ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 5, May 2013

A Review on IEEE 802.15.4- Standard for Wireless Body Network

S. A. Desai[1], P. H. Zope[2], S. R. Suralkar[3]

Assistant Professor, Department of Electronics and Telecommunication, S.S.B.T. College of Engg & Tech Jalgaon, India[1]

Assistant Professor, Department of Electronics and Telecommunication, S.S.B.T. College of Engg & Tech Jalgaon, India[2]

Assistant Professor, Department of Electronics and Telecommunication, S.S.B.T. College of Engg & Tech Jalgaon, India[3]

Abstract: This paper presents a study on IEEE 802.15.4 and its application in Wireless Body Area Network. A WBAN is one of the rapid advancements of wireless communications which is designed to operate autonomously that connects various sensor nodes within a wireless network. The sensors may be located inside or outside the human body. The IEEE 802.15.4 is fully categorized by FFD(full function devices) and RFD(reduced function devices). The FFD have an ability to connect itself to the existing wireless personal area network or establishes its own. An IEEE 802.15.4 cluster tree format is shown for its reference which totally depends on network co-ordinator. The co-ordinator periodically broadcast broadcasts beacon frames which are used to inform neighbor devices about its existence or synchronize itself with other members of same network. An IEEE 802.15.4 MAC layer is adopted globally. For this a MAC overview, its protocol architecture, topologies is described. A physical layer comparison is given. Finally, a functional overview of a superframe structure is described that uses beacon frame. The co-ordinator uses this structure to transmit the data. Its duration in terms of CAP(contention access period),CFP(contention free period) and beacon interval is provided. This paper discusses the wireless network with various standards and configurations which is developed by Institute of Electrical and Electronics Engineering (IEEE). These standards explain the need and use of wireless connectivity speed ranging from 11Mbps to 54 Mbps. Lastly, we give a functional overview about the Superframe structure, its duration, beacon interval. One of the practical applications of IEEE 802.15.4 in health monitoring has been reviewed. The paper's focus is WLAN & its Applications for various implementations.

Keywords : WLAN, wireless standards, topologies, AlarmNet architecture, Superframe structure.

I. INTRODUCTION

In recent years, interests in the application of wireless body network (WBN) have grown considerably. Among the well-known specifications, IEEE 802.15.4 originally designed for low-power, low-rate, and short-distance wireless personal area networks (WPANs) has become one of the promising candidates for interconnections between wireless sensor nodes. IEEE 802.15.4 uses a modified carrier-sense multiple access with collision avoidance (CSMA/CA) MAC protocol to access channel for transmission data; however, it suffers from inefficient channel utilization because the physical carrier sensing is only performed after the backoff period[1].

In WBNs, sensor nodes are equipped in the human body with small transmission region so that they do not have hidden node situation. Some information has real-time properties and then must transmit periodically. Sensor nodes have different transmission time periods according to priorities. Furthermore, reserved time allocations do not satisfy all requests of sensor nodes because the numbers of used request of sensor node are limited.

A basic wireless sensor network (WSN) consists of one sink and a number of sensor nodes, which are equipped with wireless transceiver and sensor(s). It provides specific services such as ecological detection, health monitoring, digital home, and so on[1]. Among existent wireless standards, the IEEE 802.15.4 low-rate wireless personal area network (WPAN) fulfills the requirements of WSNs. Recently, a wireless body network (WBN) has become a realistic application in WSN. Sensor nodes are equipped in the human body to receive personal information such as pacemakers, neuro stimulators, and retinal prostheses. WBNs consist of a large number of these sensor nodes that are scattered densely in the human body to collect information. Hence, WBN offers many promising new applications in the area of remote health monitoring.

II. WIRELESS LOCAL AREA NETWORKS

The WLAN market is exploding, with reported yearly growth figures of 300% [2]. WLAN systems are a technology that can provide very high data rate applications and individual links (e.g., in company campus areas, conference centers, airports and in libraries) and represents an attractive way of setting up computers networks in environments where cable installation is expensive or not feasible. LANs and mobile computing, have recalling the attention of equipment manufactures. This shows their high potential and justifies the big attention paid to WLAN by equipment manufacturers. Whereas in the early beginning

of WLANs several proprietary products existed, nowadays they are mostly conforming to the Institute of Electrical and Electronics Engineering (IEEE) 802.11b (also known as Wi-Fi) standard [2]. It operates in the unlicensed 2.4-GHz band at 11 Mbps and it is currently extended to reach 54 Mbps [3]. A description of the MAC can be found in [6].

A) WLAN STANDARDS[2]

i) 802.11a

A physical layer standard in the 5 GHz radio band. It specifies eight available radio channels (in some countries, 12 channels are permitted). The maximum link rate is 54 Mbps per channel; maximum actual user data throughput is approximately half of that, and the throughput is shared by all users of the same radio channel. The data rate decreases as the distance between the user and the radio access point increases.

ii) 802.11b

This is a physical layer standard in the 2.4 GHz radio band. It specifies three available radio channels. Maximum link rate is 11 Mbps per channel, but maximum user throughput will be approximately half of this because the throughput is shared by all users of the same radio channel. The data rate decreases as the distance between the user and the radio access point increases.

iii) 802.11d

This standard is supplementary to the Media Access Control (MAC) layer in 802.11 to promote worldwide use of 802.11 WLANs. It will allow access points to communicate information on the permissible radio channels with acceptable power levels for user devices. The 802.11 standards cannot legally operate in some countries; the purpose of 11d is to add features and restrictions to allow WLANs to operate within the rules of these countries.

iv) 802.11e

This standard is supplementary to the MAC layer to provide QOS support for LAN applications. It will apply to 802.11 physical standards a, b, and g. The purpose is to provide classes of service with managed levels of QOS for data, voice, and video applications.

v) 802.11f

This is a “recommended practice” document that aims to achieve radio access point interoperability within a multivendor WLAN network. The standard defines the registration of access points within a network and the interchange of information between access points when a user is handed over from one access point to another.

vi) 802.11g

This is a physical layer standard for WLANs in the 2.4 GHz and 5 GHz radio band. It specifies three available radio channels. The maximum link rate is 54 Mbps per channel whereas 11b has 11 Mbps. The 802.11g standard uses orthogonal frequency-division multiplexing (OFDM) modulation but, for backward compatibility with 11b, it also supports complementary code-keying (CCK) modulation and, as an option for faster link rates, allows packet binary convolution coding (PBCC) modulation.

vii) 802.11h

This standard is supplementary to the MAC layer to comply with European regulations for 5 GHz WLANs. European radio regulations for the 5 GHz band require products to have transmission power control (TPC) and dynamic frequency selection (DFS). TPC limits the transmitted power to the minimum needed to reach the farthest user. DFS selects the radio channel at the access point to minimize interference with other systems, particularly radar.

viii) 802.11i

It will apply to 802.11 physical standards a, b, and g. It provides an alternative to Wired Equivalent Privacy (WEP) with new encryption methods and authentication procedures. IEEE 802.1X forms a key part of 802.11i

B) WIRELESS NETWORK CONFIGURATIONS

There are two kinds of wireless networks:
i) An ad-hoc or peer-to-peer wireless network consists of a number of computers each equipped with a wireless networking interface card. Each computer can communicate directly with all of the other wireless enabled computers. They can share files and printers this way, but may not be able to access wired LAN resources, unless one of the computers acts as a bridge to the wired LAN using special software. This is called "bridging". Each computer with a wireless interface can communicate directly with all of the others.
ii) A wireless network can also use an access point, or base station. In this type of network the access point acts like a hub, providing connectivity for the wireless computers. It can connect (or "bridge") the wireless LAN to a wired LAN, allowing wireless computer access to LAN resources, such as file servers or existing Internet Connectivity[3].

III.APPLICATIONS

A) AlarmNet Architecture[4]

One of the applications of IEEE 802.15.4 is in health monitoring as described below**.** A key requirement for healthcare systems is the ability to operate continuously over long time periods and still integrate new technologies as they become available. AlarmNet satisfies these objectives by unifying and accommodating heterogeneous devices in a common architecture (see Figure 1 and 2) that spans wearable body networks, emplaced wireless sensors, user interfaces, and back-end processing elements.

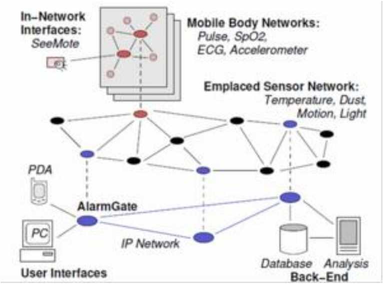

Fig. 1 Multi-tier AlarmNet architecture with emplaced sensors, mobile body area networks, a backbone of gateways, user interfaces, and back-end storage and processing[4].

Mobile Body Networks are wireless sensor devices worn by a resident which provide activity classification or physiological sensing, such as an ECG, pulse oximeter, or accelerometers. The network is tailored to the patient's own medical needs, and can provide notifications (for example, alerts to take medicine) using an in-network wearable interface, the SeeMote that has a color LCD.It also integrates SATIRE, a body network that classifies Activities of Daily Living (ADLs) by analyzing accelerometer data generated by a wearer's movements.Body networks contain a designated gateway device that mediates interaction with the surrounding WSN. This modularizes the system's interaction with the body network to ease its integration. Data are streamed directly or multi-hop through the emplaced network to the AlarmGate gateways for storage, analysis, or distribution to user interfaces.

Emplaced Sensors are deployed in living spaces to sense environmental quality, such as temperature, dust, and light, or resident activities. Motion and tripwire sensors, in particular, provide a spatial context for activities and enable location tracking. Due to their low-cost, small form factor, and limited power budget, the devices answer queries for local data and perform limited processing and caching. Though some deployment environments may enable the use of wired electrical power, it is not required so as to support ad hoc retro-fitting of existing structures. AlarmNet supports dynamically adding new devices to the network, which register their capabilities and are initialized. This flexibility allows the system to change over time as sensors are developed or new pathologies require monitoring.

AlarmGate applications run on an embedded platform, such as the Crossbow stargate, and serve as a communication backbone and application-level gateway between the wireless sensor and IP networks. Owing to their greater resources, these devices perform major aspects system operation related to dynamic privacy, power management, query management, and security. The AlarmGate software stack is shown in .

Back-end programs perform online analysis of sensor data, feeding back behavior profiles to aid context-aware power management and privacy. A database provides long-term storage of system configuration, user information, privacy policies, and audit records.

One such program, for Circadian Activity Rhythm (CAR) analysis, processes sensor data stored in the database and learns behavior patterns of residents. These are used to detect deviations from personal norms that may signal a short- or longterm decline in resident health. The back-end is extensible to new analyses using a modular framework, wherein programs consume input sensor streams, filter and process them, and produce output streams in the database for other modules to use. These are composed hierarchically from low-level sensor streams to high-level inference of symptoms and diseases.

User Interfaces allow doctors, nurses, residents, family, and others to query sensor data, subject to enforced privacy policies. We developed a patient-tracking GUI for a nurse's station, and a query issuer for a PDA that graphs sensor data in real-time. These programs are not trusted components—they must connect through AlarmGate and do not have direct access to the database. This makes it easier to develop and deploy new interfaces customized to the application's needs.

In summary, AlarmNet's architecture supports health monitoring applications due to its flexibility and extensibility in 1) supporting dynamic addition of heterogeneous devices, sensors, and body networks, 2) feeding learned resident and system context back into the network, and 3) providing an open client model for future extension.

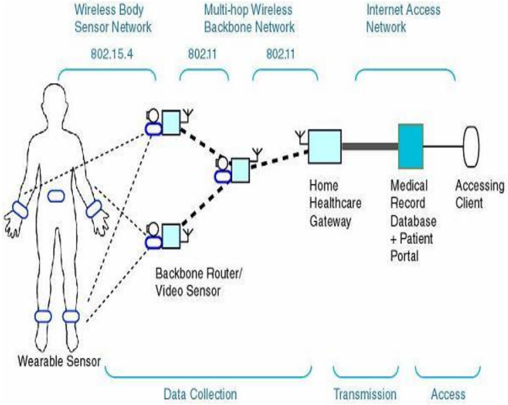

Fig 2. AlarmNet architecture

A two-tier wireless network is used to provide data sensing, collection, transmission and processing functions. At the lower tier, a body sensor network consisting of lightweight *wearable sensors* provides data sensing and transmission functions. These sensors communicate with each other and the *base-station sensors* (which are attached to the backbone wireless network) directly using IEEE 802.15.4 wireless standard. We use Telos motes as the hardware devices. For movement sensing and fall detection, these motes are equipped with accelerometers and gyroscopes. At this tier, sensor devices are lightweight, wearable and mobile, which also means they have low computation, communication power and small amount of memory. So in our design, only necessary computational and communication tasks are implemented at these devices.

At the upper tier of the network is a multi-hop IEEE 802.11-based wireless network which provides a high-performance *backbone structure* for packet routing. We use Stargate single board computers as the hardware devices. The backbone routers are connected to the base-station motes which communicate with the mobile wearable sensors directly. The Stargate board can also be connected with a web camera and serves as a video sensor. Equipped with IEEE 802.11 wireless adaptors, the backbone routers communicate with each other and relay the movement sensing data as well as video streams to the *home healthcare gateway*. Using IEEE 802.11 wireless communication standard, this stationary backbone structure provides a high-performance and high-reliability packet routing service. Since IEEE 802.11 has a larger communication range than IEEE 802.15.4, our design also scales much better in terms of local area communication coverage. Finally, the *home healthcare gateway* serves as an interface between the patient's home and the care giver's medical system, which processes all the sensing data and transmits them to the remote medical care system.

B) IEEE MAC OVERVIEW[3]

IEEE standard 802.15.4 intends to offer the fundamental lower network layers of a type of wireless personal area network (WPAN) which focuses on low-cost, low-speed ubiquitous communication between devices (in contrast with other, more end-user oriented approaches, such as Wi-Fi). The emphasis is on very low cost communication of nearby devices with little to no underlying infrastructure, intending to exploit this to lower power consumption even more.

The basic framework conceives a 10-meter communications range with a transfer rate of 250 kbit/s. Tradeoffs are possible to favor more radically embedded devices with even lower power requirements, through the definition of not one, but several physical layers. Lower transfer rates of 20 and 40 kbit/s were initially defined, with the 100 kbit/s rate being added in the current revision.

Even lower rates can be considered with the resulting effect on power consumption. As already mentioned, the main identifying feature of IEEE 802.15.4 among WPANs is the importance of achieving extremely low manufacturing and operation costs and technological simplicity, without sacrificing flexibility or generality.

Important features include real-time suitability by reservation of guaranteed time slots, collision avoidance through CSMA/CA and integrated support for secure communications. Devices also include power management functions such as link quality and energy detection.

Protocol architecture

Devices are conceived to interact with each other over a conceptually simple wireless network. The definition of the network layers is based on the OSI model; although only the lower layers are defined in the standard, interaction with upper layers is intended, possibly using an IEEE 802.2 logical link control sublayer accessing the MAC through a convergence sublayer. Implementations may rely on external devices or be purely embedded, self-functioning devices as shown in fig3..

The physical layer

Physical layer is the initial layer in the OSI reference model used worldwide as shown in fig. 7. The *physical layer* (PHY) ultimately provides the data transmission service, as well as the interface to the *physical layer management entity*, which offers access to every layer management function and maintains a database of information on related personal area networks. Thus, the PHY manages the physical RF transceiver and performs channel selection and energy and signal management functions. It operates on one of three possible unlicensed frequency bands:

- 868.0-868.6 MHz: Europe, allows one communication channel (2003), extended to three (2006)
- 902-928 MHz: North America, up to ten channels (2003), extended to thirty (2006)
- 2400-2483.5 MHz: worldwide use, up to sixteen channels (2003, 2006)

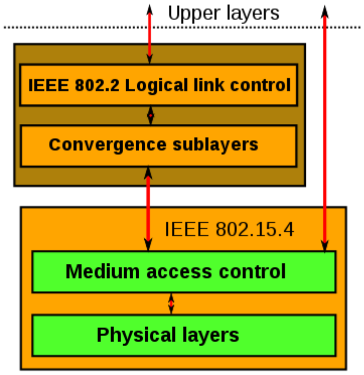

Fig3 . MAC protocol[3]

The original 2003 version of the standard specifies two physical layers based on *direct sequence spread spectrum* (DSSS) techniques: one working in the 868/915 MHz bands with transfer rates of 20 and 40 kbit/s, and one in the 2450 MHz band with a rate of 250 kbit/s.

The 2006 revision improves the maximum data rates of the 868/915 MHz bands, bringing them up to support 100 and 250 kbit/s as well. Moreover, it goes on to define four physical layers depending on the modulation method used. Three of them preserve the DSSS approach: in the 868/915 MHz bands, using either binary or offset quadrature phase shift keying (the second of which is optional); in the 2450 MHz band, using the latter. An alternative, optional 868/915 MHz layer is defined using a combination of binary keying and amplitude shift keying (thus based on parallel, not sequential spread spectrum, PSSS). Dynamic switching between supported 868/915 MHz PHYs is possible.

Beyond these three bands, the IEEE 802.15.4c study group is considering the newly opened 314-316 MHz, 430-434 MHz, and 779-787 MHz bands in China, while the IEEE 802.15 Task Group 4d is defining an amendment to the existing standard 802.15.4-2006 to support the new 950 MHz-956 MHz band in Japan. First standard amendments by these groups were released in April 2009.

In August 2007, IEEE 802.15.4a was released expanding the four PHYs available in the earlier 2006 version to six, including one PHY using Direct Sequence ultra-wideband (UWB) and another using chirp spread spectrum (CSS). The UWB PHY is allocated frequencies in three ranges: below 1 GHz, between 3 and 5 GHz, and between 6 and 10 GHz. The CSS PHY is allocated spectrum in the 2450 MHz ISM band.[3]

In April, 2009 IEEE 802.15.4c and IEEE 802.15.4d were released expanding the available PHYs with several additional PHYs: one for 780 MHz band using O-QPSK or MPSK,[4] another for 950 MHz using GFSK or BPSK.[5]

On February 6, 2012 the IEEE Standards Association Board approved the IEEE 802.15.4e which concludes all Task Group 4e efforts. IEEE802.15.4e is chartered to define a MAC amendment to the existing standard 802.15.4-2006 which adopts channel hopping strategy to improve support for the industrial markets increases, robustness against external interference and persistent multi-path fading.

The MAC layer[2]

The *medium access control* (MAC) enables the transmission of MAC frames through the use of the physical channel. Besides the data service, it offers a management interface and itself manages access to the physical channel and network beaconing. It also controls frame validation, guarantees time slots and handles node associations. Finally, it offers hook points for secure services.

Higher layers

Other higher-level layers and interoperability sublayers are not defined in the standard. There exist specifications, such as 6LoWPAN and ZigBee, which build on this standard to propose integral solutions. TinyOS, Unison RTOS, DSPnano RTOS and Contiki stacks also use a few items of IEEE 802.15.4 hardware.

Network model

Node types

The standard defines two types of network node.

The first one is the **full-function device** (FFD). It can serve as the coordinator of a personal area network just as it may function as a common node. It implements a general model of communication which allows it to talk to any other device: it may also relay messages, in which case it is dubbed a coordinator (PAN coordinator when it is in charge of the whole network).

On the other hand there are **reduced-function devices** (RFD). These are meant to be extremely simple devices with very modest resource and communication requirements; due to this, they can only communicate with FFDs and can never act as coordinators.

Topologies

Networks can be built as either peer-to-peer or star networks. However, every network needs at least one FFD to work as the coordinator of the network. Networks are thus formed by groups of devices separated by suitable distances. Each device has a unique 64-bit identifier, and if some conditions are met short 16-bit identifiers can be used within a restricted environment. Namely, within each PAN domain, communications will probably use short identifiers.

Peer-to-peer (or point-to-point)

Networks can form arbitrary patterns of connections, and their extension is only limited by the distance between each pair of nodes. They are meant to serve as the basis for ad hoc networks capable of performing self-management and organization. Since the standard does not define a network layer, routing is not directly supported, but such an additional layer can add support for multihop communications. Further topological restrictions may be added; the standard mentions the cluster tree as a structure which exploits the fact that an RFD may only be associated with one FFD at a time to form a network where RFDs are exclusively leaves of a tree, and most of the nodes are FFDs. The structure can be extended as a generic mesh network whose nodes are cluster tree networks with a local coordinator for each cluster, in addition to the global coordinator as shown in fig.4.

A more structured **star** pattern is also supported, where the coordinator of the network will necessarily be the central node. Such a network can originate when an FFD decides to create its own PAN and declare itself its coordinator, after choosing a unique PAN identifier. After that, other devices can join the network, which is fully independent from all other star networks as shown in fig.5.

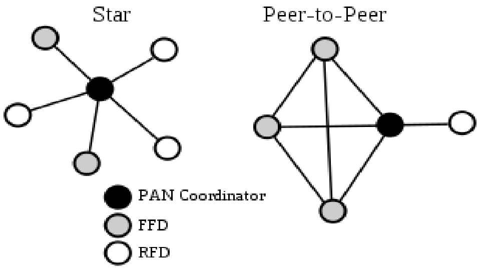

Fig 4. IEEE 802.15.4 star and peer-to-peer

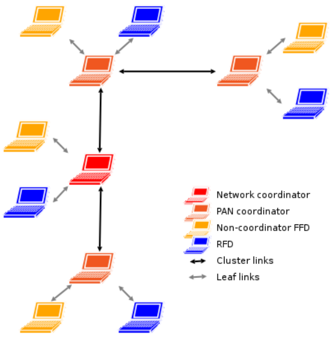

Fig 5. IEEE 802.15.4 cluster tree

Data transport architecture

Frames are the basic unit of data transport, of which there are four fundamental types (data, acknowledgment, beacon and MAC command frames), which provide a reasonable tradeoff between simplicity and robustness. Additionally, a superframe structure, defined by the coordinator, may be used, in which case two beacons act as its limits and provide synchronization to other devices as well as configuration information. A superframe consists of sixteen equal-length slots, which can be further divided into an active part and an inactive part, during which the coordinator may enter power saving mode, not needing to control its network.

Within superframes contention occurs between their limits, and is resolved by CSMA/CA. Every transmission must end before the arrival of the second beacon. As mentioned before, applications with well-defined bandwidth needs can use up to seven domains of one or more contentionless guaranteed time slots, trailing at the end of the superframe. The first part of the superframe must be sufficient to give service to the network structure and its devices. Superframes are typically utilized within the context of low-latency devices, whose associations must be kept even if inactive for long periods of time.

Data transfers to the coordinator require a beacon synchronization phase, if applicable, followed by CSMA/CA transmission (by means of slots if superframes are in use); acknowledgment is optional. Data transfers from the coordinator usually follow device requests: if beacons are in use, these are used to signal requests; the coordinator acknowledges the request and then sends the data in packets which are acknowledged by the device. The same is done when superframes are not in use, only in this case there are no beacons to keep track of pending messages.

Point-to-point networks may either use unslotted CSMA/CA or synchronization mechanisms; in this case, communication between any two devices is possible, whereas in “structured” modes one of the devices must be the network coordinator.

In general, all implemented procedures follow a typical request-confirm/indication-response classification.

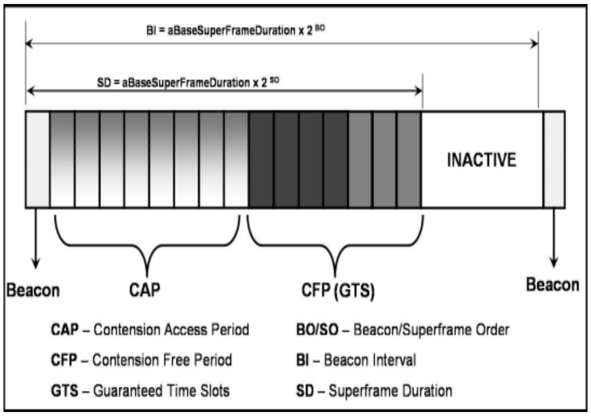

Figure 6: The SuperFrame Structure[5]

Functional Overview

The Superframe structure[5]

The superframe structure (Figure 6) is an optional part of a WPAN. It is the time duration between two consecutive beacons. The structure of the superframe is determined by the coordinator. The coordinator can also switch off the use of a superframe by not transmitting the beacons. The superframe duration is divided into 16 concurrent slots. The beacon is transmitted in the first slot. The remaining part of the superframe duration can be described by the terms, CAP, CFP and Inactive. The superframe is used to provide vital statistics like synchronization, identifying the PAN and the superframe structure, to the devices connected in a Wireless PAN. This information is critical for the operation of the PAN in a Beacon enabled network.

Contention Access Period : It is the time duration in symbols during which the devices can compete with each other to access the channel using CSMA-CA and transmit the data.

Contention Free Period/Guaranteed Time Slots : It is the time duration for which certain low-latency application devices are given exclusive rights over the channel and the devices can directly start transmitting the data. There can as many as 7 slots assigned for GTS transmissions. These transmissions start immediately after the contention access period.
Inactive Period : It is the time period during which the coordinator goes to a power save mode and it would not interact with the PAN. Therefore, during this time, there will be no beacon transmissions. This implies that the devices also go to sleep mode for this duration.
Superframe Duration : The total time duration of the CAP, CFP (GTS) and a Beacon. The Superframe duration doesn't include the inactiveperiod.
Beacon Interval : It is the time duration between two successive beacons.

Synchronization is key for better throughput in the network. Every device in the network when ready to transmit data should compete for the channel. But to compete for the channel, they should know when the contention access periods start. And this is what the superframe structure or truly, the beacon transmission does. This information is embedded into the beacon, and the device receiving the beacon can extract this information and get ready to compete for the channel. Similarly is the case when a device wants to exclusively transmit in the GTS mode. It is the coordinator that would assign a device access to the GTS.

The structure of the superframe structure is determined by two parameters. The Superframe Order (SO) and the Beacon Order (BO). The superframe order is the variable which is used to determine the length of the superframe duration. Similarly the Beacon Interval is determined by the variable BO.

$1 <= SO <= 15$

$1 <= BO <= 15$

For BO=15 shall indicate that there are no beacon transmissions. Also for SO = BO (Figure 7), the beacon interval is same as the superframe duration indicating there is no inactive portion. Similarly, when BO is greater than SO (Figure 8), indicates there is an inactive portion present in the superframe.

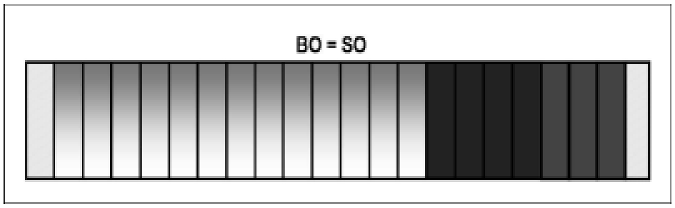

Figure 7: BO = SO

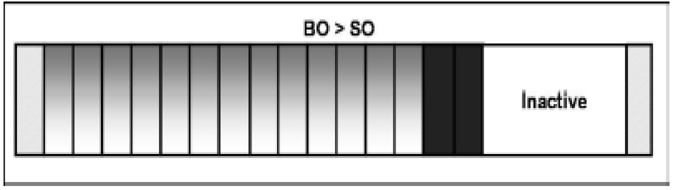

Figure 8: BO > SO

The beacon interval and the active and inactive part of the superframe are calculated, in the following computation.

Beacon Interval[5]

$BI=aBaseSuperFrameDuration\text{ï¿½}2^{BO} symbols$ (1)

$aBaseSuperFrameDuration = aBaseSlotDuration\ \text{ï¿½}aNumSuperframeSlots$ (2)

$aBaseSlotDuration = 60 symbols$

$aNumSuperFrameSlots = 16$

$aBaseSuperFrameDuration = 60\ \text{ï¿½}\ 16 symbols = 960 symbols$ (3)

Lets calculate the beacon interval with BO=8 and SO=7.

$BI = 960\ \text{ï¿½}2^{BO} symbols$

$BI|_{BO=8} = 960\ \text{ï¿½}28 = 245760 symbols$

$BI|_{20kbps} = 245760/20000 = 12.288$

$BI = 12.288 secs$ (4)

Similarly the Superframe duration can be calculated using the superframe order as follows

$SD = aBaseSuperframeDuration\ \text{ï¿½}2^{SO}$ (5)

$SD = 960\ \text{ï¿½}2^{SO} symbols$

$SD|_{SO=5} = 960\ \text{ï¿½}27 = 122880 symbols$

$SD|_{20kbps} = 122880/20000 = 6.144 secs$

$SD = 6.144 secs$ (6)

$aBaseSuperframeDuration = SD/16 = 6.144/16 = 0.384 secs$

$aBaseSuperframeDuration = 0.384 secs$ (7)

And finally the inactive portion of the superframe can be calculated as,

$InactivePortion = BeaconInterval - SuperframeDuration$ (8)

$InactivePortion = 12.288 - 6.144 = 6.144 secs$ (9)

The figure 9 indicates all the time periods for a superframe with BO=8 and SO=7.

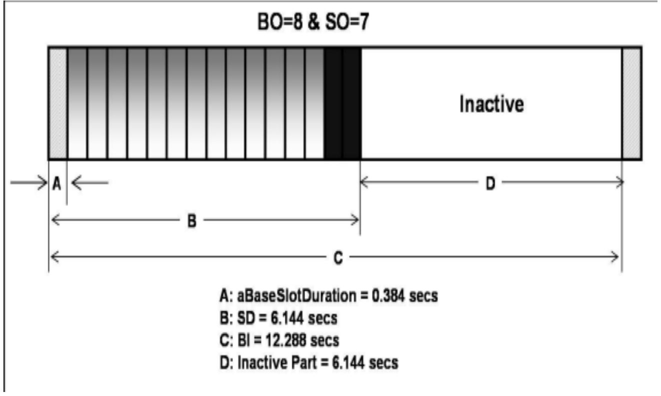

Figure 9: Superframe Duration and Beacon Interval

III. CONCLUSION

The purpose of this paper has been to describe and discuss the wireless technology and its different standards. This paper will help us in understanding the capabilities of WLAN. The evolution of wireless technology has perceived as a powerful tool for getting fast information which will become universal in the near future. But the way users receive that information is changing. WLAN and its applications provide the real-time implementation of IEEE 802.15.4.

REFERENCES

[1] Hsueh-Wen Tseng, Shiann-Tsong Sheu, *Member, IEEE*, and Yun-Yen Shih,” Rotational Listening Strategy for IEEE 802.15.4 Wireless Body Networks”, IEEE SENSORS JOURNAL,VOL. 11,NO.9,SEPTEMBER 2011.

[2] Crow, B. P., etal., “IEEE 802.11 Wireless Local Area Network,” *IEEE Communications Magazine*,Sept. 1997, pp. 116–126.

[3] IEEE 802.11, IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Nov. 1997.

[4] Anthony D. Wood, John A. Stankovic, Gilles Virone, Leo Selavo, Zhimin He, Qiuhua Cao,Thao Doan, Yafeng Wu, Lei Fang, and Radu Stoleru, University of Virginia” *Context-Aware Wireless Sensor Networks for Assisted Living and Residential Monitoring*” 0890-8044/08/$25.00 © 2008 IEEE IEEE Network • July/August 2008

[5] Seong-eun Yoo, Poh Kit Chong, *Student Member, IEEE*, Daeyoung Kim, *Member, IEEE*, Yoonmee Doh, Minh-Long Pham, *Student Member, IEEE*, Eunchang Choi, and Jaedoo Huh” Guaranteeing Real-Time Services for Industrial Wireless Sensor Networks With IEEE 802.15.4” IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 57, NO. 11, NOVEMBER 2010