file]. Lappeenranta University of Technology. [accessed on 11.09.2012]. Available from: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1265717.

Ryuji, K., Kiyoshi, H., Li, H., & Kenichi, T. 2008. *R&D and Standardization of Body Area Network (BAN) for Medical Healthcare.* [Electronic file]. University of Oulu, Finland. [accessed on 11.10.2012]. Available from: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4653402.

Schmitt, L., Falck, T., Wartena, F., & Simons, D. 2007. *Novel ISO/IEEE 11073 Standards for Personal Telehealth Systems Interoperability.* [Electronic file]. Philips Research Europe. [accessed on 11.09.2012]. Available from: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4438177.

Song, S., Cho, N., & Yoo, H. 2007. *A 0.2-mW 2-Mb/s Digital Transceiver Based on Wideband Signaling for Human Body Communications.* [Electronic file]. Department of Electrical Engineering and Computer Science, Korea Advanced Institute of Science and Technology, Daejeon Korea. [accessed on 18.10.2012]. Available from: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4295207

Song, S., Lee S. J., Cho N., & Yoo, H. 2006. *Low Power Wearable Audio Player Using Human Body Communications.* [Electronic file]. Dept. of EECS, Korea Advanced Institute of Science and Technology (KAIST). [accessed on 19.09.2012]. Available from: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4067741

Tjensvold J. M. 2007*. Comparison of the IEEE 802.11, 802.15.1,802.15.4 and 802.15.6 wireless standards*. [Electronic file]. University of Stavanger Norway. [accessed on 03.10.2012]. Available from: http://janmagnet.files.wordpress.com/2008/07/comparison-ieee-802-standards.pdf.

Wikipedia Foundation, Inc (2012). *IEEE802 Working Group.* [accessed 20.9.2012]. Available from: http://en.wikipedia.org/wiki/IEEE_802.