Analysis and comparison of the IEEE 802.15.4 and 802.15.6 wireless standards based on MAC layer

Renwei Huang, Zedong Nie*, Changjiang Duan, Yuhang Liu, Liya Jia, and Lei Wang

Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences
Shenzhen, China

zd.nie@siat.ac.cn

Abstract.IEEE 802.15.4 and IEEE 802.15.6 are two kinds of wireless area network standards for short range communication applications. IEEE 802.15.4 is proposed for Wireless Person Area Network (WPAN) that provides low data rate, low power, and low cost applications in a short range. Meanwhile, IEEE 802.15.6 is the first international Wireless Body Area Network (WBAN) standard, which distributes nodes on or inside a human body, also operates in low power and short range, mainly provides real-time monitoring and human physiological data to judge the human physiological condition. In view of many similarities in both two standards, we analyzed the two standards mainly from the MAC frame format, MAC access mechanisms in this paper. In addition, some discussions of the differences of applications in the two standards were illustrated.

Keywords: WBAN ·MAC ·IEEE 802.15.4 ·IEEE 802.15.6

1 Introduction

Nowadays, with the advancement of microelectronics technology, it becomes one of the most leading force to improve human existence and lifestyle through combing computer technology and communication technology. In this instance, the Wireless Sensor Networks (WSNs) with short distance, strong mobility, and high transmission rate is becoming more and more necessary and popular.

A WSN is composed of a large number of sensor nodes, and these nodes communicate with each other by self-organization and multi-hop [1]. A WSN is mainly used for monitoring physical or environmental conditions, such as temperature, sound, pressure, and to cooperatively pass their data through the network to a main location [2]. Earlier, several wireless communication standards have been formulated [3], such as the IEEE 802.11 [4], IEEE 802.15.1 [5], IEEE 802.15.4 [6] standards. However, these standards are not suitable for WBAN applications. The power consumption of 802.11 Wireless Local Area Network (WLAN) is too high to satisfy the wear WBAN requirements with a low power. In addition, the number of auxiliary nodes in IEEE 802.15.1 are limited. IEEE 802.15.4 is widely used in industrial sensors, smart grids and other areas of IOT (Internet of Things) [7], but it is not enough

adfa, p. 1, 2011.

to support high data rate applications (data rate > 250 Kbps). In order to develop a low power consumption communication standard which is suitable for WBAN application [8], IEEE 802 established a task group for the standardization of WBAN called IEEE 802.15.6 in November 2007 [9]. WBAN is centered on the human body, which is composed of network elements (including personal terminal, independent nodes that are situated in the clothes, on the body or under the skin of a person, and communication equipment near human body within 3~5m) and so on [10]. WBANs provide unconstrained freedom of movement for patients suffering from chronic diseases, such as diabetes, heart disease [11]. The advantage is that a patient doesn't have to stay in bed, but can move everywhere freely, which improves the quality of life for patients and reduces hospital costs. In February 2012, the first version of IEEE 802.15.6-2012 was published.

IEEE 802.15.6 is a standard for short-range, wireless communications in the vicinity of, or inside, a human body (but not limited to humans) [9]. It defines a Medium Access Control (MAC) layer that works at lower sublayer of the data link layer of the OSI (Open System Interconnection) model [12], and offers unicast, multicast, or broadcast communication service. Unfortunately, more protocol details are hidden in current version of IEEE 802.15.6 standard, it is a better way to design a new WBAN system based on IEEE 802.15.4 standard, which is a mature protocol and has been applied in many fields. So far many research groups have studied the key issues of IEEE 802.15.4 and IEEE 802.15.6, the IEEE 802.15.6 MAC, PHY (Physical Layer), and security specifications were reviewed in [3]; the IEEE 802.15.4 security framework for WBAN was analyzed in [13]; the 802.15.4 MAC protocols for WBANs was introduced in [14]. However, few study was conducted to compare the similarities and differences between IEEE 802.15.4 and IEEE 802.15.6.

Analyzing and comparing 802.15.6 with 802.15.4 would help developers choose the better communication protocol to design new application systems and propose some approaches to optimize the 802.15.6 standard. In order to introduce the differences between the two standards, we discussed the MAC sublayer starting from the MAC format and access mechanisms, because the MAC sublayer plays an important role in providing guarantee for the reliable communication between SSCS (Service-Specific Convergence Sublayer) and PHY. The MAC sublayer concludes the MAC frame format, access mechanism and security services. The MAC frame format is used to indicate the frame types with different functions. The MAC access mechanism provides guarantee for the reliable communication. The security services make sure information safety. The MAC frame format and access mechanisms occupy an important position in the MAC sublayer, so we analyzed the two standards mainly from the MAC frame format, MAC access mechanisms in this paper.

The rest of the paper was organized into five sections. Section 2 presented the differences of the MAC frame format in the two standards. Section 3 introduced the different MAC access mechanisms between the two standards. A discussion of the differences of applications in the two standards was illustrated in section 4. The final section concluded our work.

2 Mac frame format of the two standards

A MAC frame is a sequence of fields in a specific order. The MAC frame format is composed of a MAC Header, a MAC Payload, and FCS both in IEEE 802.15.4 and IEEE 802.15.6. As depicted in Table 1.

Table 1. General MAC frame format

Octets: variable	variable	2
MAC Header	MAC Payload	FCS

If a device wants to transmit data to other devices in IEEE 802.15.4, it should contains a MAC Header with at least 9 octets length which is longer than those with 7 octets length in IEEE 802.15.6. These may result in many difficulties during the frames transmission and reception, such as increasing the burden of transceivers. In addition, the data rate will decrease and the transmission power will increase.

2.1 Frame Control field

Besides the intuitionistic difference of the length of MAC Header, there are many similarities and differences between the two frame control fields, as described in Table 2 and Table 3.

Table 2. Format of the Frame Control field in IEEE 802.15.4

Bits:0-2	3	4	5	6	7-9	10-11	12-13	14-15
Frame Type	Security Enabled	Frame Pending	ACK Request	PAN ID Compression	Reserved	Destination Addressing Mode	Frame Version	Source Addressing Mode

Table 3. Frame Control format of IEEE 802.15.6

Bits:1	2	2	1	1	1	4	2	1	1	8	3	1	4
Bit order:b0	b1-b2	b3-b4	b5	b6	b7	b0-b3	b4-b5	b6	b7	b0-b7	b0-b2	b3	b4-b7
Protocol Version	ACK Policy	Security Level	TK Index	BAN Security /Relay	ACK Timing/ EAP Indicator /First Frame On Time	Frame Subtype	Frame Type	More Data	Last Frame/ Access Mode/ B2	Sequence Number /Poll-Post Window	Fragment Number /Next /Coexistence	Non-final Fragment /Cancel/Scale /Inactive	Reserved

The Frame Type subfield of IEEE 802.15.4 is 3 bits in length and shall be set to one of the non-reserved values. 0b000, 0b001, 0b010, 0b011 respectively denote the beacon frame, data frame, response frame, MAC command frame, other values were reserved. The IEEE 802.15.6 describe the Frame Type by using not only Frame Type subfield but also Frame Subtype subfield. 0b00,0b01,0b10 of the Frame Type subfield represent management frame, control frame and data frame respectively, 0b11 is reserved. On the other hand, the Frame Subtype subfield refines the frame type with 4 bits data, which is helpful to classify different frames. For example, if a frame field carries security association information, it must be a management frame not a MAC command frame. In other words, a combination of Frame Type subfield and Frame Subtype subfield is more efficient than an independent use of Frame Type subfield. In addition, the IEEE 802.15.6 defines an UP (User Priority) to decrease collision possibility.

2.2 MAC Frame body

In IEEE 802.15.4, the Frame Payload field has a variable length and contains information specific to individual frame types. The PHR (PHY header) frame length field identifies the length of the MAC frame, it is a byte long and the MSB of the PHR frame length field is not valid, so the length of the MAC frame can't exceed 127 bytes, which is not suitable to use the RTS/CTS mechanism. Nor is IEEE 802.15.6 with a variable length from 0 to 255 bytes of MAC Frame body. Because a RTS package with 20 bytes in length could account for about 20% of the MAC Frame body in IEEE 802.15.4 and 10% of those in IEEE 802.15.6 respectively, which lead to extra energy consumption, meanwhile, the RTS/CTS mechanism couldn't effectively restrain hidden conflicts [15]. In IEEE 802.15.6, when MAC Frame body has a non-zero length, it contains 1-bit Low-Order Security Sequence Number, a variable length of Frame Payload (Do not exceed pMaxFrameBodyLength) and 4-bit MIC (Message Integrity Code). The Low-Order Security Sequence Number field carries message freshness information required for nonce construction and relay detection. In addition, the last 32-bit MIC (Message Integrity Code) carries information about the authenticity and integrity of the current frame.

3 MAC Access Mechanism

As shown in in Figure 1, the IEEE 802.15.4 communication mode is represented.

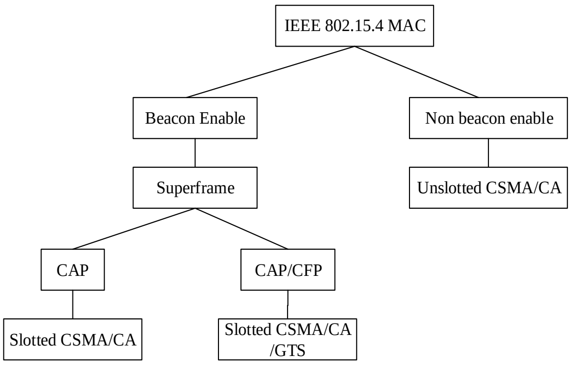

Fig. 1. IEEE 802.15.4 communication mode

In IEEE 802.15.4, the beacon-enabled with superframe uses a slotted ALOHA or slotted CSMA/CA in CAP and GTSs in CFP to exchange information between the coordinator and devices. In addition, unslotted CSMA/CA mechanism is used by non-beacon without superframe.

Similarly, the IEEE 802.15.6 also employ the slotted ALOHA and CSMA/CA mechanism, what's more, there are two other protocols named improvised and unscheduled access mechanism and scheduled and scheduled-polling access mechanisms.

3.1 Random Access Mechanism

In EAP, RAP, and CAP periods of beacon mode with superframe boundaries of IEEE 802.15.6, as shown in Figure 2, the hub may employ either a slotted ALOHA or CSMA/CA protocol, depending on the PHY. To send data type frames of the highest UPs (User Priorities) based on CSMA/CA, a hub or a node may combine EAP1 and RAP1 as a single EAP1 and EAP2 and RAP2 as a single EAP2, so as to allow continual invocation of CSMA/CA and improve channel utilization. When using slotted ALOHA for high-priority traffic, RAP1 and RAP2 are replaced by another EAP1 and EAP2 respectively but not a continuation EAP1 and EAP2, due to the time slotted attribute of slotted ALOHA access.

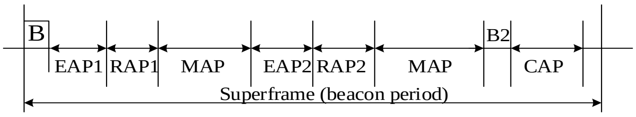

Fig. 2. Beacon mode with superframe boundaries in IEEE 802.15.6

In a slotted ALOHA protocol, the nodes access the channel using predefined UPs, as given in Table 4.

Table 4. Bounds for slotted-ALOHA and CSMA/CA protocols

User	Slotted –ALOHA		CSMA/CA	
Priorities	CP_{max}	CP_{min}	CW_{max}	CW_{min}
0	1/8	1/16	64	16
1	1/8	3/32	32	16
2	1/4	3/32	32	8
3	1/4	1/8	16	8
4	3/8	1/8	16	4
5	3/8	3/16	8	4
6	1/2	3/16	8	2
7	1	1/4	4	1

Initially, the CP (Collision Probability) is selected according to the UPs. If Z≤CP, where Z is equal to a random number in the interval [0-1], the node obtains a contended allocation in the current ALOHA slot, during which data frames transmission occur. When the transmission is fail, the CP remains the same if the number of failures are odd or be cut in half if the number of failures are even.

The IEEE 802.15.4 protocol defines two versions of the CSMA/CA mechanism: slotted CSMA/CA mechanism for beacon mode with superframe and unslotted CSMA/CA mechanism for non-beacon network. In both cases, the algorithm is implemented using units of time called backoff periods, which is equal to aUnitBackoff-Period symbols. The CSMA/CA algorithm is controlled by three variables: NB (Number of Backoffs), CW (Content Window) and BE (Back off Exponent). Where NB is initialized to zero and the maximum value is 4. CW is decreased using units of backoff, the default value is 2 and the maximum is 31. BE is related to how many backoff periods a device shall wait before attempting to assess the channel and the scope of BE is 0~5, the default value is 3. The whole CSMA-CA algorithm is illustrated in Figure 3.

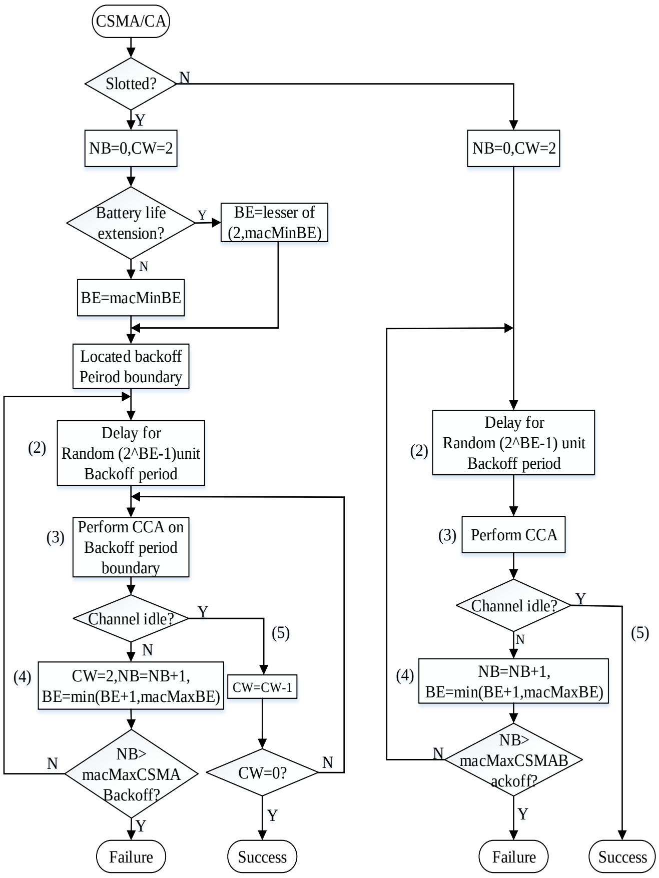
CSMA/CA
Slotted?
N
Y
NB=0,CW=2
NB=0,CW=2
Battery life extension?
Y
BE=lesser of (2,macMinBE)
N
BE=macMinBE
Located backoff Peirod boundary
(2)
Delay for Random (2^BE-1)unit Backoff period
(2)
Delay for Random (2^BE-1) unit Backoff period
(3)
Perform CCA on Backoff period boundary
(3)
Perform CCA
Channel idle?
Y
(5)
N
Channel idle?
Y
(5)
N
(4)
CW=2,NB=NB+1, BE=min(BE+1,macMaxBE)
CW=CW-1
(4)
NB=NB+1, BE=min(BE+1,macMaxBE)
N
NB> macMaxCSMA Backoff?
CW=0?
N
N
NB> macMaxCSMAB ackoff?
Y
Y
Y
Failure
Success
Failure
Success

Fig. 3. The CSMA/CA algorithm in IEEE 802.15.4

In IEEE 802.15.6, the node initially sets BC (Backoff Counter) to a random inter that is uniformly distributed over the interval [1, CW], where CW Є (CW_{min},CW_{max}). As shown in Table IV, the values of CW_{min} and CW_{max} are selected according to the UPs. Before implementing the CSMA/CA algorithm, the CSMA slot boundary and pSIFS should be located, which each idle CSMA slot is equal to pCSMASlotLength and the default value of pSIFS is 75 μs. The m is the times of the node had failed consecutively. It is important to note that if double of the CW exceeds the CW_{max}, then the CW is CW_{max}. Figure 4 shows an example of the CSMA/CA algorithm.

Comparing the two CSMA/CA protocols in IEEE 802.15.4 and IEEE 802.15.6, it is found that there are some similarities and differences between them. First of all, since they are both CSMA/CA, so the node needs to detect the channel by using CCA (Clear Channel Access) before transmitting frames. CW is both used to implement backoff algorithm which is not the same in using. In IEEE 802.15.4, BE is related to how many backoff periods a device shall wait before attempting to assess the channel and the BEth backoff is randomly chosen from {0,1,…, 2^{BE}-1}, this is done to reduce the probability of the same backoff period for different nodes. However, owing to the less nodes, the shorter distance, the faster rate, the IEEE 802.15.6 defines UPs to decrease collision possibility. Different UPs mean different CW and BC, additionally, smaller CW and BC lead to low latency and higher channel utilization. All these designs are adopt to IEEE 802.15.6 network topology.

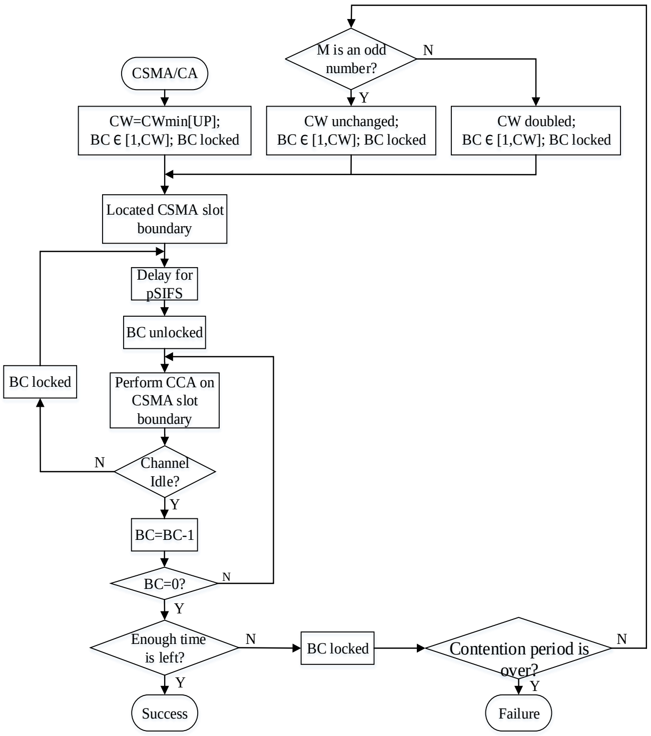

Fig. 4. The CSMA/CA algorithm in IEEE 802.15.6

3.2 Improvised and Unscheduled Access Mechanism

Besides the slotted ALOHA protocol and the CSMA/CA mechanism both in IEEE 802.15.4 and IEEE 802.15.6, there are another two access mechanisms in IEEE 802.15.6. The hub may use improvised access to send poll or post commands without advance reservation in beacon or non-beacon modes with superframe boundaries. Figure 5 illustrates an example of immediate polled allocations.

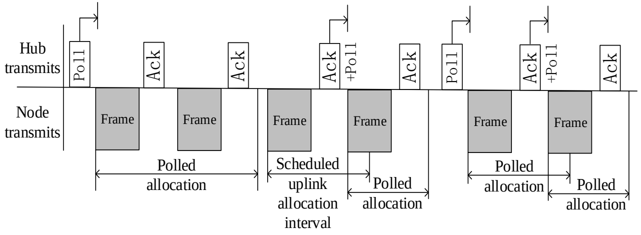

Fig. 5. Immediate polled allocations

The hub may also use an unscheduled access mechanism to obtain an unscheduled bilink allocation to apply for some specific condition, such as emergency communication service. In beacon or non-beacon modes with superframe, unscheduled bilink allocations may be 1-periodic, where frames transmission every superframe, or m-periodic, where frames transmission every m superframes. An m-periodic bilink allocation is helpful to reducing power consumption because nodes could sleep in m-periodic allocation.

3.3 Scheduled and Scheduled-Polling Access Mechanism

Unlike unscheduled allocation, a node and a hub may employ scheduled access to obtain scheduled uplink, downlink, and bilink allocations. In addition, the scheduled polling is used for polled and posted allocations. These allocations may be 1-periodic or m-periodic, but not the both in the same BAN. Figure 6 illustrates an example of scheduled 1-periodic allocations.

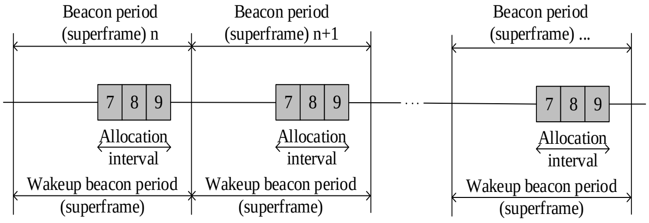
Beacon period (superframe) n
Beacon period (superframe) n+1
Beacon period (superframe) ...
7 8 9
7 8 9
7 8 9
Allocation interval
Allocation interval
Allocation interval
Wakeup beacon period (superframe)
Wakeup beacon period (superframe)
Wakeup beacon period (superframe)

Fig. 6. Scheduled one-periodic allocation

4 A discussion of differences of applications

The standards are described differ by which frequencies they used and the data rate and range they covered. According to Table 5, 802.15.6 (BAN) has a much shorter range than 802.15.4, which proves to be an advantage. Shorter range communication means lower power requirements. In addition, due to the short distance in the vicinity of, or inside, a human body only, it's more secure than 802.15.4. The lower consumption of the IEEE 802.15.6 not only comes from the sleep mode as same as IEEE 802.15.4, but also the shorter distance and less interference. In addition, it enables equipment to be smaller and frequency reuse to be better. The data rate of 802.15.6 is up to 15.6 Mbps, which is much faster than 802.15.4 with a max data rate 250 kbps [16]. All of these are good for BAN since the design of original intention is to make it unobtrusive, you can put it in the clothes, attach or implant into the human body, such as wearable devices.

Table 5. Comparison of the two wireless standards

Standard Project	802.15.4	802.15.6
MAC frame type	beacon frame, data frame response frame and command frame	management frame, control frame and data frame
MAC access mechanism	Slotted CSMA/CA Unslotted CSMA/CA	CSMA/CA mechanism Improvised and unscheduled access mechanism Scheduled and scheduled-polling access mechanism
Data Rate (Max)	20kbps,40kbps/250kbps	15.6Mbps
Transmission Range	75m	3~5m
Applications	Low data rate, industrial sensors, smart grid	Wearable devices

The major reason in increasing data rate is that the transmission medium is the human body, which with little interference. Coupling with new modulation techniques, making it possible that the data transfer rate of IEEE 802.15.6 is much higher than IEEE 802.15.4. In a word, IEEE 802.15.6 defines a new wireless communication technology for low power, high data rate, short range, high safety which is especially suitable for wearable device applications.

5 Conclusions

This paper presented the most significant features of comparison of MAC between IEEE 802.15.6 and IEEE 802.15.4 standard. An analysis of differences of MAC format and access mechanisms of the two standards were presented. At last, starting from the aspects of frequency, data rate and range, the superiority of 802.15.6 in BAN communication was discussed. We believed that this paper could be used to quickly understand the key feature of MAC sublayer of IEEE 802.15.4 and IEEE 802.15.6. Besides, it also helped you to develop the potential application of IEEE 802.15.6 on the basis of IEEE 802.15.4.

Acknowledgment

This study was financed partially by National Natural Science Foundation of China (Grant No.61403366), Shenzhen Basic Research Project Fund (JCYJ20140417113430695), the National 863 Program of China (Grant No. 2012AA02A604), the Next generation communication technology Major project of National S&T (Grant No. 2013ZX03005013).

References

1. A. Heragu, D. Ruffieux, and C. Enz, "The Design of Ultralow-Power MEMS-Based Radio for WSN and WBAN," in *Frequency References, Power Management for SoC, and Smart Wireless Interfaces*, ed: Springer, 2014, pp. 265-280.
2. P. Rawat, K. D. Singh, H. Chaouchi, and J. M. Bonnin, "Wireless sensor networks: a survey on recent developments and potential synergies," *The Journal of Supercomputing,* vol. 68, pp. 1-48, 2014.
3. S. Ullah, M. Mohaisen, and M. A. Alnuem, "A review of ieee 802.15. 6 mac, phy, and security specifications," *International Journal of Distributed Sensor Networks,* vol. 2013, 2013.
4. T. W. G. f. W. Standards. (2012). *IEEE WLAN*. Available: http://www.ieee802.org/11/
5. (2012). *IEEE WPAN Task Group 1*. Available: http://www.ieee802.org/15/pub/TG1.html
6. "IEEEStd.802.15.4:WirelessMediumAccessControl(MAC)and Physical Layer (PHY) Specifications for Low Data Rate Wireless," *IEEE Std 802.15.4™-2006,* 2006.
7. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems,* vol. 29, pp. 1645-1660, 2013.
8. Z. D. Nie, J. J. Ma, K. Ivanov, and L. Wang, "An investigation on dynamic human body communication channel characteristics at 45MHz in different surrounding environments," *Antennas and Wireless Propagation Letters, IEEE,* vol. PP, pp. 1-1, 2014.
9. "IEEE Standard for Local and metropolitan area networks - Part 15.6: Wireless Body Area Networks," *IEEE Std 802.15.6-2012,* pp. 1-271, 2012.
10. R. Chávez-Santiago, A. Khaleghi, I. Balasingham, and T. A. Ramstad, "Architecture of an ultra wideband wireless body area network for medical applications," in *Applied Sciences in Biomedical and Communication Technologies, 2009. ISABEL 2009. 2nd International Symposium on,* 2009, pp. 1-6.
11. T.-H. Kim and Y.-H. Kim, "Human effect exposed to UWB signal for WBAN application," *Journal of Electromagnetic Waves and Applications,* pp. 1-15, 2014.
12. M. G. Kumar and K. S. Roy, "Zigbee Based Indoor Campus Inventory Tracking Using Rfid Module."
13. S. Saleem, S. Ullah, and K. S. Kwak, "A study of IEEE 802.15. 4 security framework for wireless body area networks," *Sensors,* vol. 11, pp. 1383-1395, 2011.

14. S. Ullah, B. Shen, S. M. Islam, P. Khan, S. Saleem, and K. S. Kwak, "A study of MAC protocols for WBANs," *Sensors (Basel),* vol. 10, pp. 128-45, 2010.
15. N. Barroca, L. M. Borges, F. J. Velez, and P. Chatzimisios, "IEEE 802.15. 4 MAC layer performance enhancement by employing RTS/CTS combined with packet concatenation," in *Communications (ICC), 2014 IEEE International Conference on*, 2014, pp. 466-471.
16. Z. Nie, J. Ma, Z. Li, H. Chen, and L. Wang, "Dynamic propagation channel characterization and modeling for human body communication," *Sensors,* vol. 12, pp. 17569-17587, 2012.