Telecommun Syst manuscript No.
(will be inserted by the editor)

A Survey: Energy Exhausting Attacks in MAC Protocols in WBANs

Minho Jo · Longzhe Han · Nguyen Duy Tan · Hoh Peter In

Received: date / Accepted: date

Abstract Because the sensors of wireless body area networks (WBANs) have limited battery power, many studies have focused on energy efficient medium access control (MAC) protocols to extend the lifetime of the sensors. In addition, WBANs face energy-exhausting attacks, which force the sensors to consume battery power partially or thoroughly. These attacks occur mainly in the MAC layer and threaten severely the energy efficiency of MAC protocols in WBANs. Because the attacks are made abruptly and unexpectedly, the lives of human beings and the quality of health care services can be threatened. Therefore, the aim of this study was to identify the major types of energy exhausting attacks in MAC protocols in WBANs, and show how easily the attacks can cause energy exhaustion in different MAC protocols. This survey provides clues for future research into energy efficient MAC protocols in WBANs.

Keywords Wireless Body Area Networks · Energy Efficient Medium Access Control Protocol · Energy Exhausting Attacks

1 Introduction

WBANs utilize low-power medical sensors to monitor the human body constantly [5]. Because of the limited power, the energy efficiency mechanism is an important issue in WBANs [8, 12, 13, 39]. The main sources of energy waste are collisions, idle listening, overhearing and control packet overhead [42]. Collisions are caused by two or more sensor nodes that attempt to send data packets to a shared communication channel simultaneously. The receiver then discards the corrupted data packets, and the sender retransmits the data packets after certain back-off time. This retransmission consumes energy. In carrier sense multiple access/collision avoidance (CSMA/CA) and Code Division Multiple Access (CDMA) protocols, the sensor nodes need to listen to the communication channel to receive data packets. On the other hand, sensor nodes are required to keep listening, even though the communication channel can be idle for a long time. Overhearing is also a source of energy waste. In IEEE 802.11, every node is needed to listen to all packet transmissions from the neighboring nodes to perform carrier sensing. Each node will overhear many packets that are intended to transmit. If the network traffic load is heavy, overhearing consumes considerable energy. Control packets, such as request to send (RTS), clear to send (CTS) and acknowledgment (ACK) also result in energy wastage.

This paper was supported in part by a National Research Foundation of Korea grant funded by the Korea government (MEST) (No. 2011-0009454), and by Seoul R&BD Program (WR080951), and by Next-Generation Information Computing Development Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2012M3C4A7033345).

M. Jo · L. Han · H. P. In (✉)
Department of Computer Science and Engineering, Korea University, 1, 5-ka, Anam-dong, Sungbuk-ku, Seoul, 136-701, Korea
e-mail: hoh_in@korea.ac.kr

M. Jo
e-mail: minhojo@korea.ac.kr

L. Han
e-mail: lzhan@korea.ac.kr

N. D. Tan
Faculty of Information Technology, Hung Yen University of Technology Education, Vietnam
e-mail: duytan@utehy.edu.vn

Considerable research has been conducted on energy efficient MAC protocols to reduce the energy consumption and extend the lifetime of sensor nodes [1, 14, 22, 24, 34, 37, 40, 43]. Comprehensive summaries of energy efficient MAC protocols are also provided in [12, 13, 27, 41]. On the other hand, the energy exhausting attacks compromise the WBANs severely and reduce or end the lifetime of sensors that lead to a decrease in the quality of healthcare services, or in the worst case, threaten human life. This study examined energy consumption attacks in energy efficient MAC protocols in WBANs. Three major attacks were identified: collision, denial of sleep and selfish. Because collision is the main source of energy wastage, with the knowledge of MAC protocols, adversary nodes intentionally inject attacking packets into the WBANs to cause collisions. For a denial of sleep attack, the adversary node attempts to decrease the lifetime of the sensor nodes by preventing the sensor nodes from entering sleep mode. In selfish attacks, adversary nodes take advantage of MAC protocols to use the resources unfairly. For each attack type, the attack schemes against energy efficient MAC protocols in WBANs are examined further.

The remainder of this paper is organized as follows. Section II summarizes the existing energy efficient MAC protocols in WBANs. Section III analyzes the energy exhausting schemes for each type of attack in detail. The last section concludes this paper and suggests future work.

2 Energy Efficient MAC Protocols for WBANs

This section discusses the energy efficient MAC protocols that are important for WBANs. These protocols are classified into contention-based (called random access), scheduled-based (called contention free) and hybrid MAC protocols. Normally, the MAC protocols use sleep and wakeup mechanisms to save energy. In the following sections, sleep and wakeup mechanisms are first introduced and each type of MAC protocol is presented with examples.

2.1 Sleep and Wakeup Mechanisms

Sleep and wakeup mechanisms are used widely in MAC protocols to save energy. MAC protocols have a scheduled listen and sleep cycle for each transmitter and receiver to save the high-energy resource of sensor nodes, avoid collision, reduce the idle listening and achieve high throughput. Sleep and wakeup mechanisms can be classified into synchronous and asynchronous approaches.

In the synchronous approach, the nodes keep a synchronized time for wake-up schedules with their neighboring nodes. Energy consumption is reduced by simultaneously waking up and listening to the channel, such as the Timeout-MAC (T-MAC) [7] protocol. The nodes interchange synchronous RTS/CTS/SYNC packets periodically to synchronize the wake-up schedule and support both collision avoidance and reliable transmission. Wireless sensor MAC (WiseMAC) [9] utilizes a preamble sampling technique to synchronize the wake-up schedule between the access point and nodes in WBANs. In each period, the receiver nodes wake up regularly to check the channel in a short duration. If the channel is busy, the node will receive data packets and send an acknowledgement packet to the sender node. Otherwise, the receiver nodes enter sleep mode until the next sampling period. The access point updates the sampling schedule of all sensor nodes periodically, which contain the wake up and sleep interval times of each node. The access point will transmit data packets to the node after the node wakes up and receives preamble sampling to guarantee that the data packets arrive as soon as the node is awake. Therefore, the nodes consume very low battery power when the channel is idle.

In the asynchronous approach, the nodes do not wake up at the same time. The probability sensor MAC (PS-MAC) [6] protocol is one of the most well-known mechanisms. Each node generates a pseudo random number and a pre-wakeup probability. A pseudo-random number and pre-wakeup probability will be exchanged with its neighbor nodes to obtain the neighboring nodes schedule, which is called a pre-wakeup schedule. Subsequently, the nodes determine the actual listen and sleep schedule based on the pre-wakeup schedules, which is the interval time for a listen or sleep period. Therefore, the nodes reduce the unnecessary waste of energy for idle listening. A high efficient sensor MAC (HES-MAC) [28] protocol also uses the duty cycle, as in previous schemes, but the duty cycle is asynchronous with the others. The asynchronous scheduled MAC (AS-MAC) [16] protocol allows the nodes in the WBANs to exchange a Hello packet, which contains its asynchronous periodic listening and sleep interval time. The sender node will not wake up at its wakeup time if it does not have the data packet to send. Otherwise, if the node has a data packet to send, it will wait until it falls in the wakeup period. The receiver nodes wake up for a short interval to check periodically the available channel without receiving a signal. If the channel is idle, the receiver nodes will go into sleep mode. On the other hand, if the channel is busy, the receiver nodes remain

in the channel and receive the data packets. This technique is called a low power listening.

The pattern MAC (PMAC) [45] protocol introduces the concept of sleep and wakeup patterns for all nodes. In PMAC, a string of bits (slot time) indicates the sleep or wakeup period for a sensor node. If the string is bit 1, the node will remain in the wakeup period, otherwise the node is in sleep period. For example, if the string of nodes is "001", the node will sleep for two consecutive slot times, and then switch to wake up in the third slot times. The adaptive energy efficient MAC (AEEMAC) [2] and traffic aware energy efficient MAC (TEEM-MAC) [36] protocols also use sleep and wakeup mechanisms with a long sleep period to reduce idle listening and avoid collisions by using the RTS/CTS combining 'SYNC-RTS/ACK-RTS' control packets. The 'SYN-RTS' packet is a single message, which contains information on ACK and RTS control packets. The node will send the 'SYN-RTS' packet to the other node to announce to its neighbor nodes that it associates synchronization and communication with the node, which is indicated in the 'SYN-RTS' packet.

2.2 Contention-based MAC Protocols

Contention-based (called random access) MAC protocols have rules for nodes to control the channel access for solving the contention and avoiding collisions. The channel contention phenomenon occurs when many nodes attempt to access simultaneously a channel in the WBANs to transmit data packets. Contention-based MAC protocols allow nodes in WBANs to access and share the same radio channel without requiring coordination among nodes. In the IEEE 802.11 standard [11], the frame priority is defined by the different inter frame spaces. When a node wants to transmit data packets, it waits until the channel is idle for a distributed coordination function interframe space (DIFS) time before sending a RTS message. DIFS is the lowest priority time interval for asynchronous transmission services. This is because the DIFS has the longest inter frame space [11]. The sender node is only allowed to transmit its data packets when it receives a valid CTS message from the destination node. If the node receives the data packet accurately, it will send an acknowledgement packet to the sender node. The sender and receiver will go periodically into a listening and sleep mode after they have finished sending and receiving their data packets.

In CSMA/CA, called "listen before transmission", the node must listen to the channel before sending a data packet. If the channel is in an idle state, that node can transmit a packet. Otherwise, it must wait for a random time before it can try again to avoid collision. Many protocols use the contention-based mechanism, such as An energy efficient and low latency MAC (DMAC) [21] and Sensor-MAC (S-MAC) [43]. S-MAC utilizes low-duty-cycle mode for all nodes, which indicates a fixed interval time for the transmitted and received packets. In the low-duty-cycle mode, each node goes periodically to sleep to reduce idle listening. A complete duty cycle has a frame structure that includes two parts: a wake-up period and a sleep period. In the wake-up period, the nodes can transmit data packets to their neighbors. In the sleep period, the nodes reduce the idle listening time by regularly turning off their radio. If the nodes have data to send during the sleep period, they must delay transmission until the next wake up period. Energy-efficient and high throughput MAC (ET-MAC) [1], Berkeley MAC (B-MAC) [26] and Timeout-MAC (T-MAC) [7] protocols are designed not only to avoid collision with a clear channel assessment (CCA) but also to extend the lifetime of the network by periodically going to sleep or performing low power listening (LPL). Moreover, to synchronize between the nodes in a network, the nodes regularly update the schedule by sending and receiving a SYNC packet containing the address of the sender and the time of their next sleep period.

Advantages for energy efficiency

Contention-based protocols can avoid or detect collisions with a CCA and using RTS/CTS/ACK control packets. The nodes will enter a sleep period or LPL technique periodically to reduce energy consumption. Furthermore, the CSMA/CA mechanism has simple deployment, lower delay, reliable transmission and low bandwidth utilization for small size networks, such as WBANs.

Disadvantages for energy efficiency

The CSMA mechanism demands additional energy waste for RTS, CTS and ACK packets. If a node switches from listening to sending, it will not listen to the channel. Collisions can occur if a RTS or CTS packet arrives during a transceiver state switch. In addition, the nodes are also energy waste for regularly communicating SYNC packets to synchronize the schedule with their neighbor nodes.

2.3 Schedule-based MAC Protocols

Schedule-based (or called contention-free mechanism) MAC protocols are performed by assigning a predefined time slot to each node. The nodes will use these time slots for reliable communication in WBANs. The

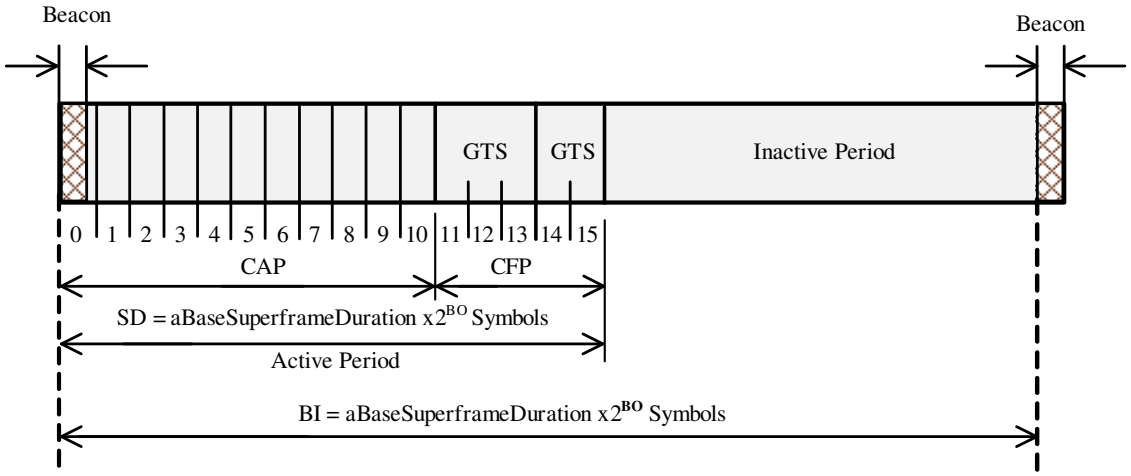

Fig. 1 IEEE 802.15.4 superframe structure

time division multiply access (TDMA) mechanism is a good example of a schedule-based mechanism. In the TDMA technique, the radio channel is bound by a superframe structure, which includes a number of time slots assigned by an access point or PAN coordinator. Each node uses an exclusive time slot that is allocated sufficient time to complete sending and receiving data packets [17]. The node goes into a larger sleep period or standby to save power. TDMA-based MAC protocols, such as BodyMAC [10], Medical MAC (Med-MAC) [38], energy efficient low duty cycle MAC (EELDC-MAC) [23], Battery Dynamics Driven MAC (BDD-MAC) [35] and Context Aware MAC (CA-MAC) [20] are developed to enhance the energy efficiency by reducing the possibility of collision of packets, radio transmission times, idle listening and control packets overhead. On the other hand, the TDMA-based [25] protocol uses link state dependent scheduling (LSDS), which schedules each independent slot time for each node. The node only transmits data packets when its slot time is predicted to be good and delays transmission when its slot time is predicted to be bad. Therefore, it reduces the power consumption in communications.

Advantages for energy efficiency

The schedule-based mechanism is an attractive solution for WBANs because it was designed for energy efficiency and reliable transmission. The TDMA-based MAC protocols can accommodate in-body nodes, which demand power-efficient and reliable communications for variable traffic in WBANs.

Disadvantages for energy efficiency

TDMA schemes support variable WBAN communications. The time slots can be allocated according to the traffic requirements whenever a node demands transmission. TDMA schemes are not scalable, flexible and adaptive with dynamic types in a network topology and limit the maximal number of nodes within a deployment area. In addition, cluster formation and time slot allocation for each node in a cluster consume energy as an overhead. The power of a gateway node or access point will deplete easily due to the more communications with other nodes.

2.4 Hybrid MAC protocols

IEEE 802.15.4 standard is a low-power protocol designed for low data rate applications. As shown in Figure 1, the beacon-enabled model of IEEE 802.15.4 has three periods: a contention access period (CAP), a contention free period (CFP) and inactive period [18, 32]. The nodes can send data packets in two different periods in a superframe that is called CAP and CFP. The beacon interval (BI) is the time interval between two beacons, and the superframe duration (SD) is the active time interval of a superframe, which includes a CAP and CFP [18]:

BI = aBaseSuperframeDuration * 2^{BO}
SD = aBaseSuperframeDuration *2^{BO}
In here:
aBaseSuperframeDuration =960 symbols
1 symbol = 16 μs
BO = Beacon Order
SO = Superframe Order

The IEEE 802.15.4 standard provides two modes of action, which are a beacon-enabled and beacon-disabled mode (or non-beacon mode) to interact with the nodes in a network [41]. In a beacon-enabled mode, the network is managed by an access point. This node sends

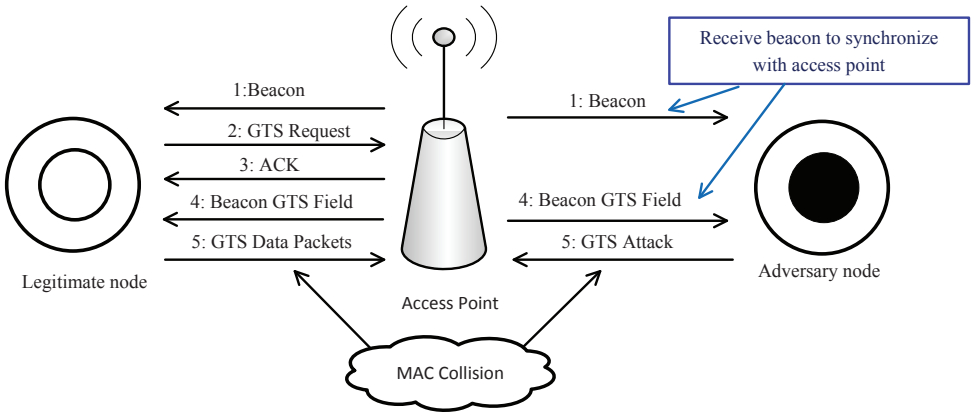

Fig. 2 Attack scenario using the GTS interval

beacon packets periodically to other nodes at beacon interval (BI) so that the nodes synchronize with the superframe structure and use the slotted CSMA/CA in the CAP protocol. In a beacon-disabled mode, the access point does not send a beacon frame. The nodes send data packets to other nodes or access points using the unslotted CSMA/CA protocol in CAP. To save energy, all the nodes will go into a sleep period during the long inactive period [45]. The CFP consists of guaranteed time slots (GTS), which are similar to the TDMA mechanism. The nodes can use the assigned time-slots to transmit data packets regularly to other nodes or access points.

The Zebra MAC (Z-MAC) [30] protocol is a hybrid protocol that utilizes the advantages of both CSMA and TDMA. Z-MAC can reduce the idle listening time using TDMA under a low level of contention. When the contention level is high, many nodes attempt to access the channel simultaneously. In this situation, Z-MAC switches to CSMA to accommodate more nodes attempting to access the channels. Accordingly, Z-MAC can improve the network performance and increase the energy efficiency. Furthermore, the Gateway MAC (G-MAC) [3] protocol organizes WBANs according to the clusters; each cluster has a cluster head (called gateway node).

The structure frame is divided into two periods: a contention period and contention-free distribution period. In the contention period, a node can send future-request-to-send (FRTS) control message to the gateway node to reserve the wake-up and sleep schedules in the contention-free period. The gateway node synchronizes the wake-up and sleep time between the nodes. After synchronization, the gateway node sends a gateway traffic indication message (GTIM) to the nodes. During the contention-free period, the nodes exchange data packets and re-elect the cluster head according to the Resource Adaptive Voluntary Election (RAVE) scheme.

Advantages for energy efficiency

Hybrid protocols employ two mechanisms: a contention-based mechanism, like the CSMA, and a contention-free mechanism, like the TDMA. In the contention-free mechanism, the nodes will go to sleep and wake up at a reserved time slot. Therefore, the idle listening time is reduced. When the content is high, the hybrid protocols switch to a contention-based mechanism to admit more channel accesses. The hybrid protocols can adapt to the different network conditions.

Disadvantages for energy efficiency

Combining the two mechanisms increases the complexity of the hybrid protocols. The transition between the contention-free and contention-based mechanism requires more control packets. The transmission of control packets will not only increase the network traffic but also consume additional energy.

3 Energy Exhausting Attacks

This section discusses three major energy-exhausting attacks: Collision, Denial of Sleep and Selfish.

3.1 Collision Attack

As mentioned above, collision is the main source of energy wastage. With the knowledge of MAC protocols, adversary nodes can intentionally inject dummy packets into the WBANs and cause collisions. In contention-based MAC protocols, such as CSMA/CA, RTS/CTS and Acknowledged control packets are used to avoid collisions between legitimate sensor nodes. On the other hand, an adversary node listens to the control packets

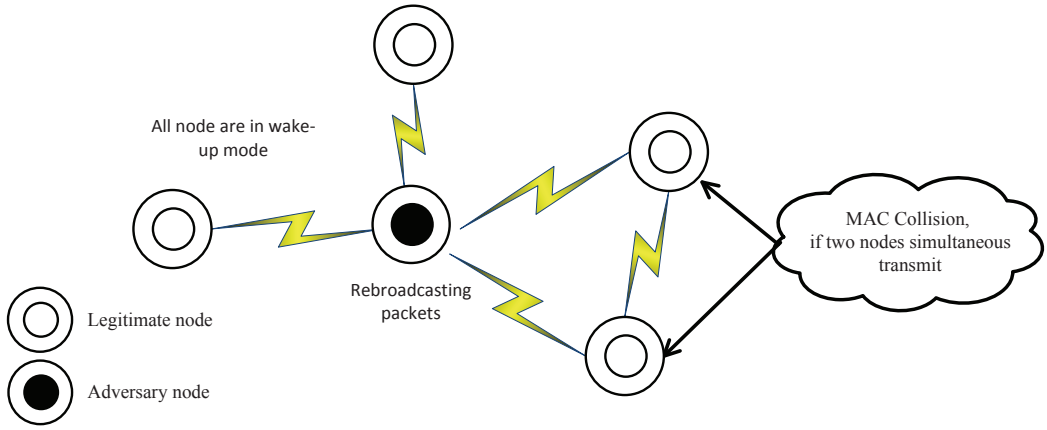

Fig. 3 Scenario of a denial of sleep attack using broadcast packets

and does not follow the normal MAC protocol operation. The RTS packet header includes duration information, which is the amount of time required to transmit the data packets. By knowing this duration information, the adversary node easily sends dummy packets to the wireless channel and performs a collision attack. For Schedule-based MAC protocols, the adversary node must synchronize with the access point by receiving the beacons successfully to conduct a collision attack.

For example, the IEEE 802.15.4 [18] standard consists of three periods: contention access period, contention free period and inactive period. The contention free period uses a schedule-based MAC protocol. The legitimate node sends a Guaranteed Time Slots (GTS) allocation request to the access point, which includes the length and direction (called descriptor) [31, 34]. If the access point accepts the GTS, it will announce a beacon message to all nodes. At that time, the adversary node will know the allocated GTS(ed note: Already defined.) by extracting the GTS descriptor from the received beacon frame. After that, the attacker can create interference and cause a collision of the GTS data packets between the legitimate nodes and access point, as shown in Figure 2 [24, 33, 44].

3.2 Denial of Sleep

In this denial of sleep attack mechanic, the adversary node attempts to decrease the life time of the sensor nodes in WBANs by prolonging the working time of sensor nodes. The principal goal of denial of sleep attacks is to force the nodes in WBANs to remain in either the wake-up period or active period. A denial of sleep attack on MAC protocols in WBANs affects the energy consumption of the node by preventing the nodes from going to a sleep period or inactive period. The adversary node with full knowledge of the layer protocols attempts to maintain the sensor nodes in the active period during the superframe structure or during the duty cycle, such as Sensor-MAC (S-MAC) [43], Timeout-MAC (T-MAC) [7], and Berkeley MAC (B-MAC) [26, 29]. Consequently, the lifetime of the sensor nodes will be reduced rapidly. Raymond, D. et al. [29] classified the denial-of-sleep attack on the MAC-layer of WBANs using the following three methods: unauthenticated broadcast attack, intelligent replay attack and full domination attack.

3.2.1 Unauthenticated Broadcast Attack

In this method attack, the adversary node knows everything about the MAC protocol but is unable to penetrate the network. The adversary node consecutively broadcasts unauthenticated packets to all nodes in the WBANs by imitating all the rules of the MAC protocol. The unauthenticated packets affect the sleep and listen cycle of almost all the nodes in the WBANs, which keeps the transceiver of nodes in the listening period to receive packets. The unauthenticated packet or fake packet is identified by deciphering and comparing the information in the receiver node. This is called a mutual authentication scheme [4, 15].

For contention-based MAC protocols, (CTS)/(RTS), Synchronization packets and low power listening (LPL) are used to handshake or control the process actions of the network. Therefore, when the adversary node broadcasts unauthenticated packets continuously into the network for a long time, these messages will be received and checked in the Link layer of the nodes because it thinks that these messages are from its legal neighbor nodes. After the nodes authenticate the packets, they will discard these messages as fake packets. On the other hand, when the nodes receive fake packets, they will have stayed in the wake up period

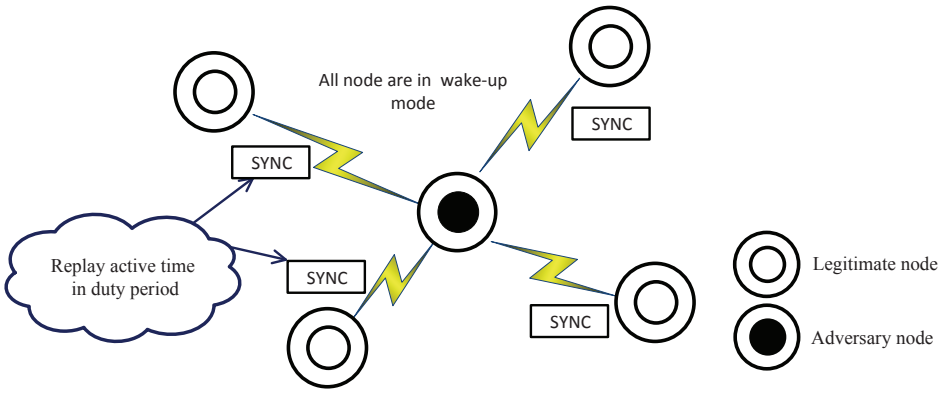

Fig. 4 Scenario of a denial of sleep attack using an intelligent replay attack

resulting in a waste of power. For example, with the Sensor-MAC (S-MAC) [43] protocol, during the sleep period, the nodes periodically wake at the scheduled listen time of its neighbors to synchronize its sleep schedule with the neighbors by broadcasting a SYNC packet. When the adversary node broadcasts unauthenticated packets at the scheduled listen time of the legitimate node, it will awake and receive these unauthenticated packets. Therefore, the nodes are unable to enter the sleep period because they have received and rejected useless packets.

In the Berkeley MAC (B-MAC) [26] protocols, the nodes will also periodically sense the channel in a fixed interval (using the LPL technique) to check the channel. If the channel is busy, the nodes will turn on their transceiver and remain awake for the time required to receive the incoming packets. Therefore, the nodes cannot enter sleep period to save power. For the Timeout-MAC (T-MAC) [7] protocol, the nodes also does not enter sleep period during the contention period because of the need to be awake to communicate periodically with its neighbors by sending and receiving the control packets. The Gateway MAC (G-MAC) protocol [3] combines contention-based and contention-free. Under this protocol, the adversary node affects the gateway more, and it will remain in the wake-up period during the entire collection period due to RTS/CTS/DATA-/ACK exchange with the other nodes.

In the schedule-based mechanism MAC protocols, the adversary node also broadcasts unauthenticated packets into the network. On the other hand, the nodes in the network have been scheduled by assigning each node a slot time to transmit to the access point or manager node. Consequently, it will be difficult for this type of attack to affect all sensor nodes but it might reduce the bandwidth network. An unauthenticated broadcast attack will have an impact on its energy consumption and decrease the lifetime of all the sensor nodes by preventing it from entering the sleep period. Figure 3 shows that adversary node broadcasts control packets (RTS-/CTS/ACK/SYN) repeatedly to all nodes in the network so that all nodes must be in the wake-up period and receive it.

3.2.2 Intelligent Replay Attack

In intelligent replay attack, the adversary node has complete knowledge of the MAC protocol but is unable to penetrate the network. The adversary node will use its full knowledge about the layer protocols to perform an intelligent replay attack in WBANs. The SYNC packets will be replayed at interval of the node's duty cycle to skip the sleep period and begin a new duty cycle for each node. Therefore, the nodes are kept in the wake up period and run out of energy, such as Timeout-MAC (T-MAC) [7] and Sensor-MAC (S-MAC) [43].

The nodes use the SYNC packet to perform synchronization for the active period and sleep period of the nodes, which is sent at the beginning of each frame. The receiver node will recalculate the next sleep time depending on the value in the SYNC packet to maintain synchronization with the other nodes whenever it receives the SYNC packets. The adversary node will record the sleep time value of each node, which is indicated in the SYNC packet to retransmit the SYNC packet to all nodes [29]. If the SYNC packet is encrypted and the adversary node cannot read the sleep time value, the node can still identify by monitoring the actions network and calculate the time of the transition from the sleep portion of a frame to the SYNC period in the next frame.

For Gateway MAC (G-MAC) [3], the GTIM and FRTS messages can be replayed to prevent all the nodes from entering the sleep period because the nodes need to be awake in a interval time during the contention-free period to listen to these packets. In schedule-based MAC protocols, each node is assigned a predefined time

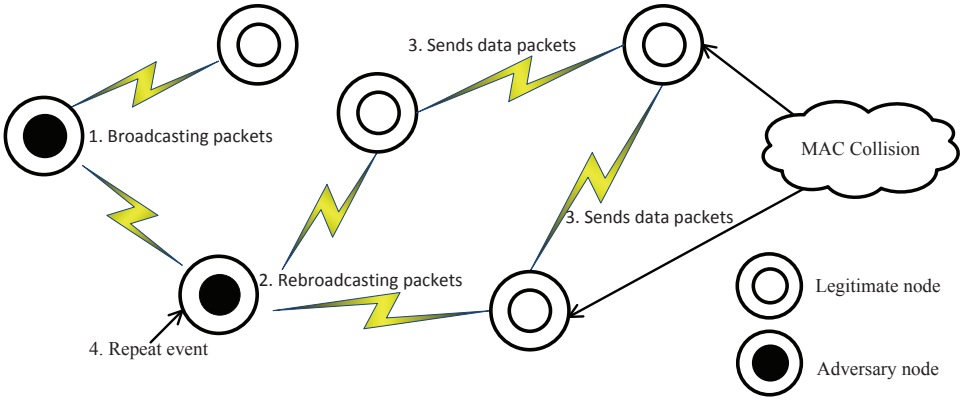

Fig. 5 Scenario of a denial of sleep attack using full domination attack

slot policy to communicate reliably in the network. With this attack type, a replay attack is difficult to perform on a legitimate node because it does not use a SYNC packet, such as Medical MAC (MedMAC) [38], which uses timestamp scavenging, and the Adaptive Guard Band Algorithm (AGBA) to synchronize between the access point and the other nodes. Energy-Efficient Low Duty Cycle MAC (EELCD-MAC) [23] performs synchronization using the same Network Control Packet (NC) at the end of the frame. This type of attack on the MAC protocols prevents the nodes from entering the sleep or inactive period. Figure 4 shows that the adversary node replays its SYNC packets to all nodes in the network. The nodes will restart the duty cycle and keep them in the wake-up period.

3.2.3 Full Domination Attack

This type of attack assumes that the adversary node knows everything about the MAC protocol and can penetrate the network. This is one of the most destructive attack types in WBANs. This type of attack increases the power consumption in almost all MAC protocols because it can penetrate the network and gain knowledge of the layer protocols. The full domination attack against the Sensor-MAC (S-MAC) [43] or Timeout-MAC (T-MAC) [7] protocol is a similar intelligent replay attack. On the other hand, in this attack method, the adversary node does not replay the SYNC packets. Instead, it modifies the sleep schedule of the nodes in the network by setting a new sleep time for the nodes, (e.g., set up a maximum value) so that nodes are unable to enter sleep period. The sleep time contained in the SYNC packets is the time the nodes begin entering the sleep period.

When the nodes receive this new sleep time, they will recalculate the next sleep time according to the new sleep time value in the SYNC packet to synchronize the sleep schedule with the other nodes in the WBANs. Against the Gateway MAC (G-MAC) [3], the adversary node will modify the wake-up and sleep schedules in the GTIM of the legitimate nodes to keep all nodes on the wakeup period during the contention-free period of the frame. Because the GTIM contains the wake-up and sleep schedules of the nodes in the contention-free period, this message will be received at all nodes in the contention period. After modification, the adversary node will broadcast the GTIMs at Point Coordination Function Interframe Space time to all the nodes in the WBANs.

To attack the gateway node, the adversary broadcasts FRTS messages to the gateway at the contention period to keep it awake during the wake up period. In addition, the full domination attack can perform an authenticated broadcast attack, alike the unauthenticated broadcast attack. On the other hand, in this case, the adversary node sends the broadcast authenticated packets to the WBANs, which will be confirmed and accepted at all receiver nodes to prevent the nodes from entering the sleep period or cause collision. For schedule-based MAC protocols, each node is assigned a predefined time slot. The nodes will use a time slot policy to transmit its data packets to the access point or other nodes. Accordingly, it is difficult for the adversary nodes to make a domination attack on all legitimate nodes but can reduce the bandwidth network or cause interference at an access point.

As shown in Figure 5, there are two adversary nodes, which are numbered 1 and 2. The details of the events are as follows: Step 1: adversary node 1 broadcasts a packet to the network. The packet is authenticated by all the nodes. Step 2: adversary node 2 broadcasts the packet to the network

Step 3: node 3 sends the data packet and causes a collision with packet of the adversary node 2 broad-

Table 1 Summary of energy exhausting attacks in MAC protocols in WBANs

EEM	MAC	Unauthenticated Broadcast Attack	Intelligent Replay Attack	Full Domination Attack	Collision Attack	Selfish Attack
	S-MAC	Keeping awake nodes by broadcast fake packets at the scheduled listen time of their neighbors	Replaying SYN packet to keep awake nodes during synchronization time	Modification sleep schedule to prevent nodes going sleep period in SYN packets	Collision or conflict by sending CTS/RTS packets	Using short back off window
C-B	T-MAC	Preventing sleep nodes during the contention period by broadcast fake packets	Replaying SYN nodes going sleep period	Preventing sleep nodes by modifying time sleep in SYN packets	Causes collisions by sending a short noise packet in WBANs	Using short back off window
M	Wise MAC	Preventing sleep nodes by receiving fake packets after getting preamble sampling	Effect on nodes lower than other attack method	Energy waste when nodes regularly check channel to enter activity mode	Collision in access point by sending attack packet	Using short back off window
	B-MAC	regularly receive fake packets due to using PLP technique	Effect on lower due to not using SYN packet	Effect on lower due to not using SYN packet	Can perform collision attack if knowing duration information	Using short back off window
S-	Body MAC	Effect on gateway node, lower effect on sleep period of nodes	Difficult to attack due to not using SYN packet	Difficult effect on sleep period of nodes	Easy effect on nodes due to sending data in GTS slot time	Difficult to attack
B M	TDMA -based	Difficult effect due to using predicted channel before sending data	Difficult to replay SYN packet in sleep period of nodes	Difficult effect on nodes in sleep period	Effect on sending data in GTS slot time, can cause delay	Difficult to attack
	Med-MAC	Difficult effect on sleep period of nodes due to adjustable time slots	Difficult effect due to using number of beacon to synchronize	Difficult effect on sleep period of nodes	Easy effect on access point and attacked node in GTS slot time	Difficult to attack
H-	Z-MAC	Effect on lower due to assigning slot time for node to transmit	Difficult to attack in a low level of contention period	Lower Effect on nodes in contention period	Effect on contention-free period in GTS time	Difficult to attack in contention period
B M	CA-MAC	Effect on nodes in low contention period	Lower effect due to using beacon packets to synchronize	Effect on lower nodes in contention period	Lower effect in contention period in GTS slot time	Difficult to attack
	G-MAC	Effect on gateway node during a collection period difficult in saving power	The GTIM or FRTS packet can replayed in collection period	Modifying GTIM or FRTS packet to prevent sleep	Effect on lower nodes or access point	Effect on contention period

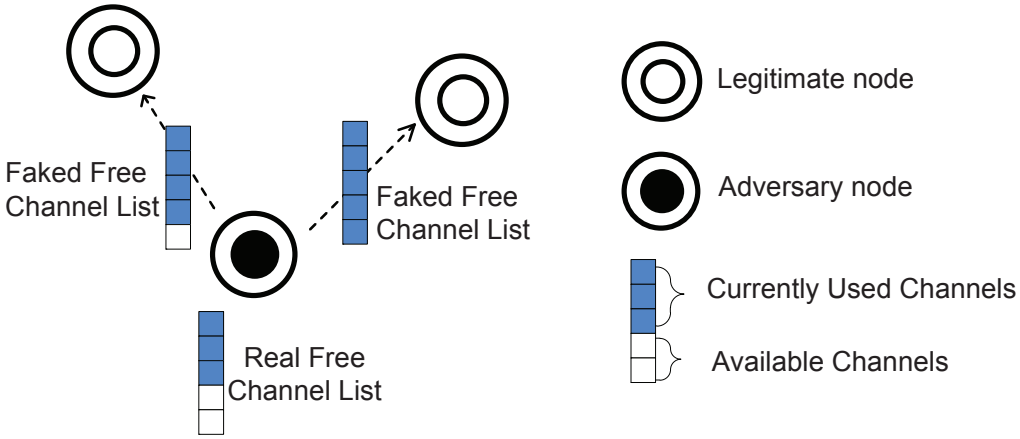

Fig. 6 Scenario of selfish attack in multichannel WBNs

cast. Step 4: adversary node 2 repeatedly broadcasts the packet to the network, which prevents the nodes from entering the sleep state and its battery power will be exhausted.

3.3 Selfish Attack

In selfish attacks, the adversary nodes take advantage of the MAC protocols to use the resources unfairly. Contention-based MAC protocols are more vulnerable than the schedule-based MAC protocols. The schedule-based MAC protocol, such as TDMA, assigns each node a predefined time slot for data transmission. The access point determines the time-slot assignment policy. Therefore, the adversary nodes find it difficult to perform a selfish attack. In the schedule-based MAC protocol, such as CDMA/CA, the sensor nodes sense the channel before sending the data packets. If the channel is idle, the sensor nodes wait until the DIFS time interval and then send the data packets. If the channel is busy, the sensor nodes increase the waiting time exponentially. On the other hand, the adversary nodes can always choose a shorter waiting time and have higher chance to access the channel than the legitimate nodes. The legitimate nodes have to wait a longer time and sense the channel that consumes more power.

In multi-channel WBANs, each sensor node has multiple channels. The channels consist of one common control channel and several data channels [19]. A common control channel is dedicated only to exchanging management information. Each sensor node will regularly broadcast the current multiple channel allocation information to all of its neighboring sensor nodes using a common control channel. The channel allocation information includes the number of channels in current use as well as the number of available channels. The adversary nodes will broadcast fake information on the available channels to pre-occupy them.

The adversary nodes will send a larger number of channels in current use than real to reserve the available channels for later use. The legitimate nodes cannot use the pre-occupy channels. With limited channels, there is high probability of collision, and the legitimate nodes will consume more energy for sensing and waiting, as shown in Figure 6. Table 1 summarizes the different attacks on the MAC protocols in WBANs. Abbreviations in table: Energy-Efficient mechanisms (EEM), Contention-based mechanism (CBM), Schedule-based mechanism (SBM), Hybrid-based mechanism (HBM).

4 Summary

Energy consuming attacks reduce severely the lifetime of the sensors and affect the quality of healthcare services. This paper identified the major types of energy consuming attacks as a denial of sleep, congestion and unfairness attacks. The MAC protocols were classified into a contention based, schedule based and hybrid based mechanism. Finally, the paper provided a detailed analysis and summary of the effect of the attacks against energy efficient MAC protocols. Future work will design and develop detection and prevention mechanisms for energy consuming attacks.

References

1. Aghdasi, H. S., & Abbaspour, M. (2008). ET-MAC: An energy-efficient and high throughput MAC protocol for wireless sensor networks. In *Proceedings of Sixth Annual Conference on Communication Networks and Services Research*, (pp. 526–532). Nova Scotia, Canada.

2. Bhuiyan, M. M., Gondal, I., & Kamruzzaman, J. (2011). I-MAC: Energy efficient intelligent MAC protocol for wireless sensor networks. In *Proceedings of IEEE 17th Asia-Pacific Conference on Communications*, (pp. 133–138). Kota Kinabalu Sabah, Malaysia.
3. Brownfield, M. I., Mehrjoo, K., Fayez, A. S., & Davis, N. J. (2006). G-MAC: Wireless sensor network energy-adaptive MAC protocol. In *Proceedings of IEEE Consumer Communications and Networking Conference*, (pp. 778–782). Nevada, USA.
4. Chen, C., Hui, L., Pei, Q., Ning, L., & Qingquan, P. (2009). An effective scheme for defending denial-of-sleep attack in wireless sensor networks. In *Proceedings of Fifth International Conference on Information Assurance and Security*, (pp. 446–449). Xi'an, China.
5. Chen, M., Gonzalez, S., Vasilakos, A., Cao, H., & C.M.Leung, V. (2010). Body area networks: A survey. *Mobile Networks and Applications*, *16*(4), 171–193.
6. Choi, S.-C., Lee, J.-W., Kim, Y., & Chong, H. (2007). An energy-efficient MAC protocol with random listen-sleep schedule for wireless sensor networks. In *Proceedings of IEEE Region 10 Conference*, (pp. 1–4). Taipei, Taiwan.
7. Dam, T. V., & Langendoen, K. (2003). An adaptive energy-efficient MAC protocol for wireless sensor networks. In *Proceedings of the 1st international conference on Embedded networked sensor systems*, (pp. 171–180). California, USA.
8. Dargie, W., Chao, X., & Denko, M. K. (2010). Modelling the energy cost of a fully operational wireless sensor network. *Telecommunication Systems*, *44*(1-2), 3–15.
9. El-Hoiydi, A., & Decotignie, J.-D. (2004). WiseMAC: an ultra low power MAC protocol for the downlink of infrastructure wireless sensor networks. In *Proceedings of the Ninth International Symposium on Computers and Communications*, (pp. 244–251). IEEE Computer Society Washington, DC, USA.
10. Fang, G., & Dutkiewicz, E. (2009). BodyMAC: Energy efficient TDMA-based MAC protocol for wireless body area networks. In *Proceedings of the 9th International Symposium on Communication and Information Technologies*, (pp. 1455–1459). Incheon, Korea.
11. Gast, M. S. (2002). *802.11 Wireless Networks: The Definitive Guide*. New York: O'Reilly.
12. Gopalan, S., & Park, J.-T. (2010). Energy-efficient MAC protocols for wireless body area networks: A survey. In *Proceedings of International Congress on Ultra Modern Telecommunications and Control Systems*, (pp. 739–744). Moscow, Russia.
13. Gopalan, S. A., Kim, D.-H., Nah, J.-W., & Park, J.-T. (2010). A survey on power-efficient MAC protocols for wireless body area networks. In *Proceedings of IEEE 3rd International Conference on Broadband Network & Multimedia Technology*, (pp. 1230–1234). Beijing, China.
14. Han, G., Xu, H., Duong, T. Q., Jiang, J., & Hara, T. (2011). Localization algorithms of wireless sensor networks: a survey. *Telecommunication Systems*.
15. Hsueh, C.-T., Wen, C.-Y., & Ouyang, Y.-C. (2011). A secure scheme for power exhausting attacks in wireless sensor networks. In *Proceedings of the Third International Conference on Ubiquitous and Future Networks*, (pp. 258–263). Dallian, China.
16. Jang, B., Lim, J. B., & Sichitiu, M. L. (2008). AS-MAC: An asynchronous scheduled MAC protocol for wireless sensor networks. In *Proceedings of IEEE 5th International Conference on Mobile Adhoc and Sensor Systems*, (pp. 434–441). Atlanta, USA.
17. Kuntz, R., Montavont, J., & Nol, T. (2011). Improving the medium access in highly mobile wireless sensor networks. *Telecommunication Systems*.
18. Lee, B. H., & Wu, H. K. (2007). Study on a delayed back off algorithm for IEEE 802.15.4 low-rate wireless personal area networks. *IET Communications*, *3*(7), 1089–1096.
19. Lee, W., Rhee, S. H., Kim, Y., & Lee, H. (2009). An efficient multi-channel management protocol for wireless body area networks. In *Proceedings of the 23rd international conference on Information Networking*, (pp. 13–17). USA.
20. Liu, B., Yan, Z., & Chen, C. W. (2011). CA-MAC: A hybrid context-aware MAC protocol for wireless body area networks. In *Proceedings of IEEE 13th International Conference on e-Health Networking, Applications and Services*, (pp. 213–216). Columbia, MO, USA.
21. Lu, G., Krishnamachari, B., & Raghavendra, C. S. (2004). An adaptive energy-efficient and low-latency MAC for data gathering in wireless sensor networks. In *Proceedings of the 18th International Parallel and Distributed Processing Symposium*. Santa Fe, New Mexico.
22. Marinkovic, S., Spagnol, C., & Popovici, E. (2009). Energy-efficient TDMA-Based MAC protocol for wireless body area networks. In *Proceedings of the Third International Conference on Sensor Technologies and Applications*, (pp. 604–609). Athens, Greece.

23. Marinkovic, S. J., Popovici, E. M., Spagnol, C., Faul, S., & Marnane, W. P. (2009). Energy-efficient low duty cycle MAC protocol for wireless body area networks. *IEEE Transactions on Information Technology in Biomedicine*, *13*(6), 915–925.
24. Pawar, P. M., Nielsen, R. H., Prasad, N. R., Ohmori, S., & Prasad, R. (2012). Behavioural modelling of WBAN MAC layer security attacks: A sequential UML approach. *Journal of Cyber Security and Mobility*, *1*(1), 65–82.
25. Phua, V., Datta, A., & Oliver, R. C. (2006). A TDMA-Based MAC protocol for industrial wireless sensor network applications using link state dependent scheduling. In *Proceedings of the Global Telecommunications Conference*, (pp. 1–6). San Francisco, CA, USA.
26. Polastre, J., Hill, J., & Culler, D. (2004). Versatile low power media access for wireless sensor networks. In *Proceedings of the 2nd international conference on Embedded networked sensor systems*, (pp. 95–107). Maryland, USA.
27. Rahim, A., Javaid, N., Aslam, M., Rahman, Z., Qasim, U., & Khan, Z. A. (2012). A comprehensive survey of MAC protocols for wireless body area networks. In *Proceedings of IEEE 7th International Conference on Broadband and Wireless Computing Communication and Applications*. Victoria, Canada.
28. Rashwand, S., Misic, J., Misic, V., Biswas, S., & Haque, M. M. (2009). A novel asynchronous, energy efficient, low transmission delay MAC protocol for wireless sensor networks. In *Proceedings of IEEE 29th International Conference on Distributed Computing Systems Workshops*, (pp. 186–193). Montreal, Canada.
29. Raymond, D., Marchany, R., Brownfield, M., & Midkiff, S. (2009). Effects of denial-of-sleep attacks on wireless sensor network mac protocols. *IEEE Transactions on Vehicular Technology*, *58*(1), 367–380.
30. Rhee, I., Warrier, A., Aia, M., Min, J., & Sichitiu, M. L. (2008). Z-MAC: A hybrid MAC for wireless sensor networks. *IEEE/ACM Transactions on Networking*, *16*(3), 511–524.
31. Saleem, S., Ullah, S., & Kwak, K. S. (2011). A study of IEEE 802.15.4 security framework for wireless body area networks. *Sensors Open Access Journal*, *11*(2), 1383–1395.
32. Shrestha, B., Hossain, E., Camorlinga, S., Krishnamoorthy, R., & Niyato, D. (2010). An optimization-based GTS allocation scheme for IEEE 802.15.4 MAC with application to wireless body-area sensor networks. In *Proceedings of IEEE International Conference on Communications*, (pp. 1–6). Cape Town, South Africa.
33. Sokullu, R., Dagdeviren, O., & Korkmaz, I. (2008). On the IEEE 802.15.4 MAC layer attacks: GTS attack. In *Proceedings of the Second International Conference on Sensor Technologies and Applications*, (pp. 673–678). Cap Esterel, France.
34. Sokullu, R., Korkmaz, I., & Dagdeviren, O. (2009). GTS attack: An IEEE 802.15.4 MAC layer attack in wireless sensor networks. *International Journal On Advances in Internet Technology*, *2*(1), 104–114.
35. Su, H., & Zhang, X. (2009). Battery-dynamics driven TDMA MAC protocols for wireless body-area monitoring networks in healthcare applications. *IEEE Journal on Selected Areas in Communications*, *27*(4), 424– 434.
36. Suh, C., & Ko, Y.-B. (2005). A traffic aware, energy efficient MAC protocol for wireless sensor networks. In *Proceedings of International Symposium on Circuits and Systems*, (pp. 2975–2978). Kobe, Japan.
37. Tang, Z., & Hu, Q. (2010). ALLEE-MAC: An adaptive low latency and energy efficient MAC protocol for wireless sensor networks. In *Proceedings of the Sixth Advanced International Conference on Telecommunications*, (pp. 269–274). Barcelona, Spain.
38. Timmons, N. F., & Scanlon, W. G. (2009). An adaptive energy efficient MAC protocol for the medical body area network. In *Proceedings of First International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronics Systems Technology*, (pp. 587–593). Denmark.
39. Ullah, S., Higgins, H., Braem, B., Latre, B., Blondia, C., Moerman, I., Saleem, S., Rahman, Z., & Kwak, K. S. (2010). A comprehensive survey of wireless body area networks: On PHY, MAC and network layers solutions. *Springer Netherlands Journal of Medical Systems*, *36*(3), 1065–1094.
40. Ullah, S., & Kwak, K. S. (2010). Performance study of low-power MAC protocols for wireless body area networks. In *Proceedings of the 21st Annual IEEE International Symposium on Personal Indoor and Mobile Radio Communications*, (pp. 112–116). Istanbul, Turkey.
41. Ullah, S., Shen, B., Islam, S. M. R., Khan, P., Saleem, S., & Kwak, K. S. (2010). A study of MAC protocols for WBANs. *Sensors Open Access Journal*, *10*(1), 128–145.
42. Ye, W., Heidemann, J., & Estrin, D. (2002). An energy-efficient MAC protocol for wireless sensor networks. In *Proceedings of the 21st Annual Joint*

Conference of the IEEE Computer and Communications Societies, (pp. 1567–1576). New York, USA.
43. Ye, W., Heidemann, J., & Estrin, D. (2004). Medium access control with coordinated adaptive sleeping for wireless sensor networks. *IEEE/ACM Transactions on Networking*, *12*(3), 493–506.
44. Zapata, M. G., Zilan, R., Barcel-Ordinas, J. M., Bicakci, K., & Tavli, B. (2010). The future of security in wireless multimedia sensor networks. *Telecommunication Systems*, *44*(1), 77–91.
45. Zheng, T., Radhakrishnan, S., & Sarangan, V. (2005). PMAC: An adaptive energy-efficient MAC protocol for wireless sensor networks. In *Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium*. Denver, Colorado.

Minho Jo is a Professor of the Dept. of Computer Science and Engineering, Korea University, Seoul. He received his B.S. degree in Dept. of Industrial Engineering from Chosun University, S. Korea, and Ph.D. degree in networks and algorithms from the Dept. of Industrial and Systems Engineering, Lehigh University, USA in 1994. He was one of the founding members of the LCD Division, Samsung Electronics, S. Korea. He serves as an Editor of IEEE Wireless Communication, Editor of IEEE Network, Associate Editor of Wileys Security & Communications Network, and Associate Editor of Wireless Communications and Mobile Computing. Dr. Jo is the Founder and Editor-in-Chief of the KSII Transactions on Internet and Information Systems. He is the Vice President of Institute of Electronics of Korea (IEEK), and is the Executive Director of the Korean Society for Internet Information (KSII). His current research interests include WBAN, cognitive radio, network security, and wireless communications and mobile computing.

Longzhe Han is a Ph. D candidate in the Dept. of Computer Science at Korea University, Seoul. He received his M.S. degree in computer software from Myongji University, in 2006. His research interests include cognitive radio networks, network security, multimedia communications, WBAN, and embedded software engineering.

Nguyen Duy Tan received his B.S. and M.S. degrees in Information Technology from HaNoi Academy of Military Technology in 2006 and VietNam National University, HaNoi College of Technology in 2009, respectively. Currently, he is a lecturer of the Faculty of Information Technology, HungYen University of Technology Education and postgraduate in HaNoi College of Technology.

Hoh Peter In is a Professor in the Dept. of Software Technology and Enterprise at Korea University, Seoul. He received his Ph. D in Computer Science from University of Southern California (USC). He was an Assistant Professor at Texas A&M University. He earned the most influential paper award for 10 years in ICRE 2006. His primary research interests include WBAN, embedded software engineering, social media platform and service, and software security management. He has published more than 100 research papers.