# The Need, Advances and Challenges Related to Wireless Body Area Network Communication Technology

## Wireless Communication Networks

Richard A. Kramer (kramerri@oregonstate.edu), Jin Phoy Rhee (rheej@oregonstate.edu)
*Oregon State University*

***Abstract* — In the U.S. alone: (1) every year, 800,000 people have a stroke, and (2) one person dies every four minutes from a stroke [1]. Once a person has a stroke, if they survive, their quality of life is changed forever. Astonishingly, 80 percent of all strokes are preventable, simply requiring early detection using technology that is seemingly well within reach [1][2], yet has not yet been fully to the masses for a number of reasons. As a result, society and technology are at unique crossroads based on the advent of wireless wearable and even implantable body sensors that can measure important life threatening vital signs. In order to enable communications with wearable and implantable body sensors, researchers have responded by developing and standardizing Wireless Body Area Networks (WBANs) protocols such as IEEE 802.15.6 [3]. The objective of our work is to take the reader to the forefront of the battle to improve wireless network communications within the overall WBAN body sensor system. Specifically, we focus on the areas of: (1) optimization of transmitter power to conserve energy, (2) performance improvements for WBAN devices under interference, and (3) WBAN security. We conclude with a summary of the significant impact that WBAN technology can make in saving lives.**

***Keywords— Wireless Body Area Networks (WBANs), IEEE 802.15.6, IEEE 802.15.4j, secure network, anti-jamming, interference, adaptive power control (APC), adaptive power efficiency, body sensors.***

## I. INTRODUCTION /MOTIVATION

As mentioned above, the statistics are staggering: every year, 800,000 people have a stroke and one person dies every four minutes from a stroke in the U.S. alone [1]. More astonishingly is that fact that it is estimated that *80 percent of all strokes are preventable*, by simply providing early detection [1]. As a result, society and technology are at a unique crossroads based on the advent of wireless wearable and even implantable body sensors to measure life threatening vital signs. The timing could not be better: it is estimated that the population of those ages 60 to 80 years old will increase by 300% by 2050 based on 2000 statistics [2].

Like the technological revolutions ushered in by the advent of life changing technologies such as the cell phone, the computer, and the Internet, wearable and even implantable body sensor devices, like those shown below in Figure 1, stand to make a dramatic impact on society. Imagine a simple, mass produced and cost effective device that can detect artrial fibrillation (the leading cause of a stroke) [1] in its early stages to prevent a stroke and the tragic aftermath - with the outcome instead being replaced with taking preventative medication.

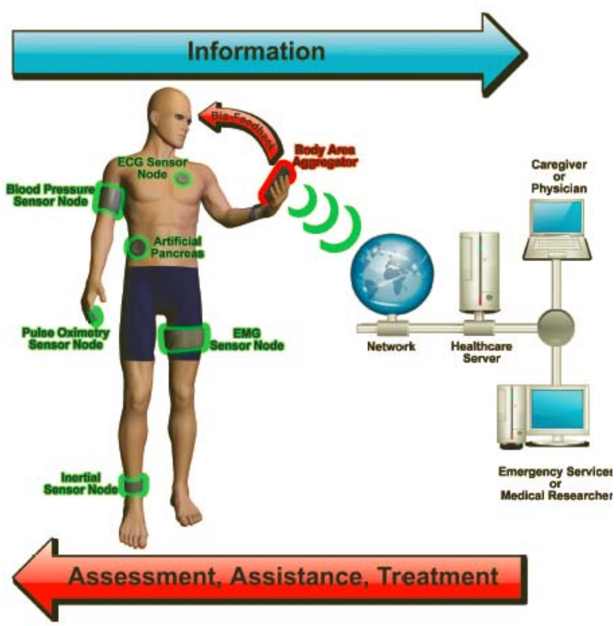



*Figure 1: Body area sensor network and its environment [4].*

While impressive strides have been made related to Wireless Body Area Networks (WBAN) sensor technology, disappointingly, few products are presently offered to the masses that would seemingly fulfill the need to provide early detection of an impending life threatening health crisis such as a stroke.

As further discussed below, in Section II, entitled "Objectives and Contribution", the motivation of our work is to provide the reader with insight into the most recent challenges confronting WBAN body sensors wireless technology. Our paper not only provides insight into the current state of the art challenges confronting WBAN but we also provide a roadmap for future research to improve WBAN performance overall.

## II. OBJECTIVES AND CONTRIBUTION

The objective of our work is to take the reader to the forefront of the battle to improve wireless network communication performance within the overall WBAN system. Specifically, we provide a detailed analysis and proposed improvements within a number of core areas that are further described below:

- In Section IV, entitled "Optimization of Transmitter Power to Conserve Battery Energy", we point to leading research to conserve transmitter power. We introduce the concept of "battery energy cost per bit" for WBAN communications as an improved metric as compared to RSS (Receive Signal Strength), transmit power, and BER (Bit Error Rate) methods currently used in WBAN systems.
- In Section V entitled, "Performance Improvements for WBANs Under Interference", we focus on current communications schemes, we point to deficiencies, and we provide insight into potential improvements.
- In Section VI, entitled: "WBAN Security", we review interesting research to protect patients from malicious cyber attacks from an adversary.

## III. OVERVIEW OF WBAN STANDARDS, SYSTEMS AND DEVICES

In order to enable communications with wearable and implantable body sensors, researches have responded by developing and standardizing WBANs. WBANs were first introduced in draft form in 2010 as IEEE standard 802.15.6 [5], ratified in 2012 [3] and further standardized in the IEEE standard 802.15.4j (amendment 4) in 2013 [6]. The charter of 802.15.6 is stated to be: "Short-range, wireless communications in the vicinity of, *or inside, a human body*" [3] (emphasis added).

A typical WBAN device system is shown in Figure 1. As shown, a wide variety of body sensor technologies are used, both implantable (e.g., an artificial pancreas sensor) and external (e.g., a pulse oximetry sensor). These sensors are bound by a common network and wireless transceiver interface. Per Figure 1, patient data flows from the patient's sensor nodes to the healthcare provider systems [4].

As shown below in Figure 2, each sensor node commonly includes an energy source, sensors, a mixed signal processor, an actuator, storage and a transceiver [4].

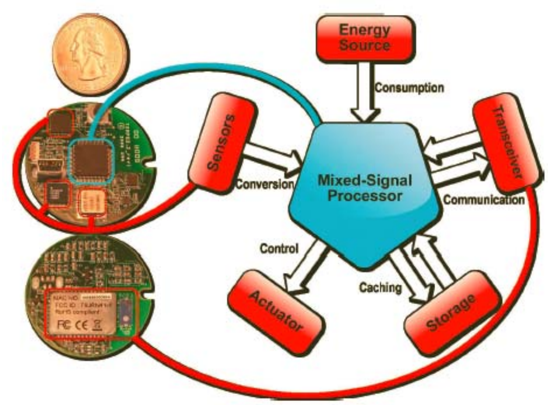



*Figure 2: WBAN node architecture [4].*

One of the most prevalently cited wireless transceivers modules in modern day WBAN research papers [7][8] is the CC2420 Zigbee IEEE 802.15.4 single chip solution introduced in 2004. The CC2420 single chip solution is merely 7x7 mm in size and is implemented on a PCB (Printed Circuit Board) measuring about 1x1 cm, as shown in Figure 3 [9][10][11].

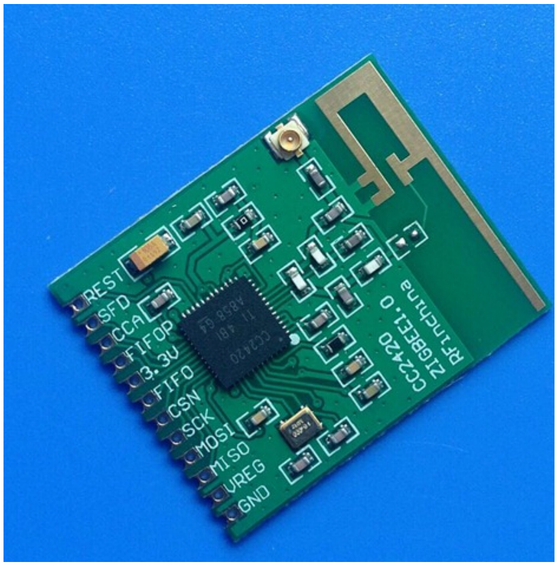



*Figure 3: Zigbee CC2420 wireless module [10].*

As we discuss in detail below, the primary challenges with such a system entails optimization of transmitter power to conserve battery energy, WBAN interference resiliency, and WBAN security.

## IV. Optimization of Transmitter Power to Conserve Battery Energy

### A. *Overview of Transmitter Power Control within WBAN Devices*

*For WBAN devices, especially implantable WBAN devices, conservation of battery power is of the utmost importance. Unfortunately, the WBAN device's wireless transceiver uses more energy from the battery than the overall energy used by the processing system within the WBAN device [12][4]. This is further shown* in Figure 4 as follows.

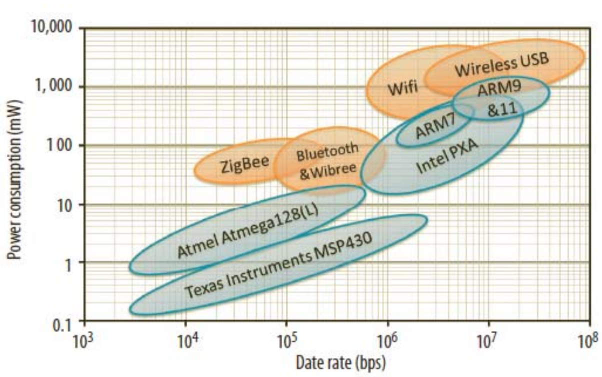



*Figure 4: Average power consumption of wireless transceivers (orange) versus microprocessors (blue) [4].*

For WBAN devices: the human body, human activity, and the body's surroundings have a significant impact on the integrity of the wireless communication channel. The wireless communication channel impairments include both temporal loss and spatial wireless transmission loss. To expand, such transmission losses are dramatically impacted by the surrounding environment, distance, multipath fading, antenna direction, and small scale fading transmission loss [12][13]. For example, a person exhibiting a brief running motion introduces a path loss variation of 45 dB [14] with a Tc (channel coherence time) ranging from 36-73 ms for a walking motion to 23-66 ms for a running motion [14].

To compensate for these factors, Adaptive Transmission Power Control (ATPC) techniques have been heavily researched and are well known. The heavily researched techniques include the use of ATPC within wireless sensor networks [13]. The primary emphasis to improve the link quality and to reduce the BER (Bit Error Rate) is to monitor the RSSI (Received Signal Strength Indication) and the Link Quality Indication (LQI) levels at the receiver and provide feedback to the WBAN device. In turn, this information is then used by the WBAN device, whereas the WBAN device increases transmitter power at the detriment of battery energy consumption while benefiting BER and RSSI [12][13]. Such a modern day ATPC proposed solution is shown below, characteristically absent of feedback related to actual energy consumed from the battery.

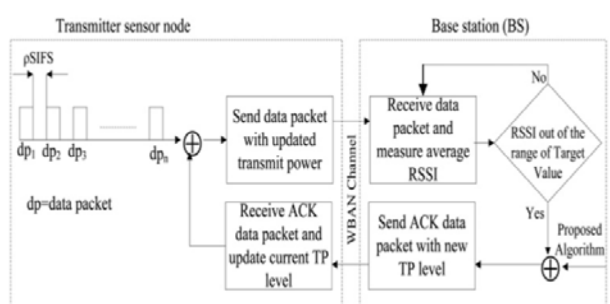



*Figure 5: Typical RSSI based ATPC implementation [7].*

### B. *Present day ATPC optimization research advances*

1) Overview

To address the optimization of transmitter power versus BER, significant research has been done to develop adaptive algorithms

[8][11][12][14] including the development of fuzzy adaptive power control algorithms [15]. The research related to WBAN ATPC has been overwhelming based on RSS and BER evaluation as the basis of optimizing wireless link performance. Some of the more promising research for WBAN ATPC entails determining *when to transmit* (e.g., (1) sense when loss is minimal, and (2) transmit while loss is minimal).

2) Transmission time adaptation

Novel solutions, such as that proposed by Zang, et al. [16], entails sensing body movement via an accelerometer so that the optimal time to transmit can be determined. As shown in Figure 6 below, there is a significant correlation between body movement (including slow fading) and RSSI. By taking advantage of the input from an accelerometer that is integrated with the WBAN device, an intelligent ATPC algorithm was developed to only transmit during optimal periods as detected by the accelerometer.

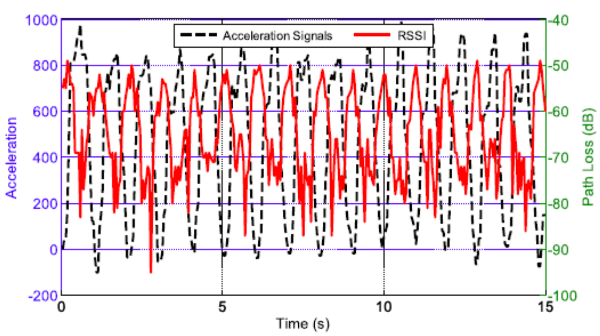



*Figure 6: RSSI "path loss" versus body movement as measured by an accelerometer [16].*

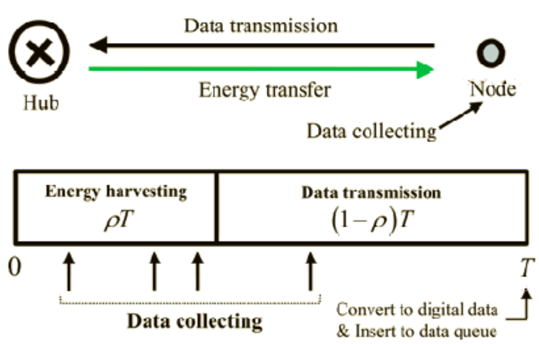



*Figure 7: Adaptive time splitting between energy harvesting and data transmission [17].*

Jang, et al. [17], proposes another promising solution utilizing an intelligent algorithm to determine the optimal duty cycle to allow data transmissions based on battery conditions. To expand, as shown in Figure 7, Jang, et al. discloses an algorithm that determines the optimal time to gather RF energy received (via various recharging methods based on heat, etc.) in order to recharge the battery, versus the optimal time to use battery energy to transmit data [17].

3) Intelligent ATPC algorithms

Significant research effort has been expended in the development of better algorithms that allow the wireless system to adapt to the dynamic environment. Such solutions include those that use Markov learning processes to learn the environment and in turn, to reward good responses, and penalize poor responses related to transmitter adaptation [11]. Yet other solutions use adaptive channel gain estimation and fade prediction algorithms, such as the algorithm shown in Figure 8 [8]:

Initialization: $\rho = 1dB$, $THR_L = 2dB$, $THR_H = 4dB$, $\theta = 3dB$, $K = 10$ and $\delta = 2dB$
$\mu(0) = 3dB$
**for** each superframe $n$ **do**
  **if** $\sqrt{\widehat{MSE}(n)} > \mu(n-1) - THR_L$ **then**
    $\mu(n) = \mu(n-1) + \rho$
  **else if** $\mu(n-1) > THR_{min}$ **and** $\sqrt{\widehat{MSE}(n)} < \mu(n-1) - THR_H$ **then**
    $\mu(n) = \mu(n-1) - \rho$
  **end if**
  **if** last data frame lost (no ACK) **then**
    $\mu(n) = \mu(n-1) + \theta$
  **end if**
  $THR_{min}$ Optimization
  **if** $(\sqrt{\widehat{MSE}(n)} < \delta)$ **and** (ACK received successfully) **then**
    $THR_{min} = THR_{min} - \rho/K$
  **else if** $(\sqrt{\widehat{MSE}(n)} < \delta)$ **and** (No ACK received) **then**
    $THR_{min} = THR_{min} + \rho$
  **end if**
**end for**

*Figure 8: Adaptive fade margin estimator [8].*

While such approaches are certainly feasible, these approaches may not be practical to implement on a low-processing power embedded device that is highly optimized for low-end and thus low power applications.

### C. *Proposed improvements / additional research to optimize both battery energy consumption and transmission efficiency*

As discussed above, significant work has been done related to ATPC based adaption techniques using RSSI, LQI, motion detection, battery level monitoring, and the like. Further, research has been done to correlate power consumption from the power supply to the wireless transmit bit rate [18], calculate the energy per bit [19], and relate power consumption of a CC2420 [9][10][11] based on antenna position [8].

While the research related to ATPC for WBAN devices is impressive, it is our opinion that a more important factor for WBAN is to directly correlate "Battery Energy Cost per Bit" to determine the energy efficiency of the received data. To illustrate the important distinction between: (1) RSSI and/or LQI based ATPC, versus (2) Battery Energy Cost per Bit based ATPC, consider the following trivial scenario that exaggerates the BER to better illustrate the method:

**<u>Scenario 1:</u>**

$$Bit\ rate\text{:}\ 100\ kbps$$

$$\frac{Error\ rate}{Bit\ rate} = \frac{50\ kbps}{100\ kbps} = 0.5$$

$$Bits\ recieved\ = (100 - 50) =\ 50\ kbps$$

$$Tx\ Power\ =\ 50\ mW$$

$$\frac{Bits\ received}{Tx\ Power\ \cdot\ time} = \frac{50\ kbps}{50mW \cdot s} = \mathbf{1.0}\,\frac{\boldsymbol{kb}}{\boldsymbol{mW}}$$

**<u>Scenario 2:</u>**

$$\frac{Error\ rate}{Bit\ rate} = \frac{30\ kbps}{100\ kbps} = 0.3$$

$$Bits\ recieved\ = (100 - 30) =\ 70\ kbps$$

$$Tx\ Power\ =\ 60\ mW$$

$$\frac{Bits\ received}{Tx\ Power \cdot\ time} = \frac{70\ kbps}{60mW \cdot s} = \mathbf{1.2}\,\frac{\boldsymbol{kb}}{\boldsymbol{mW}}$$

From above, it would appear that Scenario 2 is better than Scenario 1, whereas Scenario 2 delivers 1.2 kbps of data per 1 mW-second as compared to Scenario 1 which delivers only 1.0 kbps for the same 1 mW-second.

Now consider the following: we further correlate the deliverable data payload to the battery energy used. In short, we *measure the total consumption from the battery while transmitting* (total energy consumption based on the processor, transmitter, transmitter inefficiencies, etc.).

**<u>Scenario 1 (from above)</u>:**

$$Battery\ power\ @\ 50\ mW\ Tx\ Power\ =\ 75\ mW\ (battery\ power)$$

$$\frac{Bits\ received}{Battery\ Power\ \cdot\ time} = \frac{50\ kbps}{75mW \cdot s} = \mathbf{0.67}\,\frac{\boldsymbol{kb}}{\boldsymbol{mW}}$$

**<u>Scenario 2 (from above)</u>:**

$$Battery\ power\ @\ 60\ mW\ Tx\ Power\ =\ 100\ mW\ (battery\ power)$$

$$\frac{Bits\ received}{Battery\ Power\ \cdot\ time} = \frac{60\ kbps}{100mW \cdot s} = \mathbf{0.6}\,\frac{\boldsymbol{kb}}{\boldsymbol{mW}}$$

As can be seen, for WBAN devices, ATPC techniques that correlate wireless payload data throughput *with* battery energy consumption are better suited to prolong battery life while maximizing transmission efficiency. This is in sharp contrast to the RSSI and/or LQI based ATPC techniques discussed above. Thus in conclusion, it would seem that additional research in this area is warranted.

## V. Performance Improvements for WBANs Under Interference

Reliable communications is essential for medical devices. The implanted or attached medical devices should be able to monitor the condition of the body in real time and take quick action through external communications in the case of an emergency[20]. In such cases, reliable communications is critical, however, interference degrades the quality of the wireless signal transmission, thus putting the patient at risk[21]. In this section, we address the causes of interference in wireless communications for WBAN systems and present solutions to improve overall system performance.

A. WBAN signal interference with Wi-Fi

As an "information society", the use of Wi-Fi is prolific. A significant challenge confronting WBAN devices is the fact that both Wi-Fi (IEEE 802.11) and WBAN (IEEE 802.15.4) devices use the same unlicensed Industrial, Scientific, and Medical radio (ISM) band as is further shown in Figure 9. Using the same ISM band for both Wi-Fi and WBAN devices causes significant signal interference problems, ranging from increased error rates, to the inability to acquire a communication channel. Such interference is significantly increased when people who use WBAN devices are located near Wi-Fi devices.

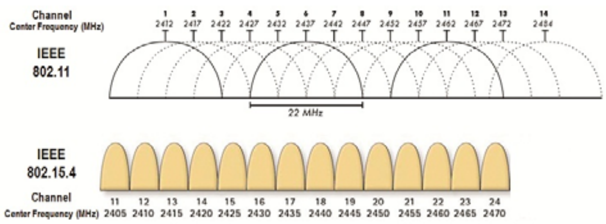



*Figure 9: IEEE802.11 and IEEE 802.15.4 Channels in the 2.4 GHz ISM band [22].*

1) Background

The WBAN IEEE 802.15.4 protocol standard implements both slotted and unslotted Carrier-Sense Multiple Access (CSMA) algorithms. One major difference between the two CSMA algorithms is that the CSMA unslotted algorithm does not require time division and synchronization with nodes using a periodic beacon. For this reason, the unslotted CSMA algorithm is more useful when devices lose the control signals due to signal interference [23]. Using the unslotted algorithm is also more suitable than the slotted algorithm for sending emergency messages when the WBAN device detects that the patient has an emergency situation. This is due to the fact that the unslotted algorithm has a shorter latency for sending emergency packet data [24].

To expand, when a WBAN, IEEE 802.15.4 device desires to transmit a packet using the unslotted CSMA algorithm, the transmitting device waits a randomly selected wait time based on a [0, $2^{BE}$-1] backoff period (where "BE" is called the Backoff Exponent with a range = [$BE_{min}$ , $BE_{max}$]). If after waiting the backoff period and there is an available channel during the Clear-Channel Assessment (CCA) duration, the node will send a packet. If the channel is busy, BE is increased by 1 and the system will try again using the new backoff period. This process repeats until the $BE_{max}$ value is reached, at which point the packet will be discarded. Once the transmitting WBAN device transmits a packet, an ACK signal must be received from the receiver within the SIFS (Short Inter Frame Spacing) time period.

*Similarly, when a Wi-Fi, IEEE 802.11 device desires to transmit a packet*, the transmitting device senses the medium during the Distributed coordination function Inter Frame Space (DIFS) period. If the transmitting device is unable to transmit, a backoff period process is invoked. The backoff period is based on a Contention Window size (CW) from [1, $CW_{max}$]. If the medium is free then the CW value is decremented (or the CW value is paused when system cannot find a valid channel). Like WBAN devices, Wi-Fi devices initiate transmission after the backoff period. If the transmitting Wi-Fi device does not get an ACK signal during SIFS period, then the transmitter assumes that the transmission failed, doubles the CW value, and repeats the backoff process. The transmitting device repeats this process until the $CW_{max}$ value is reached at which point the packet is deleted. On the other hand, the CW value remains at the $CW_{min}$ value when the transmission is a success [25].

2) IEEE 802.11 and IEEE 802.15.4 interference

Both Wi-Fi, IEEE 802.11g and WBAN, IEEE 802.15.4 devices transmit data packets in almost the same manner using the same channels, however, the IEEE 802.11g standard calls for a shorter backoff period than does the IEEE 802.15.4 standard. In other words, *Wi-Fi devices have lower latency than WBAN devices. Subsequently, Wi-Fi devices have the advantage of finding and acquiring a channel quicker as compared to WBAN devices.* Another major difference between Wi-Fi and WBAN devices is that Wi-Fi devices utilize higher transmission power, thus causing interference for WBAN devices [26].

3) WBAN performance improvement with Wi-Fi

Since WBAN devices involve the transmission of potentially life threatening (or life saving) data, ideally WBAN devices would use independent channels as compared to Wi-Fi devices. In the paper, “Performance Improvement of the Wireless Body Area Network (WBAN) Under Interferences” [25], Sarra et al., seeks to optimize software settings within Wi-Fi and WBAN devices, without changing hardware, to mitigate interference. The goal is to introduce a simple parameter tuning solution that improves WBAN device communication stability during high contention periods or when interference levels are high. To identify the optimal solution, four experiments were performed in a WBAN system composed of 12 nodes. Table 1 describes the setting values of each WBAN device used in the experiment.

Table 1. WBAN parameter setup

| | Packet size | Backoff time | CCA |
|---|---|---|---|
| Test 1 | 512 bits | 320 us | 128 us |
| Test 2 | 512 bits | 160 us | 64 us |
| Test 3 | 128 bits | 320 us | 128 us |
| Test 4 | 128 bits | 160 us | 64 us |

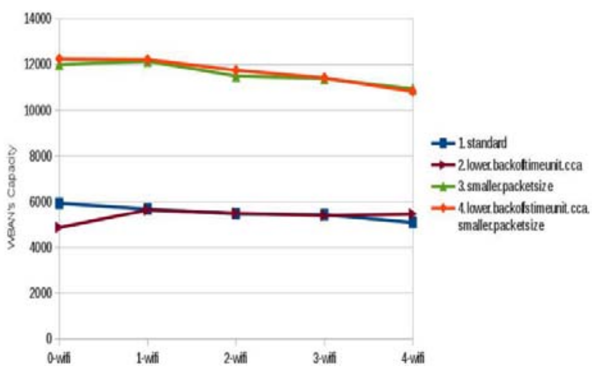


*Figure 10: The average capacity in receiving packets in the WBAN’s node [25].*

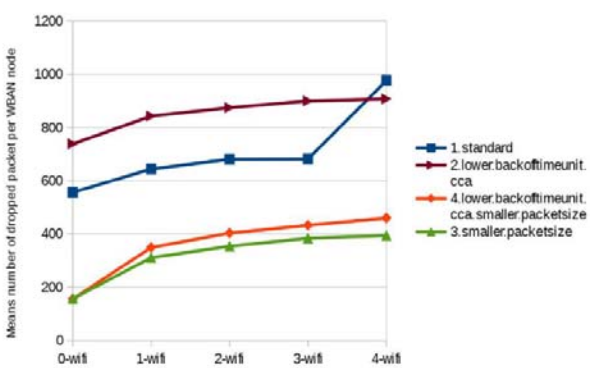


*Figure 11: The average number of dropped packet per WBN node [25].*

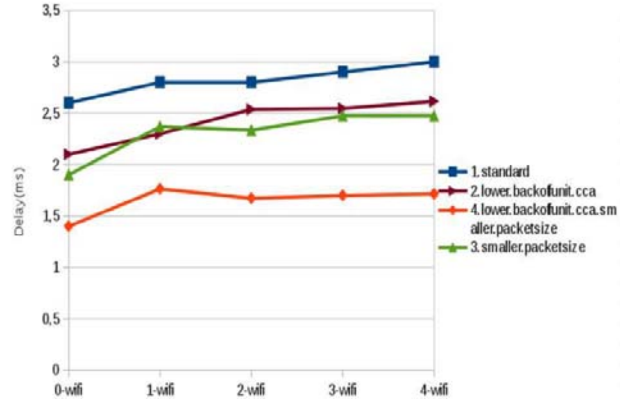


*Figure 12: Packet’s delay [25].*

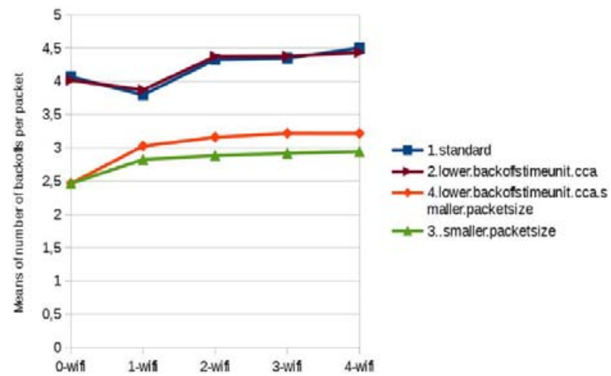


*Figure 13: The average number of backoffs per packet* [25].

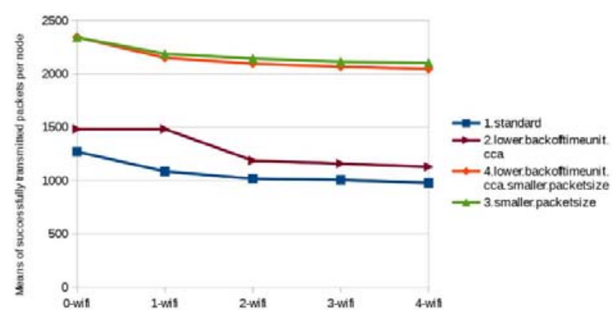


*Figure 14: The average number of successful transmitted packet per node* [25].

As shown above in Table 1 and Figures 10-14, Test 1 is the baseline for all other test methods. Test 1 uses standard WBAN system settings. In comparison, Test 2 has the same packet size as Test 1, however in Test 2, the backoff time and CCA time values have been decrease so that packets are sent more often. As the results indicate, decreasing the backoff and CCA time values are not optimal because the receiving efficiency of the nodes is decreased as shown in Figure 10 and packet loss is increased as shown in Figure 11. Overall, Test 2 is not suitable for medical devices because the increase in packet loss results in decrease power efficiency. In contrast, Test 3 reduces the packet size as compared to Test 1 and 2, and as a result, performance improves as shown in Figures 10-14. Lastly, Test 4 not only reduces backoff and CCA time, but also reduces the packet size. As a result, Test 4 improves overall performance as shown in Figures 10-14. In summary, because Test 4 reduces packet size and propagation delay, nodes can send data much faster and packet loss is reduced. Thus Test 4 identifies the optimal settings to improve WBAN communications with signal interference without changing hardware.

B. Wireless communication interference with EMI

All electronic devices generate electromagnetic interference (EMI), including electronics on circuit boards. EMI causes signal interference in wireless communications [27][28]. Since WBAN devices are for medical uses, immunity to EMI is critical [29]. In the paper "Experimental Assessment of Using Network Coding and Cooperative Diversity Techniques in IEEE 802.15.4 Wireless Sensor Networks" [30], Valle et al. proposes network coding combined with cooperative diversity techniques that enable reliable communication within Wireless Sensor Networks (WSN).

1) Cooperative diversity techniques:

Cooperative diversity techniques aim to increase network reliability by having every available node retransmit data to the target node[31]. One major disadvantage of cooperative diversity is that all nodes need to remain in operation even if the node is not the intended end receive node. The techniques further use network coding. As shown in Figure 15, using network coding, a signal is encoded by an XOR operation, thus allowing the transmission of different information from one node to multiple other nodes via a single transmission. By combining the data at the intermediate node, the number of data packets to be transmitted can be reduced while at the same time, each receiver node can decode the desired data by using the XOR operation of the received data with the receiving node's own data.

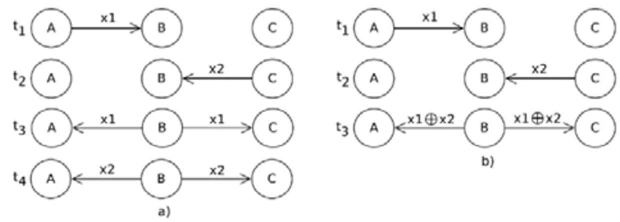



*Figure 15: Network coding in wireless environment [30].*

As can be seen in Figure 15, a) shows no network coding which takes 4 time cycles to communicate the data. On the other hand, b) uses network coding and only requires 3 time cycles to communicate the same amount of data.

2) Improvement of WSN under EMI interference

In the presence of EMI signal interference, direct wireless communications between the sender and receiver is not possible. Valle et al. further proposes a wireless transmission method using a star topology network with a set of nodes that periodically send information to a coordinator. In this work, two methods are used to transmit the message: 1) each message is sent by the node itself (1st chance) and an additional node relays (e.g., a relay node) the message which is decoded by the coordinator (2nd chance). As shown in Figure 16 below, the coordinator selects a new relay set in a two step process. In the first step, the number of relay nodes available on the network is determined based on the PER (Packet Error Rate) value, which is based on the network error rate (line 2). In the second step, the coordinator determines what relay nodes are available based on the Received Signal Strength Indication (RSSI) (line 3). The coordinator then transmits information to all nodes regarding the available set of relay nodes in the network. The relay nodes subsequently send messages as well as receive messages from other nodes. The first message originates from the reserved slot (line 8). The second transmission occurs in a reserved slot coded for the message, which is encoded in one message and retransmitted to that slot (lines 9 and 10). The coordinator that sent the beacon message receives all messages from both the node and the relay node (line 12). The coordinator decodes messages that were not resolved by the linear system (e.g. resolves network coding), and computes the PER value for these unresolved messages (line 12 to 14).

```
For ever do
    Coordinator determines the number of relay nodes based
    on the PER, and
    Determines the set of relay nodes to be used based on the
    RSSI value of each node and transmits the beacon payload
    for each node in the network do
        Receive the beacon information
        Waits until the reserved slot and then transmit the  message
    end
    for each relay node in the network do
        Overhear the messages from neighbors and encode them,
        Wait until the reserved slot and then transmit the message
    end
    Coordinator receives messages from nodes and relay nodes,
    Solves the linear system,
    Estimates the network PER and the values of node's RSSI
end
```

*Figure 16: Transmission Algorithm Overview* [30].

3) Experiment and results

The setup used by Valle et al. to test signal/EMI interference is shown in Figure 17 which was implemented within an anechoic chamber.

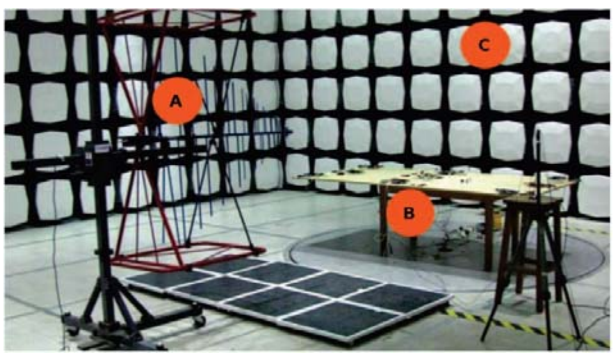



*Figure 17: Anechoic chamber* [30].

Table 2. Anechoic Chamber Setup

| | | |
|---|---|---|
| (A) | EMI generator | AM/FM noise, 2.425 GHz (Channel 15 of 802.15.4) |
| (B) | WSN on a table | 10 WSN nodes, ATmega256RFR2 |
| (C) | Chamber | Testing area |

Table 2 provides information about the test setup environment. All experiments were carried out in the anechoic chamber. The noise source utilized 80% AM modulation with an AM modulation carrier frequency of 20 kHz, a signal bandwidth of 40 MHz, with an output power ranging from -20 dBm to -10 dBm. Experiments were conducted using 10 WSN node devices. The WSN node devices were laid out on the table as shown in *Figure 17*, arranged as further shown in Figure 18.

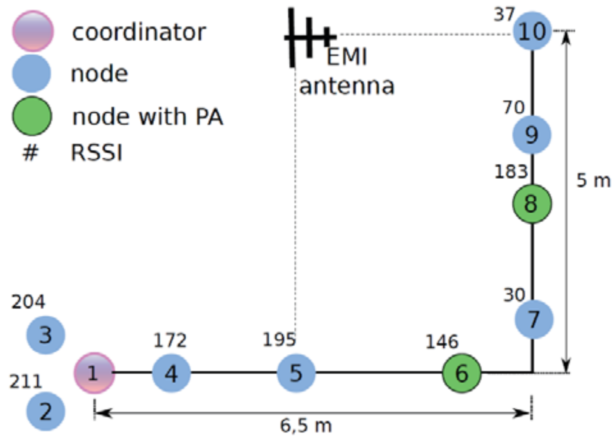



*Figure 18: Monitored area setup [30]*

As shown in Figure 18, the coordinator node is node 1. Additionally, the EMI antenna is directed toward nodes 6 through 10, and thus those nodes are the nodes that are the most impacted by EMI. Nodes 2 and 3 serve a relay nodes and communicate with the coordinator node because nodes 2 and 3 are least impacted by EMI. Finally, nodes 6 and 8 serve as Power Amplifier (PA) nodes.

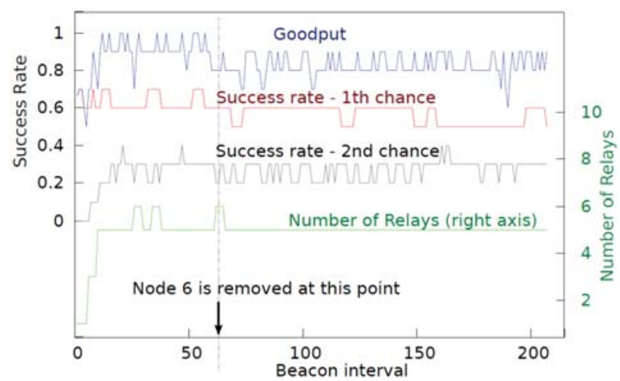



*Figure 19: Success rate and number of relays* [30].

Figure 19 shows the results when the beacon interval was executed 200 times. The average success rate at the first opportunity (1st transmission) was 60%. The first unsuccessful message reached an average throughput of 90% by restoring nearly 75% of the second chance transmissions using network coding and cooperative diversity techniques.

## VI. WBAN SECURITY

With the proliferation of information technology, the number of malicious cyber attacks continues to increase [32]. The communication of the medical device data contains personal information which can be further exploited by a malicious third party [33]. Subsequently, it is of paramount importance that WBAN medical devices are protected against malicious cyber attacks [34][35]. In this section we discuss various safeguards to protect personal information within WBAN systems.

### A. WBAN security in PHY layer.

Most cyber security solutions utilize both encryption and device authentication techniques. The typical method for securely establishing a communication session is via an encryption key[36]. A significant challenge arises during a medical emergency when, for example, hospital personnel needs access to the encryption key to make adjustments to a WBAN Implantable Medical Devices (IMDs) [37]. Another significant challenge relates to the risk of jamming the WBAN device by a malicious unauthorized user. In the paper, "Physical Layer Security for Wireless Implantable Medical Devices", Ankaralı et al. introduces a system to establish a secure communication connection between a WBAN IMD and a WBAN Wearable External Device (WED). Figure 20 shows the system concept including the "secure region".

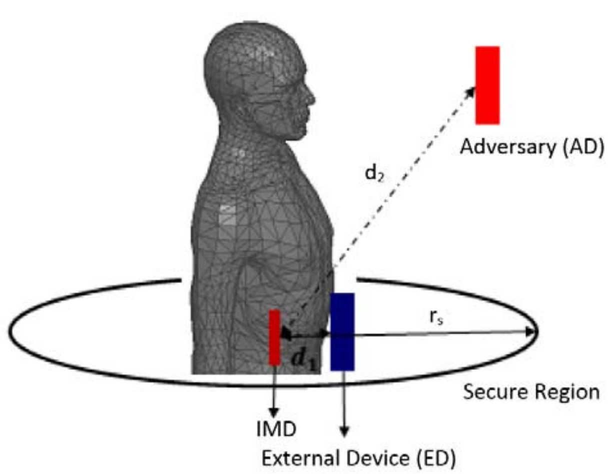



*Figure 20: System Concept for Secure Region [37].*

#### 1) Concept of PHY layer security

As shown in Figure 20, the goal is to secure communications between the IMD and the WED within the secure region, whereas the secure region extends the radius around the patient. The objective is to prevent an Adversary (AD), at a distance of $d_2$, from maliciously attacking the IMD. In this proposed scenario, the IMD sends the pilot signal p(t) so that the WED can estimate the channel. Channel estimation is performed through the following process.

$$h_{\in} = h(t) + w(t)p^{-1}(t)$$

The channel estimate assumes that w(t) is additive noise and $h_{\in}$ is defined as a scalar value based on the channel estimation and one-tap frequency-domain equalization for transmission between am IMD and a WED.

$$x(t) = h_{\in}^{-1} \sum_{n=-\infty}^{\infty} X_n g(t - n\tau_0)$$

N, g(t), and $\tau_0$ are respectively: (1) a symbol representing QAM, (2) a pulse shaping filter function, and (3) the time spacing between symbols.

$$y(t) = \int_{-\infty}^{\infty} h(\tau)x(t-\tau)d\tau$$

A signal containing additional noise after passing through the linear time-varying channel is denoted as r(t) as shown below, where h(t) represents the channel gain as a function of time, and w(t) is additive noise.

$$r(t) = h(t)x + w(t)$$

Pilot symbols received by the channel also have potential impairments. Therefore, the estimated channel response can be calculated as follows, where P denotes a pilot symbol:

$$\hat{h} = h + w(t)/P, \tau = w(t)/P$$

The above formula has a direct impact on the BER and is used to identify the secure region around the patient's body. In addition, the pilot signal transmitted by the IMD can be used as a "wake-up" signal to wake-up the WED. Uniquely, based on this solution, if the IMD is attacked from an external AD device, the IMD can defend itself by using the WED. To expand, when the IMD detects an external attack from an AD device, the IMD sends a wake-up signal to the WED. In turn, the WED comes out of sleep/idle mode and sends a jamming signals to AD attacker [38].

2) Simulation, setup and results

Ankaralı et al. presents the effects of the abovementioned jamming technique based on simulation results[39]. Table 3 shows the path loss parameters used for BER testing where d is distance of transmission (e.g., between the WED and IMD), $d_0$ is the reference distance, and $P_{0dB}$ is the path loss for the reference distance [40].

Table 3: Path Loss Model Parameters [37]

| Parameter | Parameter Value |
|---|---|
| N | 1.48 |
| $d_0$ | 0.01 m |
| $P_{0dB}$ | 39.37 dB |

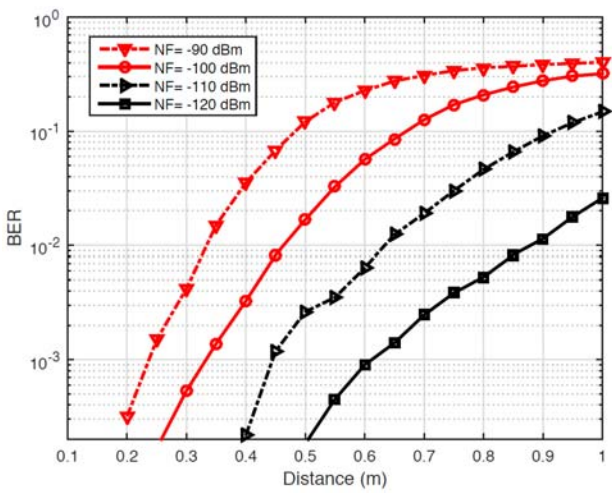



*Figure 21: BER and NFs [37].*

Based on the path loss model, Figure 1 shows the BER performance versus distance for various noise floors (NFs). As the distance between the IMD and the WED increases, the BER also increases. As the device moves away from the IMD, the received pilot signal is reduced, which causes errors in channel estimation. Figure 21 shows the change in BER as the distance increases.

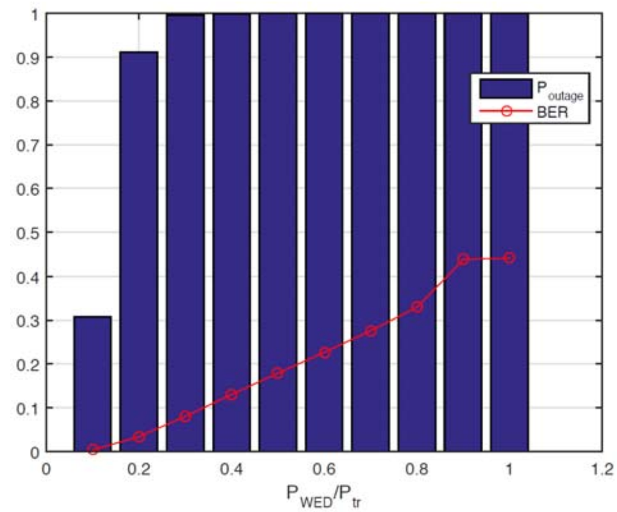



*Figure 22: Adversary output probabilities for different jammer signal powers[37].*

Figure 22 shows the overall anti-jamming performance of the systems as a function of the ratio $P_{WED}/P_{tr}$, where $P_{WED}$ is the WED jamming signal power and $P_{tr}$ is the power threshold. In short, $P_{WED}/P_{tr}$ represents the transmitter jamming power of the WED toward the AD device. The Y-axis shows the amount that the AD device is jammed (the blue bar) which ranges from 0 (not jammed at all) to 1 (completely jammed). Figure 22 also shows the BER between the IMD and the WED (the red line)[1] in order to maintain communications. As shown, the AD device is completely jammed (P = 1) staring at a $P_{WED}/P_{tr}$ ratio of 0.3 while the BER is at an acceptable level to allow communication between the IMD and the WED. In other words, when the $P_{WED}/P_{tr}$ ratio equals 0.3 or more, external attacks can be avoided.

## VII. Conclusion

In this paper, we have disclosed encouraging research that is at the core of providing WBAN technology that is necessary to detecting life threatening emergencies *in advance* to save lives. The advances in WBAN devices related to power management, interference avoidance and security research are serious matters where impressive strides have been made. Nonetheless, this is only the beginning until such technology is widely available to those that need it. Just think of the impact that such technology could make based on

[1] Note: the author does not provide a clear description of what the BER reading in this graph represents.

U.S. statistics alone: 800,000 strokes a year, 80% preventable = 640,000 people's lives saved. If we could only impact a fraction of that many people, image the impact we could make [1][2].

**800,000 strokes a year x 80% preventable = 640,000 people's lives changed** [1][2]**.**

*In memory of Richard's mother Rosemary*
*1930-2016*
*The victim of a preventable stroke.*

## BIBLIOGRAPHY


[1] National Stoke Association, "Reduce Your Risk of Stoke Starting Now," 2015. [Online]. Available: https://www.stroke.org/sites/default/files/resources/prevention-brochure-2015.pdf. [Accessed 12 April 2017].

[2] Samaneh Movassaghi, Mehran Abolhasan, Justin Lipman, David Smith, Abbas Jamalipour, "Wireless Body Area Networks: A Survey," *IEEE COMMUNICATIONS SURVEYS & TUTORIALS,* pp. 1658-1686, 2014.

[3] IEEE, "Part 15.6-2012: Wireless Body Area Networks," IEEE Standards Association, 2012.

[4] Mark A. Hanson, Harry C. Powell Jr., Adam T. Barth, "Body Area Sensor Networks: Challenges and Opportunities," *Computer,* vol. 42, pp. 58-65, 2009.

[5] IEEE, "P802.15.6/D04, Jun 2011 - IEEE Draft Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 15.6," IEEE Standards Association, 2011.

[6] IEEE, "Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) (Amendment 4)," IEEE Standards Association, 2013.

[7] Ali Hassan Sodhro, Ye Li, Madad Ali Shah, "Energy-efficient adaptive transmission power control for wireless body area networks," *IET Communications10.1,* pp. 81-90, 2016.

[8] Fabio Di Franco, Yu Ge, Ilenia Tinnirello, "On-body and off-body transmit power control in IEEE 802.15.6 scheduled access networks," *2014 IEEE 25th Annual International Symposium on Personal,* pp. 1254-1258, 2014.

[9] Chipcon, "SmartRF CC2420 2.4 GHz IEEE 802.15.4 / ZigBee-ready RF Transceiver," 9 June 2004. [Online]. Available: https://inst.eecs.berkeley.edu/~cs150/Documents/CC2420.pdf. [Accessed 22 April 2017].

[10] "ZIGBEE CC2420 wireless module," [Online]. Available: https://www.aliexpress.com/item/ZIGBEE-CC2420-wireless-module-So-the-best-best-antenna-on-sale-The-first-generation-of-classic/32687356651.html?spm=2114.40010208.4.6.d2SApt. [Accessed 22 April 2017].

[11] Abbas Arghavani, Haibo Zhang, Zhiyi Huang, "LPA: Learning-Based Power Aware Communication Protocol in WBANs," *2016 IEEE 14th Intl Conf on Dependable,* pp. 512-519, 2016.

[12] Mónica Vallejo, Joaquín. Recas, José L. Ayala, "Proactive and Reactive Transmission Power Control for Energy-Efficient On-Body Communications," *Sensors 15.3,* pp. 5914-5934, 2015.

[13] Shan Lin, Fei Miao, Jingbin Zhang, Gang Zhou, Lin Gu, Tian He, John A. Stankovic, Sang Son, George J. Pappas, "ATPC: Adaptive transmission power control for wireless sensor networks," *ACM Transactions on Sensor Networks (TOSN),* 2016.

[14] Sukhumarn Archasantisuk, Takahiro Aoyagi, Minseok Kim, Jun-ichi Takada, "Transmission power control in WBAN using the context-specific temporal correlation model," *2016 IEEE 27th Annual International Symposium on Personal, Indoo,* pp. 1-6, 2016.

[15] S.-L. Chen, "A Power-Efficient Adaptive Fuzzy Resolution Control System for Wireless Body Sensor Networks," *IEEE Access,* vol. 3, pp. 743-751, 2015.

[16] Mónica Vallejo, Joaquín. Recas, José L. Ayala, "An Accelerometer-Assisted Transmission Power Control Solution for Energy-Efficient Communications in WBAN," *IEEE Journal on Selected Areas in Communications,* vol. 34, pp. 3427-3437, 2016.

[17] Young Rok Jang, Yongok Kim, Jang-Won Lee, Daesik Hong, Sooyong Choi, "Adaptive Queue Management Scheme for Body Area Network with Energy Harvesting," BodyNets, 2013.

[18] Francesco Ivan Di Piazza, Stefano Mangione, Ilenia Tinnirello, "On the effects of transmit power control on the energy consumption of WiFi network cards," *International Conference on Heterogeneous Networking for Quality,* 2009.

[19] Huseyin Cotuk, Kemal Bicakci, Bulent Tavli, "The Impact of Transmission Power Control Strategies on Lifetime of Wireless Sensor Networks," *IEEE Transactions on Computers,* vol. 63, pp. 2866-2879, 2014.

[20] Marwa Salayma, Ahmed Al-Dubai, Imed Romdhani, Youssef Nasser, "Wireless Body Area Network (WBAN): A Survey on Reliability, Fault Tolerance, and Technologies Coexistence," *ACM Computing Surveys (CSUR),* vol. 50, no. 1, April 2017, 2017.

[21] J.N. Laneman, D.N.C. Tse, G.W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Transactions on Information Theory,* vol. 50, pp. 3062-3080, 2004.

[22] "Five Factors to Consider When Implementing a Wireless Sensor Network (WSN)," *National Instruments,* 2017.

[23] M. Maman, F. Mani, B. Denis, "Evaluation of multiple coexisting Body Area Networks based on realistic on-body and Body-to-Body channel models," *2016 10th International Symposium on Medical Information and Communication Technology (ISMICT),* pp. 1-15, 2016.

[24] Yena Kim, SeungSeob Lee, SuKyoung Lee, "Coexistence of ZigBee-Based WBAN and WiFi for Health Telemonitoring Systems," *IEEE Journal of Biomedical and Health Informatics,* vol. 20, pp. 222-230, 2016.

[25] Essafi Sarra, Tahar Ezzedine, "Performance improvement of the wireless body area network (WBAN) under interferences," *2016 IEEE 18th International Conference on e-Health Networking,* pp. 1-6, 2016.

[26] Bin Yuan, Jing Liu, Wenlong Liu, "DIM: A novel decentralized interference mitigation scheme in WBAN," *2015 International Conference on Wireless Communications & Signal Processing (WCSP),* pp. 1-5, 2015.

[27] Idrissa Abubakar, Jafri Din, Manhal Alhilali, Hong Yin Lam, "Interference and Electromagnetic Compatibility Challenges in 5G Wireless Network Deployments," *Indonesian Journal of Electrical Engineering and Computer Science,* pp. 612-621, 2017.

[28] Dong-Yeol Choi, Won-Kyung Kim, Jae-Hyun Kim, "Performance of analog and digital modulation schemes under sweep jamming," *2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN),* pp. 13-15, 2016.

[29] Jung-Hwan Hwang, Tae-Wook Kang, Jong-Hwa Kwon, "Effect of Electromagnetic Interference on Human Body Communication," *IEEE Transactions on Electromagnetic Compatibility,* vol. 59, pp. 48-57, 2017.

[30] O. T. Valle, G. Budke, C. Montez, "Experimental Assessment of Using Network Coding and Cooperative Diversity Techniques in IEEE 802.15.4 Wireless Sensor Networks," *2016 IEEE World Conference on Factory Communication Systems (WFCS),* pp. 1-4, 2016.

[31] O. T. Valle, C. Montez, G. M. Araújo, R. Moraes, F. Vasques, "A WSN data retransmission mechanism based on network coding and cooperative relayers," *2015 IEEE World Conference on Factory Communication Systems (WFCS),* pp. 1-4,

2015.

[32] Gaurav Somani, Manoj Singh Gaurb, Dheeraj Sanghic, Mauro Contid, "DDoS attacks in cloud computing: Collateral damage to non-targets," *Computer Networks,* vol. 109, pp. 157-171, 2016.

[33] Shyamnath Gollakota, Haitham Hassanieh, Benjamin Ransford, Dina Katabi, Kevin Fu, "They can hear your heartbeats: non-invasive security for implantable medical devices," *ACM SIGCOMM Computer Communication Review,* vol. 41, no. 4, pp. 2-13, 2011.

[34] Kanchan Kaushal, Varsha Sahni, "Early Detection of DDoS Attack in WSN," *International Journal of Computer Applications,* vol. 134, pp. 14-18, 2016.

[35] A.J. BURNS, M. ERIC JOHNSON, AND PETER HONEYMAN, "A brief chronology of medical device security," *Communications of the ACM,* vol. 59, pp. 66-72, 2016.

[36] W. Shen, "Secure In-Band Bootstrapping for Wireless Personal Area Networks," *in IEEE Internet of Things Journal,* vol. 3, pp. 1385-1394, 2016.

[37] Z. Esat Ankaralı,Marwa Qaraqe, "Physical layer security for wireless implantable medical devices," *2015 IEEE 20th International Workshop on Computer Aided Modelling and Design of Communication Links and Networks (CAMAD),* pp. 144-147, 2015.

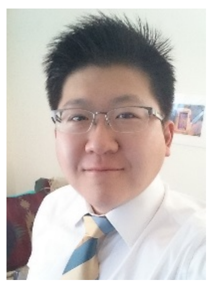
[38] Caixia Xie, Liang Xiao, "User-centric view of smart attacks in wireless networks," *2016 IEEE International Conference on Ubiquitous Wireless Broadband (ICUWB),* pp. 1-6, 2016.

[39] Miftadi Sudjai, Le Chung Tran, Farzad Safaei, Tadeusz Wysocki, Son Lam Phung, "High-speed adaptive wireless body area networks," *EURASIP Journal on Wireless Communications and Networking,* 2016.

[40] A. Fatih Demir, Qammer H. Abbasi, Z. Esad Ankaralı, "Numerical characterization of in vivo wireless communication channels," *2014 IEEE MTT-S International Microwave Workshop Series on RF and Wireless Technologies for Biomedical and Healthcare Applications,* pp. 1-3, 2014.

## About the Authors

Richard Kramer is a Ph.D. student at Oregon State University and a member of IEEE. Richard’s research areas and interests include: video, video compression (encoding / decoding), optimization of video streaming content, network coding, video streaming, cryptography, encryption, and data security. Before attending Oregon State University, Richard served as a top-technology leader in the industry including: Vice President, Engineering/General Manager of Technology for multiple world-wide divisions at General Electric including the Video Systems Group; Vice President, Engineering for high-tech startup Ivex Corporation (a pioneer in video streaming technology); and Vice President, Engineering for Home Wireless Networks (a pioneer in wireless LAN communications).



Jin Phoy Rhee (JP) is a Master of engineering student at Oregon State University. JP has 5 years of hands-on product development experience. JP’s industry product development experience includes: broadcast TV and Ethernet streaming related products for battery powered tablet devices, digital to analog converters, and Wi-Fi access points. Based on JP’s solid industry experience, JP has direct experience with government certification and safety regulation approvals.