Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 950704, 12 pages
http://dx.doi.org/10.1155/2013/950704

Review Article

A Review of IEEE 802.15.6 MAC, PHY, and Security Specifications

Sana Ullah,[1,2] Manar Mohaisen,[3] and Mohammed A. Alnuem[1,2]

[1] *Department of Information System, College of Computer and Information Science, King Saud University, Riyadh 11543, Saudi Arabia*
[2] *Chair of Pervasive and Mobile Computing, King Saud University, Riyadh 11543, Saudi Arabia*
[3] *Department of EEC Engineering, Korea Tech, Cheonan 330-708, Republic of Korea*

Correspondence should be addressed to Sana Ullah; sanajcs@gmail.com

Received 24 December 2012; Accepted 12 March 2013

Academic Editor: Muhammad Khurram Khan

IEEE 802.15.6 is the first international Wireless Body Area Network (WBAN) standard that supports communications in the vicinity of or inside a human body to serve a variety of medical and nonmedical applications. The standard defines a Medium Access Control (MAC) layer that supports several Physical (PHY) layers. In this paper, the key features of the IEEE 802.15.6 standard are presented. The MAC, PHY, and security specifications of the standard are explained in detail. Different communication modes and access mechanisms are presented. The Narrowband (NB), Ultra-wideband (UWB), and Human Body Communications (HBC) specifications are reviewed in terms of frame structure, modulation, and other important parameters. Finally, the security paradigm and services of the standard are highlighted.

1. Introduction

Wireless Body Area Networks (WBANs) are replacing conventional healthcare systems by enabling the ambulatory and continuous health monitoring of patients suffering from chronic diseases, such as heart disease [1–3]. The recent popularity of WBANs has attracted a number of researchers from academia and industry in the past few years. The heterogeneous WBAN requirements have allowed the realisation of a standard model that can support all of the relevant requirements. In November 2007, IEEE 802 established a task group for the standardisation of WBAN called IEEE 802.15.6 [4]. Earlier, IEEE 802 had several successful experiences in developing international standards for wireless communications [5–8], including the IEEE 802.11 [9], IEEE 802.15.1 [10], and IEEE 802.15.4 [11] standards. The aim of the IEEE 802.15.6 standard was to develop a communications standard for miniaturised low-power devices that are deployed on or implanted inside a human body to serve a variety of medical, consumer electronics (CE), and entertainment applications [12]. The standardisation body received a total of 34 proposals, which were later merged into a single proposal. In July 2011, the initial draft of the standard was approved to start a sponsor ballot. The final version of the standard was published in February 2012.

The IEEE 802.15.6 standard defines a Medium Access Control (MAC) layer that supports several Physical (PHY) layers, such as Narrowband (NB), Ultra-wideband (UWB), and Human Body Communications (HBC) layers, as illustrated in Figure 1. The proper selection of PHYs or frequency bands has remained one of the important issues to be considered in the development of WBANs [13]. Generally, the available frequencies for WBANs are regulated by communication authorities in different countries. Figure 2 shows the available frequency bands for WBANs [14]. The Medical Implant Communications Service (MICS) band is a licensed band used for implant communications and has the same frequency range of 402–405 MHz in most countries. Wireless Medical Telemetry Services (WMTSs) is a licensed band used for medical telemetry systems. The problems with the MICS and WMTS bands are their inability to support high-data-rate applications. The Industrial, Scientific, and Medical (ISM) and Ultra-wideband (UWB) bands support high-data-rate applications and are available worldwide. However, there is a high probability of interference because many wireless

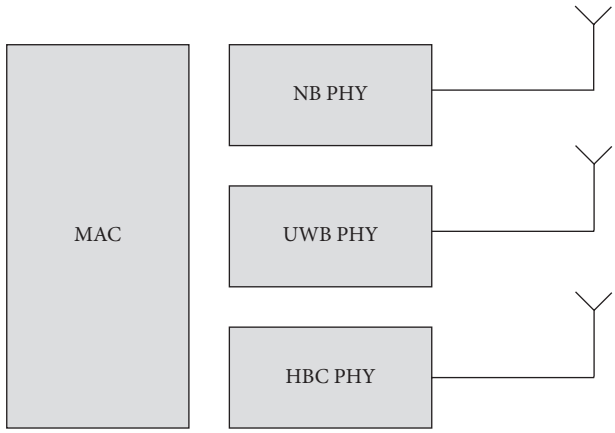


Figure 1: IEEE 802.15.6 MAC and PHY layers.

devices, including those using the IEEE 802.11 and IEEE 802.15.4 standards, operate in the 2.4 GHz band [15]. For efficient resource allocation on the channel, the standard allows the nodes and hubs (which are also known as coordinators) to establish a time reference base, where the time axis is divided into multiple superframes of equal length [16–18]. In this paper, we present the key features of the IEEE 802.15.6 standard. Starting from the fundamental details, we provide deep insight into the MAC and PHY layers and the security specifications of the standard. We review different communication modes and access mechanisms and explain the NB, UWB, and HBC specifications in detail. We also review the security paradigm and services of IEEE 802.15.6.

The remainder of this paper is organised into four sections. Sections 2 and 3 present the IEEE MAC and PHY specifications, respectively. Section 4 presents the security specifications, and Section 5 concludes our work.

2. IEEE 802.15.6 MAC Specifications

According to the IEEE 802.15.6 standard, the nodes are organised into one- or two-hop star WBANs. A single coordinator or hub controls the entire operation of each WBAN. The WBAN must have one hub and a number of nodes, ranging from zero to *mMaxBANSize*. In a two-hop start WBAN, a relay-capable node may be used to exchange data frames between a node and the hub. The standard divides the time axis or channel into beacon periods or superframes of equal length. Each superframe contains a number of allocation slots that are used for data transmission. These slots have equal duration and are numbered from 0 to s, where $s \leq 255$. The hub transmits beacons to define the superframe boundaries and allocate the slots. For nonbeacon modes, the superframe boundaries where beacons are not used are defined by polling frames. Generally, the hub transmits beacons in each superframe except those that are inactive. The hub may shift or rotate the offsets of the beacon periods, thus shifting the schedule allocation slots. The following sections present the MAC frame format, communication modes, and access mechanisms defined in the IEEE 802.15.6 standard.

2.1. IEEE 802.15.6 MAC Frame Format. Figure 3 shows the general MAC frame format consisting of a 56-bit header, variable length frame body, and 18-bit Frame Check Sequence (FCS). The maximum length of the frame body is 255 octets. The MAC header further consists of 32-bit frame control, 8-bit recipient Identification (ID), 8-bit sender ID, and 8-bit WBAN ID fields. The frame control field carries control information including the type of frame, that is, beacon, acknowledgement, or other control frames. The recipient and sender ID fields contain the address information of the recipient and the sender of the data frame, respectively. The WBAN ID contains information on the WBAN in which the transmission is active. The first 8-bit field in the MAC frame body carries message freshness information required for nonce construction and replay detection. The frame payload field carries data frames, and the last 32-bit Message Integrity Code (MIC) carries information about the authenticity and integrity of the frame.

2.2. IEEE 802.15.6 Communication Modes. The IEEE 802.15.6 supports the following communication modes.

2.2.1. Beacon Mode with Superframe Boundaries. In this mode, the hub transmits beacons in active superframes. The active superframes may be followed by several inactive superframes whenever there is no scheduled transmission. As illustrated in Figure 4(a), the superframe structure is divided into Exclusive Access Phases (EAP1 and EAP2), Random Access Phases (RAP1 and RAP2), a Managed Access Phase (MAP), and a Contention Access Phase (CAP). The EAPs are used to transfer high-priority or emergency traffic. The RAPs and CAP are used for nonrecurring traffic. The MAP period is used for scheduled and unscheduled bilink allocations, scheduled uplink and downlink allocations, and Type I (not Type II) polled and posted allocations. The length of Type I and Type II allocations is represented in terms of the transmission time and number of frames, respectively. A detailed discussion of these allocations is presented in Section 2.3.

2.2.2. Nonbeacon Mode with Superframe Boundaries. In this mode, the hub operates during the MAP period only, as illustrated in Figure 4(b).

2.2.3. Nonbeacon Mode without Superframe Boundaries. In this mode, the hub provides unscheduled Type II polled or posted allocations or a combination of both, as depicted in Figure 4(c).

2.3. IEEE 802.15.6 Access Mechanisms. The IEEE 802.15.6 supports the following access mechanisms.

2.3.1. Random Access Mechanism. In EAP, RAP, and CAP periods, the hub may employ either a slotted ALOHA or Carrier Sensor Multiple Access/Collision Avoidance (CSMA/CA) protocol, depending on the PHY. The hub considers slotted ALOHA and CSMA/CA protocols for UWB and NB PHYs, respectively. To send high-priority data frames using CSMA/CA, the hub may combine EAP1 and RAP1

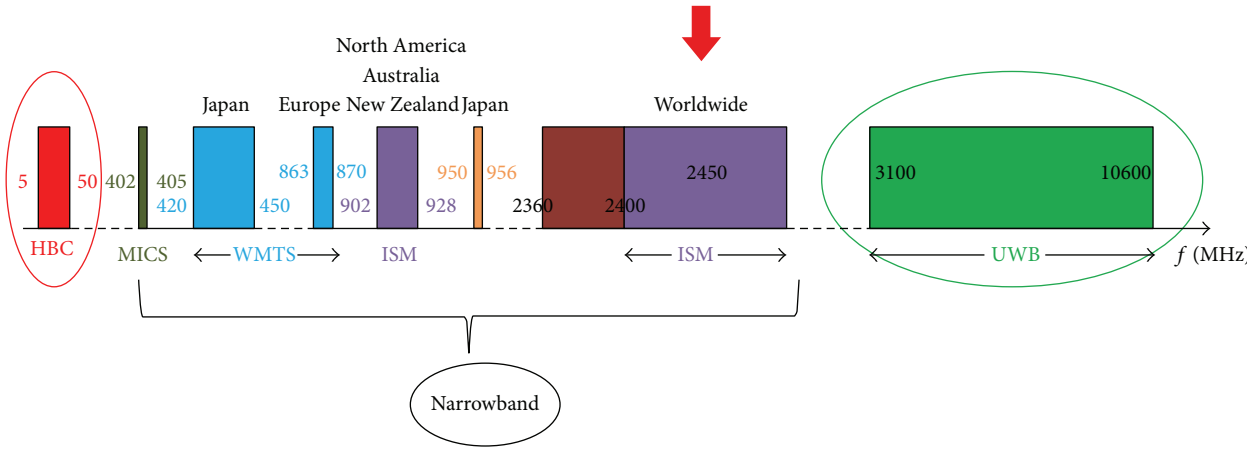


Figure 2: IEEE 802.15.6 frequency bands.

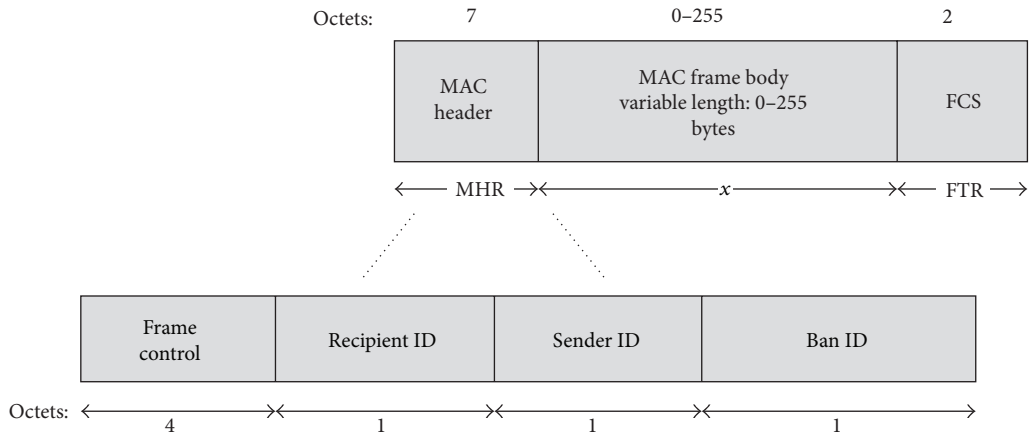
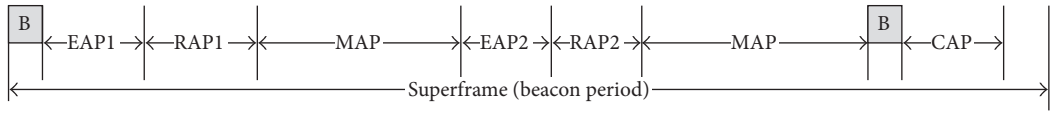
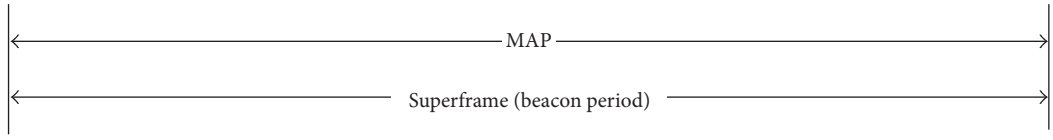


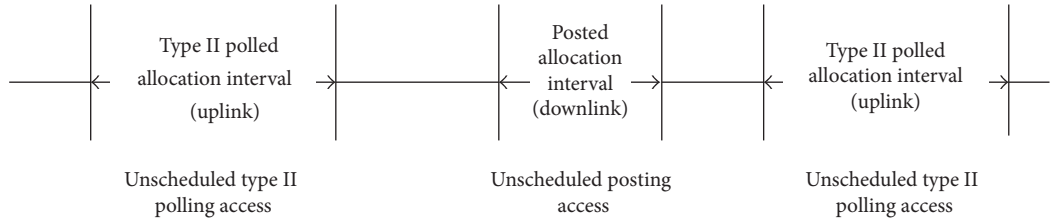
Figure 3: IEEE 802.15.6 MAC frame format.



(a) Beacon mode with superframe boundaries



(b) Nonbeacon mode with superframe boundaries



(c) Nonbeacon mode without superframe boundaries

Figure 4: IEEE 802.15.6 communication modes.

Table 1: Bounds for slotted-ALOHA and CSMA/CA protocols.

User Priorities	Slotted-ALOHA		CSMA/CA	
	CP_{max}	CP_{min}	CW_{min}	CW_{max}
0	0.125	0.0625	16	64
1	0.125	0.0937	16	32
2	0.25	0.0937	8	32
3	0.25	0.125	8	16
4	0.375	0.125	4	16
5	0.375	0.1875	4	8
6	0.5	0.1875	2	8
7	1	0.25	1	4

into a single EAP1 period and EAP2 and RAP2 into a signal EAP2 period. When using slotted ALOHA for high-priority traffic, EAP1 and EAP2 are not extended, but RAP1 and RAP2 are simply replaced by another EAP1 and EAP2 period. The following sections briefly describe the slotted ALOHA and CSMA/CA protocols.

(1) Slotted ALOHA Protocol. In the slotted ALOHA protocol, the nodes access the channel using predefined User Priorities (UPs), as given in Table 1. These priorities are used to classify the high- and low-priority traffic. Initially, the Collision Probability (CP) is selected according to the UPs. The nodes obtain contended allocation if $z \leq \mathrm{CP}$, where z is randomly selected from the interval [0, 1]. If the node fails to transmit, the CP remains unchanged into an odd number of failures and the node divides it equally for an even number of failures.

(2) CSMA/CA Protocol. In the CSMA/CA protocol, the node initially sets its backoff counter to a random integer that is uniformly distributed over the interval [1, Contention Window (CW)], where $\mathrm{CW} \in (\mathrm{CW}_{min}, \mathrm{CW}_{max})$. As given in Table 1, the values of CW_{min} and CW_{max} are selected according to the UPs. The high-priority traffic will have a small contention window compared to that of low-priority traffic, which increases the probability of accessing the channel to report emergency events. The node starts decrementing the backoff counter by one for each idle CSMA slot with a length equal to *pCSMASlotLength*. Particularly, the node considers a CSMA slot to be idle if it determines that the channel has been idle between the start of the CSMA slot and *pCCATime*. The node decreases the backoff counter *pCCATime* after the start of the CSMA slot. Once the backoff counter reaches zero, the node transmits the frame. If the channel is busy due to frame transmission, the node locks its backoff counter until the channel is idle. The CW is doubled for an even number of failures until it reaches CW_{max}. Figure 5 shows an example of the CSMA/CA protocol. As shown in the figure, the node unlocks the backoff counter in RAP1. However, the contention fails and the value of CW remains unchanged because CW does not change for an odd number of failures. In the following CAP period, the backoff counter is set to five; however, it is locked at two because the time between the end of the slot and the end of the CAP is not sufficient to accommodate the data frame transmission and Nominal Guard Time (GT_n). The backoff counter is then unlocked in the RAP2 period. This time, the value of CW is doubled because there is an even number of contention failures. The backoff counter is set to eight and is unlocked. Once the backoff counter reaches zero, the data are transmitted and the value of CW is set to CW_{max}.

We analysed the performance of an IEEE 802.15.6-based CSMA/CA for NB PHYs in terms of the theoretical throughput, delay and bandwidth efficiency, as presented in Table 2 [19–21]. The theoretical bounds are presented for No Acknowledgement (NACK) and Acknowledgement (ACK) policies. This analysis considers a single sender and single receiver with no collisions on the channel. The theoretical throughput and delay are bounded because of the additional overhead accumulated in each layer. These strict bounds cannot be achieved in a practical environment. However, these bounds can be used by the system designer for network provisioning and packet-size optimisation for different application scenarios.

2.3.2. Improvised and Unscheduled Access Mechanism. As discussed above, the hub may use improvised access to send poll or post commands without prereservation or advance notice in beacon or nonbeacon modes with superframe boundaries. These commands are used to initiate the transactions of one or more data frames by the nodes or hub outside the scheduled allocation interval. The polls are used to grant Type I or Type II polled allocation to the nodes, while the posts are used to send management frames. The Type I polled allocation starts after the duration of *pSIFS* and stops at the end of the allocated slot in the current superframe. Similarly, the Type II polled allocation starts after the duration of *pSIFS* and stops after all of the data frames are sent by the polled node. Figure 6 illustrates an example of immediate polled allocations.

The hub may also use an unscheduled access mechanism to obtain an unscheduled bilink allocation. The unscheduled bilink allocation may be (1) one-periodic, where frames are exchanged between the nodes and hub every superframe, or (2) multiple-periodic (m-periodic), where frames are exchanged every m superframes thus allowing the devices to sleep between m superframes. An m-periodic bilink allocation is suitable for low-duty cycle nodes because nodes in m-periodic allocation sleep between m superframes.

2.3.3. Scheduled and Scheduled-Polling Access Mechanisms. Unlike unscheduled allocation, the scheduled access mechanism is used to obtain scheduled uplink, downlink, and bilink allocations. In addition, the scheduled polling is used for polled and posted allocations. These allocations may be one-periodic or m-periodic; however, neither of these allocations is allowed in a single WBAN at the same time. The nodes consider the superframe periods (with allocated slots) as the wakeup periods. The uplink and downlink allocations are used to send management and data frames to and from the hub, respectively. Figure 7 illustrates an example of scheduled one-periodic allocations.

Table 2: Theoretical limits of IEEE 802.15.6 for NB PHYs.

420–450 MHz (PHY header rate = 57.5 kbps, PHY symbol rate = 187.5 kbps)							863–870 MHz (PHY header rate = 76.6 kbps, PHY symbol rate = 250 kbps)						
Data rate (kbps)	Maximum Throughput (kbps)		Theoretical delay (ms)		Bandwidth efficiency (%)		Data rate (kbps)	Maximum Throughput (kbps)		Theoretical delay (ms)		Bandwidth efficiency (%)	
	NACK	ACK	NACK	ACK	NACK	ACK		NACK	ACK	NACK	ACK	NACK	ACK
75.9	70.45	67.5	28.34	29.63	92.82	88.9	101.2	93.87	89.7	21.31	22.29	92.75	88.6
151.8	134.8	129	14.79	15.45	88.8	85.2	404.8	329.9	315.5	6.06	6.33	81.5	77.9
187.5	163.2	156	12.21	12.75	87.03	83.6	607.1	457.8	437.9	4.36	4.56	75.4	72.1

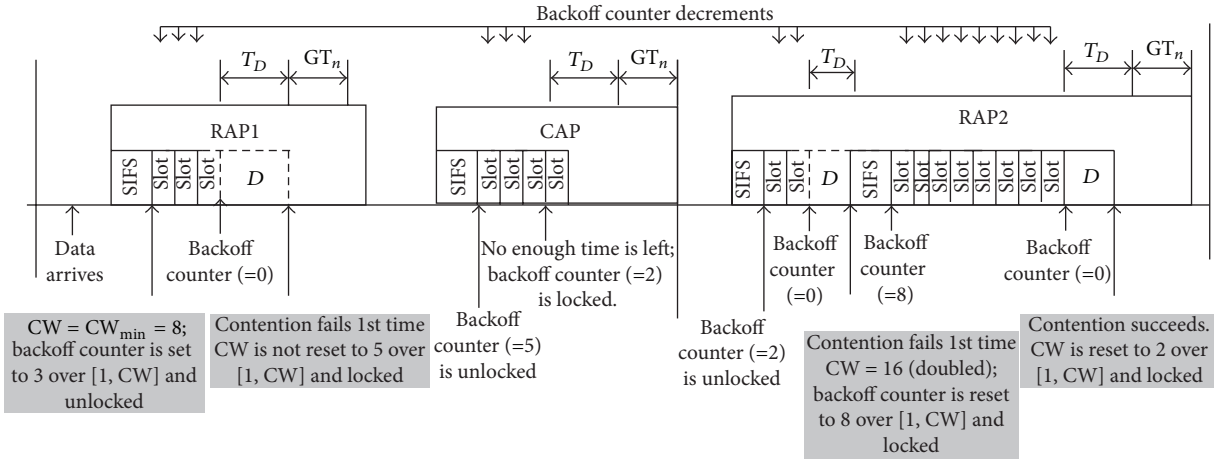


Figure 5: IEEE 802.15.6 CSMA/CA protocol: slot = CSMA slot SIFS = Psifs, D = frame transaction initiated by node 1 in a contended allocation (e.g., a data type frame and an I-Ack frame with pSIFS in between), T_D = time required to complete D, GT$_n$ = nominal guard time.

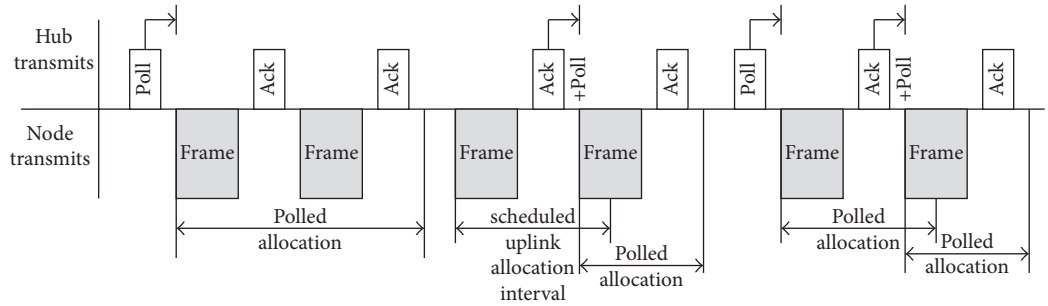


Figure 6: Immediate polled allocations.

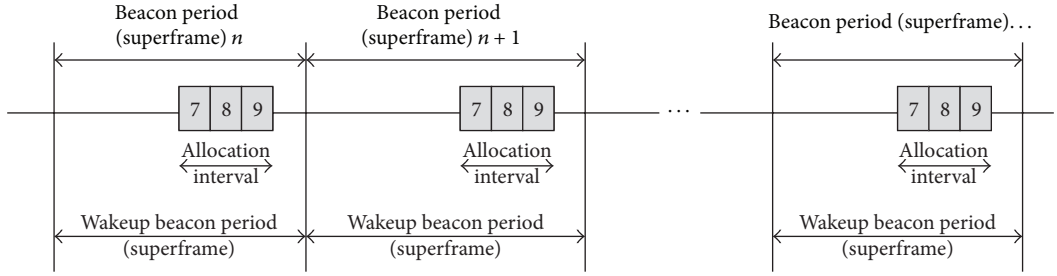


Figure 7: Scheduled one-periodic allocation.

Table 3: Transmission parameters in NB PHY.

Frequency band	Packet component	Modulation	Modulation order (M)	Symbol rate (R_s ksps)	Code rate BCH (n, k)	Spreading factor (SF)
402–405 MHz	PLCP header PSDU	π/M-DPSK	2 {2, 2, 4, 8}	187.5	(31, 19) (63, 51)	2 {2, 1, 1, 1}
420–450 MHz	PLCP header PSDU	GMSK	2	187.5	(31, 19) {(63, 51), (63, 51), 1}	2 {2, 1, 1}
863–870 MHz	PLCP header PSDU	π/M-DPSK	2 {2, 2, 4, 8}	250	(31, 19) (63, 51)	2 {2, 1, 1, 1}
902–928 MHz	PLCP header PSDU	π/M-DPSK	2 {2, 2, 4, 8}	250	(31, 19) (63, 51)	2 {2, 1, 1, 1}
950–958 MHz	PLCP header PSDU	π/M-DPSK	2 {2, 2, 4, 8}	250	(31, 19) (63, 51)	2 {2, 1, 1, 1}
2360–2400 MHz	PLCP header PSDU	π/M-DPSK	4 {2, 2, 2, 4}	600	(31, 19) (63, 51)	4 {4, 2, 1, 1}
2400–2483.5 MHz	PLCP header PSDU	π/M-DPSK	2 {2, 2, 2, 4}	600	(31, 19) (63, 51)	4 {4, 2, 1, 1}

3. IEEE 802.15.6 PHY Specifications

IEEE 802.15.6 supports three operational PHYs, two of which are mandatory and one of which is optional. The two mandatory PHYs are UWB and HBC PHYs, while the NB PHY is considered optional. In IEEE 802.15.6, PHY is responsible for (1) the activation and deactivation of the radio transceiver, (2) clear channel assessment, and (3) data reception and transmission. The following sections present the NB, HBC, and UWB PHY specifications of IEEE 802.15.6.

3.1. NB PHY Specifications

3.1.1. Operation Bands and Rate-Dependent Parameters. Table 3 summarises the supported frequency bands and corresponding PHY parameters, where WBAN devices must be able to support transmission on at least one of those frequency bands. Differential Phase Shift Keying (DPSK) is used except in the case of the 420 to 450 MHz frequency band, where Gaussian Minimum Shift Keying (GMSK) is employed. In some bands, several parameters have a set of values, where the underlined configurations in Table 3 are optional. Based on the table, the information data rate R_d is given by

$$R_d = \left(\frac{R_s \cdot N}{S} \times \frac{k}{n} \right) (\text{kbps}), \quad (1)$$

where R_s is the symbol rate, S is the spreading factor, k/n is the BCH coding rate, and M is the modulation order and is given by $M = 2^N$.

3.1.2. NB PHY PPDU Structure. The Physical-layer Protocol Data Unit (PPDU) encapsulates the Physical-layer Service Data Unit (PSDU) in its frame and appends several control fields that are used to synchronise the transmission and identify the transmission parameters. Figure 8 depicts the structure of the NB PPDU, and we identify the goal of each field in the following clauses.

PLCP Preamble. The preamble of the Physical-layer Convergence Protocol (PLCP) is a concatenation of two sequences. The first sequence has a length of 63 bits and is used for coarse time synchronisation, carrier-offset recovery, and packet detection. This sequence has two patterns; one pattern is used with odd-indexed channels, and the other is used with even-indexed channels. The second sequence has a fixed pattern length of 27 bits. It is appended to the first sequence and used for fine timing synchronisation.

PLCP Header. The PLCP header consists of several fields that convey the PHY parameters to the receiver, which is referred to as the PHY header and has 16 parity check bits appended. The details of these fields are as follows.

(1) Rate: three bits are used to indicate the information data rate computed using (1), which implicitly indicates the modulation, modulation order, code rate, and spreading factor.

(2) Length: eight bits are used to indicate the length of the MAC body in bytes (0–255 bytes).

(3) Burst mode: one bit is used to indicate the burst transmission.

(4) Scrambler seed: a 1-bit seed that identifies the initial state of the registers in the scrambler. It is initiated to zero and inverted after each PHY frame transmission.

(5) HCS: the Header Check Sequence, which is used for error detection, consists of a 4-bit Cyclic Redundancy Check (CRC-4) that is used to protect the PHY header.

(6) BCH parity check: the BCH field is computed for the concatenation of PHY header and HCS and is used for error correction. This check corrects up to two erroneous bits.

PSDU. As discussed above, the PSDU consists of a MAC header, a MAC frame body, and the FCS.

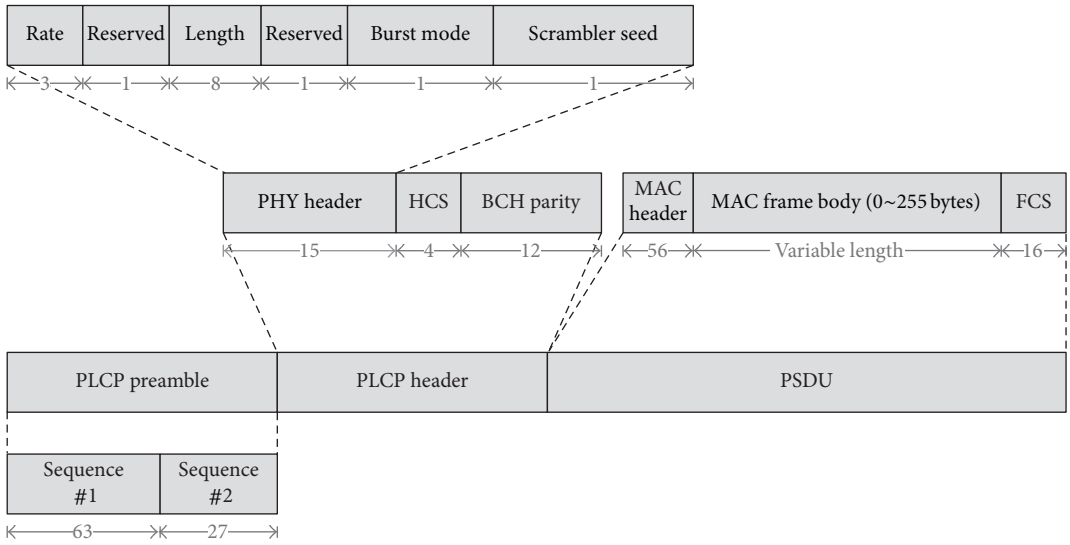


Figure 8: Standard PPDU structure for NB PHY (indicated lengths are in bits).

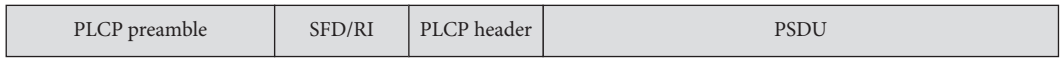


Figure 9: PPDU structure for HBC PHY.

3.1.3. Other NB PHY Specifications

Pulse Shaping. Square-root Raised Cosine (SRRC) is used as the shaping filter in all bands except in the 420 to 450 MHz band, where the Gaussian filter with a bandwidth-time product of 0.5 is used because the latter pulse shaping is recommended for use with GMSK.

Spreading. Bits are spread using simple repetition coding.

Transmit Mask. The transmitter should keep its out-of-band radiations to −20 dBr at most.

Power-On and Power-Off Ramp. The transmit power-on to power-off (or vice versa) ramp should take the duration of five symbols at most.

Receiver Sensitivity. The receiver sensitivity depends on the frequency band and transmission rate, and it ranges from −95 dBm (low frequency and low data rate) to −83 dBm.

Scrambler. The PSDU is whitened using a scrambler with a polynomial of order 14.

3.2. HBC PHY Specifications. HBC PHY uses Electric Field Communication (EFC) technology with the band of operation centred at 21 MHz. Similar to the NB PHY, the HBC packet structure encapsulates the PSDU in the packet after adding control bits and error correction and detection bits, as depicted in Figure 9. In the following, we introduce details about the packet structure.

PLCP Preamble. The initial preamble is generated as a 64-bit gold code sequence that is then repeated four times and spread using a Frequency Shift Code (FSC) with a Spreading Factor (SF) of eight to attain a chip rate of 42 Mcps, where cps denotes chips per second.

Start Frame Delimiter. The SFD indicates the starting point of the frame. Its sequence is generated using a 64-bit gold code generator, which is spread using an FSC with an SF of eight.

Rate Indicator. The SFD/RI field can be used to indicate the rate of transmission. In this case, the receiver does not need to read the PHY header to determine the data rate.

PHY Header. The PHY header is a 32-bit sequence, which is spread at a rate of 42 Mcps. The PHY header is composed of the following fields (we omit the fields already explained for the NB PHY).

(1) Pilot information: two bits indicate the length of the pilot insertion interval. The pilot sequence, which is the same as the SFD sequence, is periodically inserted in the PSDU to maintain synchronisation. If the PSDU is less than the pilot insertion interval, that is, short packet, the pilot is not needed.

(2) CRC8: CRC value is calculated over the PHY header to detect errors at the receiver side.

Scrambler. The PSDU is whitened using a scrambler with polynomial of order 32.

3.3. UWB Specifications. Compared to the two preceding PHY specifications, UWB PHY aims to achieve high performance, low complexity, and low power consumption. In addition, this specification is robust and in compliance with

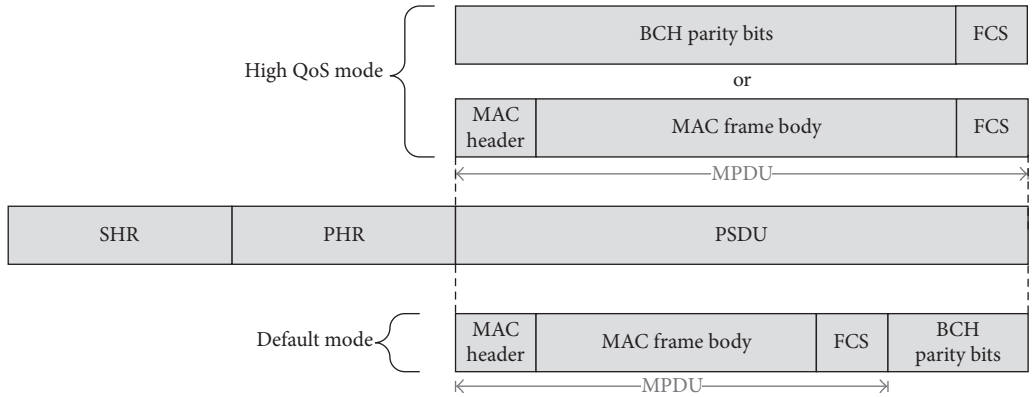


Figure 10: PPDU frame structure for UWB PHY.

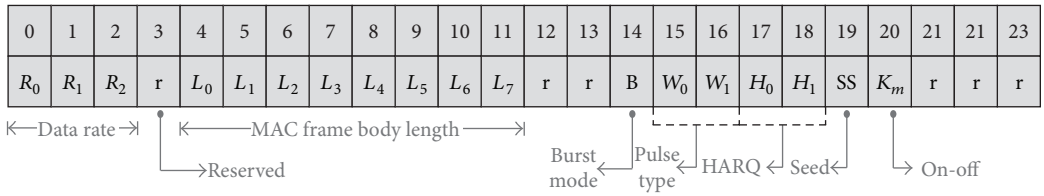


Figure 11: PHR frame structure.

the MICS power limits, which provide safe power levels for human body exposure. UBW PHY supports 11 channels; three in the low band (channels 0–2) and eight in the high band (channels 3–10), where the central frequencies range from 3,494.4 MHz for channel 0 to 9,984 MHz for channel 10, each with a 499.2 MHz bandwidth.

3.3.1. Supported Transceivers and Modes. UWB PHY supports Impulse Radio UWB (IR-UWB) and wideband Frequency Modulation UWB (FM-UWB) technologies. A hub can implement only one of these technologies, but a device can implement either IR- or FM-UWB or both technologies. Furthermore, UWB PHY supports two modes of operation, default mode and high Quality of Service (QoS) mode, where the latter is designated for high-priority medical applications and the default mode is used for medical and nonmedical applications.

3.3.2. Modulation. On-off modulation, Differential-BPSK (DBPSK) modulation, and Differential-QPSK (DQPSK) modulation schemes are supported for the IR-UWB, whereas Continuous Phase Binary FSK (CP-BFSK) is used for the FM-UWB, where the signal obtained from the CP-BFSK modulator is modulated again using wideband FM to create a constant-envelope UWB signal. The wideband FM increases the required transmission bandwidth by a factor of 256.

3.3.3. IR-UWB Symbol Structure. Each symbol time T_{sym} consists of an integer number of pulse waveform positions N_w, each of duration T_w. In DPSK and on-off modulation, the $N_w - 1$ and $((N_w/2) - 1)$ waveform positions, respectively, are used for time hopping. As such, UWN PHY supports the coexistence of multi-BANs.

3.3.4. UWB PHY Frame Format. The PPDU for a UWB frame consists of the Synchronisation Header (SHR), Physical-layer Header (PHR), and PSDU.

PSDU. As shown in Figure 10, the content of the PSDU depends on the operation mode; in the default mode operation, the PSDU is the concatenation of the MAC Protocol Data Unit (MPDU) and the BCH parity bits, whereas it consists of either the MPDU or BCH parity bits when operated in high QoS mode. The data bits of the MPDU are scrambled to randomise the data stream, block encoded, and interleaved to generate the PDSU for transmission.

BCH Encoder. The BCH (63, 51) and BCH (126, 63) are used in the default mode and high QoS mode, respectively. The BCH (126, 63) is used in accordance with the Hybrid Automatic Repeat Request (HARQ), which is explained below.

Bit Interleaving. Interleaving is applied to achieve robustness against error propagation; that is, multiple consecutive bits are erroneous at the receiver side. A simple modulus interleaver with a fixed size is used.

3.3.5. PHR Construction. The 24 PHR data fields shown in Figure 11 are appended with 4-bit CRC-4 ITU error detection before being encoded using BCH (40, 28) and are finally fed to the PPDU frame.

Data Rate (R_0 – R_2). These three bits specify the data rate, the symbol duration, the BCH coding rate, and other modulation-related parameters. In the case of IR-UWB, five sets of parameters are defined in the case of on-off modulation, and eight sets are defined when any of the

supported differential modulation schemes is used. In the case of FM-UWB, a single datum is defined by setting the three bits to zero, and the other options are reserved.

Pulse Shape (W_0 – W_1). UWB PHY supports three pulse shapes: chirp pulse, chaotic pulse, and short pulse shapes. The last option, that is, $W_0 = W_1 = 1$, is reserved.

Hybrid Automatic Repeat Request ($H_0 - H_1$). HARQ is used to permit the repetition of the transmission of certain packets in case an error occurs during the transmission. In UWB PHY, the maximum number of retransmissions is set to four. In the default mode, the BCH parity bits are appended to the MPDU to form the PSDU without requiring the HARQ technique. In the high QoS mode, the transmitter encodes the systematic data D (the MAC header and MAC frame body) to obtain the parity sequence P of the same size. Both sequences are saved at the transmitter. First, D is appended with its FCS to form the transmitted PSDU. If an error occurs and thus no ACK is received, P is appended with its FCS and transmitted. At the receiver, both D and P are used to recover the original data using BCH decoding. This process is repeated until either a successful decoding is achieved or the maximum number of retransmissions is exceeded. In this algorithm, $(H_0, H_1) = (0, 0)$, $(1, 0)$, $(0, 1)$, and $(1, 1)$ indicates that HARQ is disabled (default mode). BCH encoding is applied to D and P, and the algorithm sends D, D, and P.

Scrambler Seed (SS). This bit selects the initial state of the registers of the scrambler among the two available initial states.

Constellation Mapper for On-Off Modulation. The $K_m = 0$ and 1 refer to 16-ary (optional) and 2-ary (mandatory) waveform coding, respectively.

3.3.6. Synchronisation Header. The SHR consists of the preamble, which is used for timing synchronisation, packet detection, and carrier frequency offset recovery, and the start-of-frame delimiter (SFD), which is used for frame synchronisation.

Preamble. The preamble is a Kasami sequence of length 63, where eight sequences are available. The first four sequences are used for physical channels with an odd number, and the last four sequences are used for physical channels with an even number. The coordinator uses the preamble sequence with the minimum receiver power.

Start-of-Frame Delimiter. The SFD is the inversion of the Kasami sequence used ($0 \rightarrow 1$ and $1 \rightarrow 0$.) This choice leads to a minimised correlation between the SFD and preamble such that the detection of the SFD becomes more accurate.

4. IEEE 802.15.6 Security Specifications

The IEEE 802.15.6 supports three security levels with different security properties, protection levels, and frame formats.

Unsecured Communication Level. This level is the lowest level of security, where data are transmitted in unsecured frames. This level has no mechanisms for data authentication and integrity, confidentiality, or privacy protection.

Authentication Level. This level is the medium level of security, where data are transmitted in secured authentication with no encryption. This level does not support confidentiality or privacy.

Authentication and Encryption. This level is the highest level of security, where data are transmitted in authenticated and encrypted frames. This level provides solutions to all problems that are not covered by the lowest and medium security levels.

One of the security levels above is selected during the association process. A Master Key (MK) is activated for unicast secured communication. The MK may be preshared or established using unauthenticated association. Then, a Pairwise Temporal Key (PTK) is created for a single session. For multicast secured communication, a Group Temporal Key (GTK) is shared with the corresponding group using the unicast method. Figure 12 illustrates the process of activating MK and establishing PK for secured communication.

4.1. Security Association and Disassociation Procedure. IEEE 802.15.6 security protocols are generally based on the Diffie-Hellman key exchange, which employs the elliptic curve public key cryptography. The private keys used in the association and disassociation processes should be independent and unique 256-bit integers. The Cipher-based Message Authentication Code (CMAC) is used to derive the Key Message Authentication Codes (KMAC) and MK [22–24]. Initially, the node and hub have a preshared MK, which is used for the security association procedure. The node initiates the process by sending a security association frame request to the hub, as illustrated in Figure 13(a). The hub responds by either joining or aborting the association procedure. If the node receives a respond indicating an abortion, it stops the current association procedure. If the node receives a joining response, the preshared MK is activated and shared between the node and hub upon mutual agreement, which is then used to generate a PTK.

The disassociation procedure can be initiated either by the node or hub. As illustrated in Figure 13(b), the sender sends a security disassociation frame request and eventually removes the MK and corresponding PTK from its storage. When the recipient receives the request, it also removes the aforementioned key information from its storage.

4.2. PTK and GTK Procedures. After the MK is shared using the association procedure above, the node or hub steps towards generating a PTK. The node (or hub) sends a PTK frame request to the hub (or node). The recipient responds by either joining or aborting the procedure using the PTK field in the frame payload. The sender stops the procedure if a negative response is received; otherwise, it continues to send PTK frame requests to the recipient. The second PTK request is sent only after the successful verification of the PTK field in the frame payload. Once the second PTK request is received, the sender and recipient generate a new PTK.

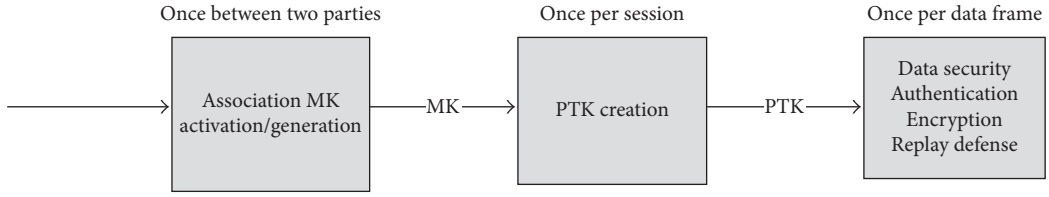
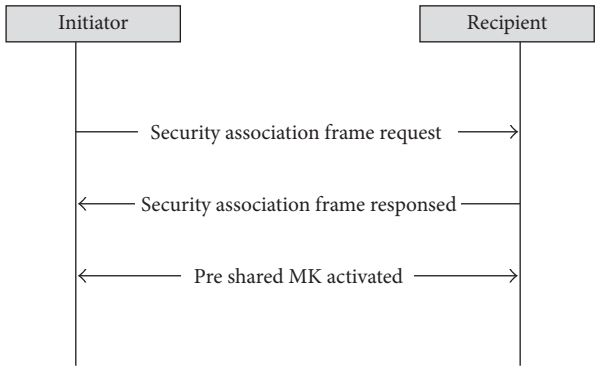
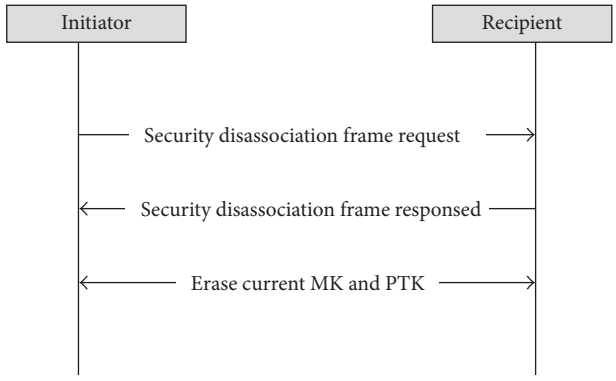


Figure 12: IEEE 802.15.6 security structure.



(a) Security association procedure of IEEE 802.15.6



(b) Security disassociation procedure of IEEE 802.15.6

Figure 13: Security association and disassociating procedures of IEEE 802.15.6.

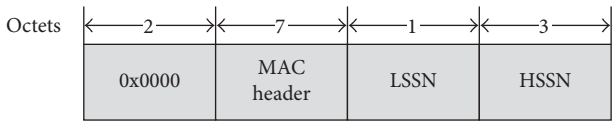


Figure 14: IEEE 802.15.6 nonce format.

The GTK is distributed among the nodes using the PTK. The hub sends a GTK to the node to multicast secured frames to other nodes.

4.3. Message Security. The frames can be transmitted in both secured and unsecured communication modes. The nodes that do not require security receive all frames including beacons without validating the security information. The secured frames are authenticated and encrypted or decrypted using the AES-128 Counter (CCM) [25–27] mode. As illustrated in Figure 14, a 13-octet nonce is required for each instance of CCM frame authentication and encryption or decryption.

The Low-order Security Sequence Number (LSSN) is set to zero if the frame is secured with a new PTK or GTK and is incremented by one if the frame is a retransmission of the last frame. The High-order Security Sequence Number (HSSN) is set to zero if the frame is secured with a PTK. The HSSN is incremented by one if the security sequence number of the current frame is less than that of the last frame.

5. Conclusions

This paper presented the most important features of the IEEE 802.15.6 standard. A deep explanation of MAC, PHY, and security specifications of the standard was presented. Different communication modes and access mechanisms were explained. The NB, HBC, and UWB PHY specifications were reviewed in terms of frame structure, modulation, and other key parameters. In addition, the security services, including key generation and message security, were discussed. We believe that this paper could be used to quickly understand the key features of the standard and to analyse its potential for different applications.

Abbreviations

MAC:	Medium Access Control
PHY:	Physical layers
NB:	Narrowband PHY
UWB:	Ultra-wideband PHY
HBC:	Human Body Communications
WBANs:	Wireless Body Area Networks
CE:	Consumer Electronics
MICS:	Medical Implant Communications Service
WMTS:	Wireless Medical Telemetry Services
ISM:	Industrial, Scientific, and Medical
FCS:	Frame Check Sequence
ID:	Identification
MIC:	Message Integrity Code
EAP:	Exclusive Access Phases
RAP:	Random Access Phases
MAP:	Managed Access Phase
CAP:	Contention Access Phase
CSMA/CA:	Carrier Sensor Multiple Access/Collision Avoidance
Ups:	User Priorities
CP:	Collision Probability

NACK: No Acknowledgement
ACK: Acknowledgement
DPSK: Differential Phase Shift Keying
GMSK: Gaussian Minimum Shift Keying
PPDU: Physical-layer Protocol Data Unit
PSDU: Physical-layer Service Data Unit
PLCP: Physical-layer Convergence Protocol
CRC-4: 4-bit Cyclic Redundancy Check
HCS: Header Check Sequence
SRRC: Square-root Raised Cosine
EFC: Electric Field Communication
FSC: Frequency Shift Code
SF: Spreading Factor
IR-UWB: Impulse Radio UWB
FM-UWB: Frequency Modulation UWB
QoS: Quality of Service
DBPSK: Differential-BPSK
DQPSK: Differential-QPSK
CP-BFSK: Continuous Phase Binary FSK
SHR: Synchronization Header
MPDU: MAC Protocol Data Unit
HARQ: Hybrid automatic repeat request
SS: Scrambler seed
SFD: Start-of-frame Delimiter
MK: Master Key
PTK: Pairwise Temporal Key
GTK: Group Temporal Key
KMAC: Key Message Authentication Codes
CCM: AES-128 Counter
LSSN: Low-order Security Sequence Number
HSSN: High-order Security Sequence Number.

Authors' Contribution

All of the authors contributed equally to this paper.

Acknowledgment

This work is supported by the Research Center of College of Computer and Information Sciences, King Saud University. The authors are grateful for this support.

References

[1] S. Ullah, H. Higgins, B. Braem et al., "A comprehensive survey of wireless body area networks—on PHY, MAC, and network layers solutions," *Journal of Medical Systems*, vol. 36, no. 3, pp. 1065–1094, 2012.

[2] M. Chen, "Body area networks: a survey," *Mobile Networks and Applications*, vol. 16, no. 2, pp. 171–193, 2011.

[3] B. Latré, B. Braem, I. Moerman, C. Blondia, and P. Demeester, "A survey on wireless body area networks," *Wireless Networks*, vol. 17, no. 1, pp. 1–18, 2011.

[4] 2012, http://www.ieee802.org/15/pub/TG6.html.

[5] T. Baykas, C. S. Sum, Z. Lan et al., "IEEE 802.15.3c: the first IEEE wireless standard for data rates over 1 Gb/s," *IEEE Communications Magazine*, vol. 49, no. 7, pp. 114–121, 2011.

[6] E. Karapistoli, F. N. Pavlidou, I. Gragopoulos, and I. Tsetsinas, "An overview of the IEEE 802.15.4a standard," *IEEE Communications Magazine*, vol. 48, no. 1, pp. 47–53, 2010.

[7] R. Lampe, R. Hach, and L. Menzer, "Chirp spread spectrum (CSS) PHY presentation for 802. 15. 4a, IEEE P802. 15," Working Group for Wireless Personal Area Networks (WPAN), 2004.

[8] J. A. Gutierrez, M. Naeve, E. Callaway, M. Bourgeois, V. Mitter, and B. Heile, "IEEE 802.15.4: a developing standard for low-power low-cost wireless personal area networks," *IEEE Network*, vol. 15, no. 5, pp. 12–19, 2001.

[9] IEEE WLAN, 2012, http://www.ieee802.org/11/.

[10] IEEE WPAN Task Group 1, 2012, http://www.ieee802.org/15/pub/TG1.html.

[11] *IEEE Std. 802. 15. 4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Data Rate Wireless Personal Area Networks (WPAN)*, IEEE, Piscataway, NJ, USA, 2006.

[12] "IEEE P802. 15. 6, Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs) used in or around a body," 2012.

[13] M. Hernandez and R. Miura, "Coexistence of IEEE Std 802. 15. 6TM-2012 UWB-PHY with other UWB systems," in *Proceedings of the IEEE International Conference on Ultra-Wideband (ICUWB)*, pp. 46–50, September 2012.

[14] A. W. Astrin, H. B. Li, and R. Kohno, "Standardization for body area networks," *IEICE Transactions on Communications*, vol. 92, no. 2, pp. 366–372, 2009.

[15] H. B. Li, K. Takizawa, and R. Kohno, "Trends and standardization of body area network (BAN) for medical healthcare," in *Proceedings of the 1st European Wireless Technology Conference (EuWiT' 08)*, pp. 1–4, Amsterdam, The Netherlands, October 2008.

[16] S. Rashwand, J. Mišić, and H. Khazaei, "IEEE 802.15.6 under saturation: some problems to be expected," *Journal of Communications and Networks*, vol. 13, no. 2, pp. 142–148, 2011.

[17] S. Rashwand and J. V. Misic, "Effects of access phases lengths on performance of IEEE 802. 15. 6 CSMA/CA," *Computer Networks*, vol. 56, no. 12, pp. 2832–2846, 2012.

[18] S. Rashwand and J. Mišić, "Performance evaluation of IEEE 802.15.6 under non-saturation condition," in *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM' 11)*, pp. 1–6, Houston, Tex, USA, December 2011.

[19] S. Ullah and K. S. Kwak, "Throughput and delay limits of IEEE 802.15.6," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC' 11)*, pp. 174–178, Cancun, Mexico, March 2011.

[20] S. Ullah, M. Chen, and K. S. Kwak, "Throughput and delay analysis of IEEE 802. 15. 6-based CSMA/CA protocol," *Journal of Medical System*, vol. 36, no. 6, pp. 3875–3891, 2012.

[21] K. S. Kwak, S. Ullah, and N. Ullah, "An overview of IEEE 802.15.6 standard," in *Proceedings of the 3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL' 10)*, pp. 1–6, Rome, Italy, November 2010.

[22] NIST Special Publication 800-38B, 2005.

[23] H. E. Michail, A. P. Kakarountas, G. Selimis, and C. E. Goutis, "Throughput optimization of the cipher message authentication code," in *Proceedings of the15th International Conference on Digital Signal Processing (DSP' 07)*, pp. 495–498, Cardiff, UK, July 2007.

[24] A. A. Adekunle and S. R. Woodhead, "Zone based systems design framework for the realisation of efficient block cipher

based message authentication code algorithms," in *Proceedings of the 5th International Conference on Availability, Reliability, and Security (ARES' 10)*, pp. 216–221, Krakow, Poland, February 2010.

[25] A. Astarloa, A. Zuloaga, J. Lázaro, J. Jiménez, and C. Cuadrado, "Scalable 128-bit AES-CM crypto-core reconfigurable implementation for secure communications," in *Proceedings of the Applied Electronics International Conference (AE' 09)*, pp. 37–42, Pilsen, Czech Republic, September 2009.

[26] M. K. Khan and J. Zhang, "Improving the security of 'a flexible biometrics remote user authentication scheme'," *Computer Standards and Interfaces*, vol. 29, no. 1, pp. 82–85, 2007.

[27] NIST Special Publication 800-38C, 2004.