

Received March 22, 2019, accepted April 5, 2019, date of publication May 1, 2019, date of current version May 6, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2910029

A New Externally Worn Proxy-Based Protector for Non-Secure Wireless Implantable Medical Devices: Security Jacket

SELMAN KULAÇ¹

Department of Electrical and Electronics Engineering, Faculty of Engineering, Düzce University, 81620 Düzce, Turkey

e-mail: selmankulac@duzce.edu.tr

ABSTRACT Wireless transmission systems of implantable medical devices (IMDs) should be secure against eavesdroppers and adversaries because of patient rights and health. This paper focuses on full-duplex secure communication of wireless IMD systems, proposing a new protector that is compatible with existing unsecure systems. This new protector is an externally worn jacket and therefore called a security jacket. Because some advanced sensors are placed on the jacket to provide physical layer security. Randomly multi-jamming with a great number of sensors is applied when IMD transmission occurs with the jamming extraction and maximum ratio combining (MRC) reception simultaneously. When reception by IMD is performed, a randomized spoofing-based transmit beamforming technique is applied. This protector also supports higher power efficiency and longer battery life.

INDEX TERMS Transmit beamforming, physical layer security for IMDs, spoofing-based transmit beamforming, wireless implantable medical devices, wireless wearable sensors.

I. INTRODUCTION

Wireless communication has become more important in human life in recent years. Therefore, different areas of wireless communication have emerged. One of these areas is healthcare. The wireless implantable medical device (IMD) technology in healthcare domain is further developed due to its wireless capability. Being able to communicate wirelessly with a device placed inside the human body at any time offers great benefits in patient monitoring, device status and treatment. Thus, wireless IMDs will be used in the treatment of different diseases in the future. Some examples of wireless IMDs currently used are deep brain neorostimulators (DBS)s which are used against some movement disorders, cochlear implants which run in the damaged parts of the inner ear (cochlea) to provide sound signals to the brain, implantable cardiac defibrillators (ICD)/Pacemaker which regulate heart rhythms, gastric stimulators for gastroparesis, insulin pumps which deliver insulin. For example, if we consider DBS, it is possible for the physician to observe and follow up the neurochemical and anatomical changes in a certain region of the patient's brain using the DBS system, and to be able to

upload the appropriate treatment to the DBS. It should be noted here that the remote control of the DBS and generating of electrical stimulation signals by the physician requires proper telemetry and command transmissions.

Some important requirements or demands for wireless IMDs can be summarized as follows. They should be biocompatible, environmental resistant and robust. They should have low complexities, a minimum number of parts that will reduce the possibility of failure, dimensions as small as possible, superior and precise functionalities and a very long battery and device lives working at maximum efficiency without needing to be updated periodically. Moreover, they must be secure and sensitive to privacy and confidentiality.

Security and confidentiality are recognized as patient rights. Therefore, confidential and vital information considering illness and treatment records of the patients should be secured. Because, for wireless IMDs, it is possible to reach the data of health status of patients, treatments and device status. Moreover, it is possible to change and even destroy this data and block the usual data communication. It is even possible that the implantable device may be exposed to lethal functioning by changing this data. During the wireless communication of IMDs, there may be malicious listening to data of communication, which is considered passive attack.

The associate editor coordinating the review of this manuscript and approving it for publication was Lorenzo Mucchi.

If communication protocol is solved by listening with time, it can be switched to active attack mode causes spoofing and running abnormally. Active attack may be more effective and have worse effects, which is possible by taking over the remote control of the IMDs.

In wireless communication, physical layer security provides secure communication by staying away from cryptographic methods [1]. Physical layer security aims to provide good channel conditions for the communicating parties and poor channel conditions for the eavesdroppers. Processing power, hardware complexity, power consumption etc. is generally shared between the two communicating parties when performing physical layer security. Some similar recent studies considering the physical layer security are as follows. In [2], it is emphasized that how physical layer security increases the security of battery-powered Internet of Things (IoT) devices effectively. In [3], a watermark-based blind physical layer security using a jamming receiver with a spread spectrum watermarking method is proposed. In [4], physical layer authentication method expresses that human palm has distinct transmission coefficient (S_{21}) for each of the users and is used for in vivo fingerprint identification. In [5], physical layer security based authentication technique using the user's behavioral fingerprint extracted from the radio channel characteristics is proposed.

Cryptographic process for wireless IMDs may increase complexity, number of parts, size, power consumption and so on. Furthermore, changing with the existing devices considering cryptographic structure requires surgery. Thus, providing security in the communication with the implanted devices can be achieved by the external proxy-based or physical layer security rather than by the usage of cryptographic methods [6]. Furthermore, in the case of the physical layer security scenario for existing battery operated implant devices implanted to the patients, all processing power, hardware complexity, power consumption etc. should also be assigned to the external device for the above reasons [7]–[9].

There are some studies in the literature related with physical layer or external proxy-based security for wireless IMDs. An external device called the Communication Cloaker was first proposed in [10]. It acts as a relay or transmitter when it is worn. But it involves some cryptographic process. Another wearable and external device is called IMDGuard or Guardian which provides secure transmission [11]. The IMDGuard or Guardian method is focused on the cryptographic key handling operation based on the patient's electrocardiogram (ECG) signals. In the previous solutions, already implanted IMDs require modification due to the placement of cryptographic hardware and these methods cause an increase in undesired complexity and power consumption. Another external device called MedMon, which contains the anomaly detection method, has been proposed in [12]. The MedMon does not behave as a relay but rather focuses on the physical characteristics of the transmitted signals. If there is an abnormal transmissions, the patient will be warned or it will emit a powerful jamming signal and suppress the

abnormal transmissions. MedMon does not offer any protection against eavesdroppers or passive attackers as known eavesdroppers while providing good protection against active attackers.

Another recommended external device is called Shield, which has been developed to protect ICDs from an active and passive attackers [13]. The shield jams all replies from all the ICDs and all signals from the active attackers. It extracts the replies from composed replies plus jamming signals. But its own query signals or commands (treatment prescription data, etc.) are transmitted without jamming or protection. Therefore, while the queries and commands are publicly and unreliably spread wirelessly, passive listeners or eavesdroppers can easily capture or record all these command data transmitted to the ICDs. Eavesdroppers can thus develop new intelligent techniques through the recorded and not protected data. For example, eavesdroppers can understand the treatment performed by the physician by analyzing the protocol, and can reach the data considering the condition of patient and the status of the ICD (battery life, functioning properly, etc.). If eavesdroppers fully understand and solve the command structure sent, they can obtain capabilities such as changing device settings and IMD therapy (electrical stimulation) parameters, disabling the device, terminating therapy, and sending an electrical shock command [13], [14]. In the literature, some researchers have also recognized the vulnerability of the physical layer, and this has been explicitly expressed in some articles [12], [15], [16] and [17].

Other proxy-based solution, called the Security Belt, focuses on full-duplex secure communication of the wireless IMD systems, a safe design has been proposed that can be integrated into existing unsecure systems [18]. This belt is a body worn device and seen as a belt. Some relaying antennas are installed on this belt to ensure secure transmission in both directions. When reception by the IMD occurs, three antennas at the optimal positions on the belt randomly transmit. When transmission by IMD occurs, Maximal Ratio Combining (MRC) or majority rule techniques with randomized jamming and extraction by three jammers/antennas are applied. In this approach, the belt has a small number of relays or antennas. With more relays or antennas, efficiency could have been increased. However, due to limited surface area on the belt for relays or antennas, the number of relays has to be remain limited.

The purpose of this study is to protect full-duplex transmissions in more efficient way. A special security jacket is proposed containing sensors placed on to ensure security and diversity. When transmissions are carried out from IMD to the sensors in single input multiple output (SIMO) mode, randomly multi-jamming and jamming extraction technique applied. When transmissions are carried out to IMD, randomized spoofing-based transmit beamforming technique applied in multiple input single output (MISO) mode. Frequency shift keying (FSK) modulation in IMD transmissions has some advantages as mentioned in [19], [20]; and therefore, it is given a priority to FSK modulation in this study. Since FSK

modulation is robust to power amplifier non-linearity and noise resistant characteristics, FSK modulation is mostly used as a modulation type in medical implant communication service (MICS) systems [19], [20].

The rest of this paper is organized as follows. System model and proposed protection solution are carried out in Section II. Section III expresses numerical results of the proposed method, and conclusions are drawn in Section IV finally.

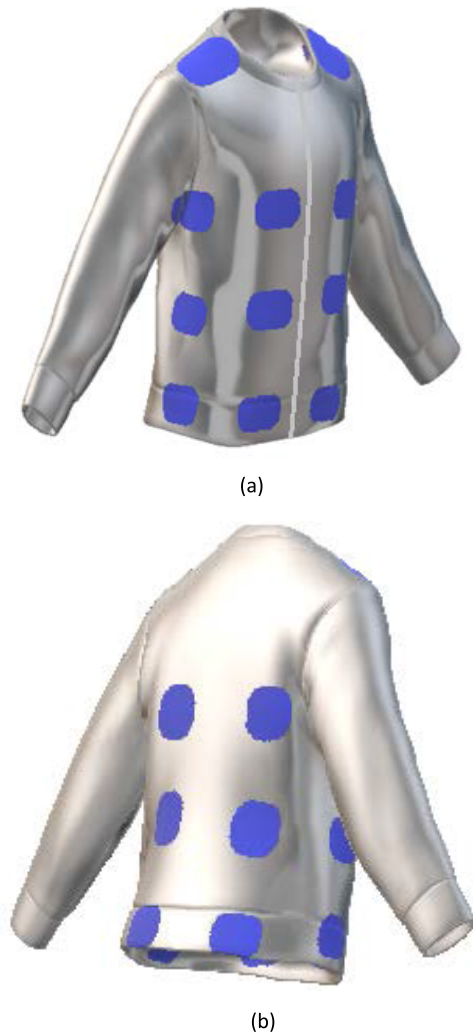


FIGURE 1. (a) Front view of security jacket and (b) back view of security jacket.

II. SYSTEM MODEL AND PROPOSED SOLUTION

In this study, it is assumed that a jacket which has multiple wireless sensors on the inner surface is designed as in Fig. 1. This jacket is assumed to be as a faraday cage structure. In this way, going out of the signals transmitted inside the jacket and entering of the incoming signals from outside are minimized. In this study, calculations and performance evaluations have performed with 20 sensors. This number can be further increased. These wireless sensors are

wired together and this connection structure is grid-shaped. There is a main signal processor responsible for management including combining, beamforming, extraction from jamming etc.

It is assumed that the MICS band is used as the transmission frequency in this study. Because Federal communication commission (FCC) has assigned a frequency band between 402 MHz and 405 MHz which is called as MICS band for the communication of IMD systems [21]. This band is more convenient for propagating of the signals in human body with the international acceptability [22]. Consequently, sensors with their antennas are mounted at a distance of at least $1/4$ wavelength apart (nearly 18 cm) each other. This amount of spatial separation improves the probability that at least one sensor is not in a deeply faded signal condition. For this reason, it is planned that approximately 20 sensors have been placed at around 18 cm intervals on the Security Jacket.

In vivo wireless communication channel, small-scale fading (like Rayleigh fading) is observed due to the reflections of biological tissues inside the human body lead to multipath propagation as indicated in [23]. In vivo channels are also known as fading channels. In this study, popular non-line of sight Rayleigh fading (small-scale fading) channel is used.

In wireless communication, diversity is needed in fading channels. In this study, antenna diversity option is preferred; SIMO and MISO structure is set up. Because antenna diversity provides performance gain in all fading channels. As in [24], MIMO technology (similar to SIMO and MISO) provides significant performance gain against single input single output (SISO) structure.

Wireless secure communication takes place between IMD and the sensors and this secure communication in both ways is detailed under two headings.

A. SECURE TRANSMISSION FROM IMD-SIMO STRUCTURE

When transmission from the IMD to the sensors occurs, communication takes place in the SIMO structure. In the Fig. 2, there is a 2-dimensional cross-sectional view (only one layer) of security jacket with the sensors. On this cross-section, it is shown that all the sensors jam the IMD reply. Eavesdropper also receives jamming signals along with the IMD reply.

To ensure security, all sensors have the ability to perform jamming at the same time as the receiving. When transmission occurs from IMD at each time interval, each sensor switches to active jamming-mode or off-mode randomly when receiving IMD replies. In Fig. 3, it is seen an example of a scenario of transmission on security jacket which is horizontally sliced. Jamming of IMD reply by some sensors selected randomly and IMD reply reception by all the sensors in SIMO mode in a time interval occur.

In wireless communication, receiver diversity is a form of space diversity, where there are multiple antennas at

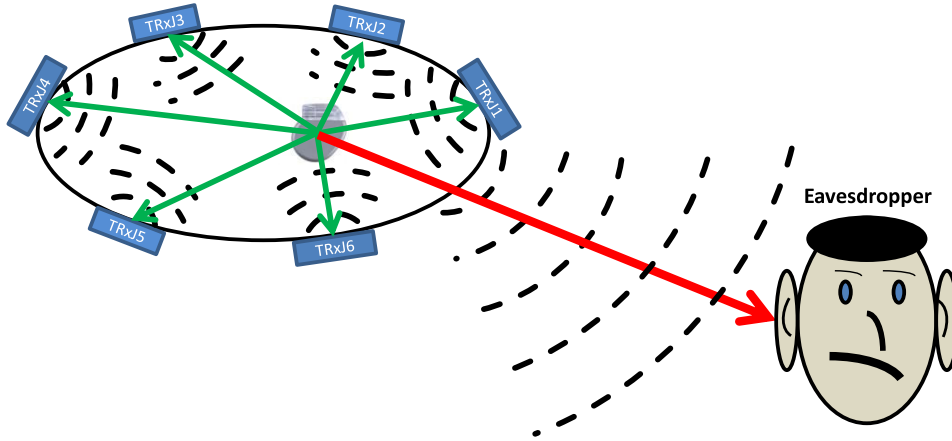


FIGURE 2. A 2D cross-sectional view of security jacket with SIMO transmission and jamming.

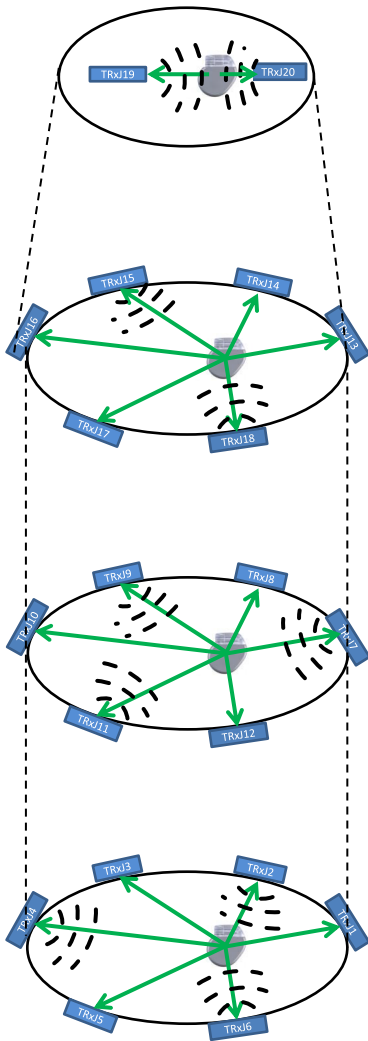


FIGURE 3. A scenario of jamming of IMD reply with randomly selected sensors.

the receiver. Expressing the received signal in a vector form, it is

$$\bar{y} = \bar{h}x + \bar{n} \quad (1)$$

where $\bar{y}$ is the received vector which expresses the symbols obtained on all receive antennas, $\bar{h}$ is the channel vector which contains the channel coefficients for all branches between the transmit antenna and receive antennas, x is the transmitted symbol and $\bar{n}$ is the noise vector which expresses the additive noises on all receive antennas. The received signal considering each signal on each receiver antenna is

$$\begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_k \end{bmatrix} = \begin{bmatrix} h_1 \\ h_2 \\ \vdots \\ h_k \end{bmatrix} x + \begin{bmatrix} n_1 \\ n_2 \\ \vdots \\ n_k \end{bmatrix} \quad (2)$$

where k is the total number of the antennas on receiver. It is assumed that all elements of channel vector and noise vector are independent.

In receiver diversity, Maximum Ratio Combining (MRC) technique has the best performance when compared with Selection Diversity and Equal Gain Combining (EGC) [25]. MRC may involve more complexity, but adding complexity to the sensors on the security jacket does not create problems, rather than IMD. Therefore, MRC has been preferred. Optimal weight vector used for combining is defined as

$$\bar{w} = \frac{\bar{h}}{\|\bar{h}\|} = \frac{1}{\sqrt{|h_1|^2 + |h_2|^2 + \dots + |h_k|^2}} \begin{bmatrix} h_1 \\ h_2 \\ \vdots \\ h_k \end{bmatrix} \quad (3)$$

where $\|\cdot\|$ denotes norm of the vector [26]. The output of the MRC is

$$\tilde{y} = \bar{w}^H \bar{y} = \bar{w}^H \bar{h}x + \bar{w}^H \bar{n} = \frac{\bar{h}^H \bar{y}}{\|\bar{h}\|} = \|\bar{h}\| x + \bar{w}^H \bar{n} \quad (4)$$

where H denotes Hermitian transpose of the vector. The combined and equalized symbol is finally obtained by the

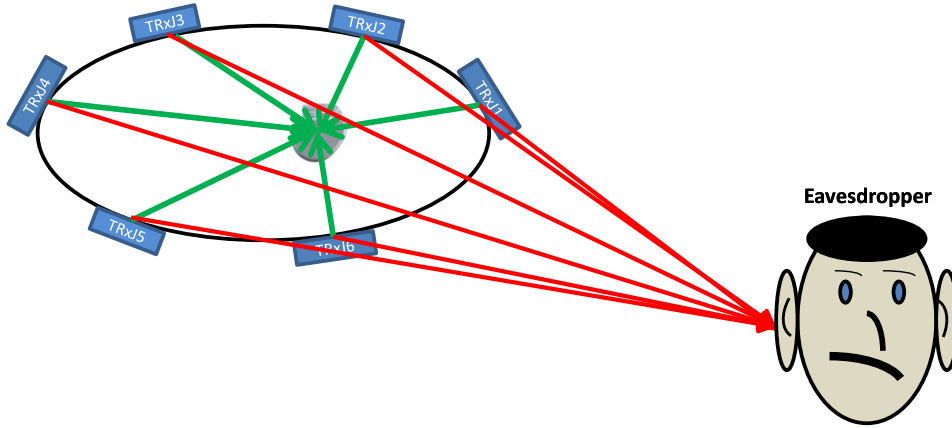


FIGURE 4. 2D cross-sectional view of security jacket with MISO transmission.

equation below.

$$\tilde{x} = \frac{\tilde{y}}{\|h\|} = \frac{\bar{w}^H \tilde{y}}{\|\bar{w}\|} = \frac{\bar{h}^H \tilde{y}}{\|\bar{h}\|^2} = x + \frac{\bar{w}^H \bar{n}}{\|h\|} \quad (5)$$

Taking into account the above theoretical background, IMD replies or signals received by all sensors are combined by the main processor. But this processor also discards all jamming signals. Expressing the received signal in a vector form, it is

$$\bar{y} = \bar{h}_{IMD}x + H_J \bar{s}_J + \bar{n} \quad (6)$$

where $\bar{y}$ is the received vector which expresses the symbols obtained on all sensors, $\bar{h}_{IMD}$ is the channel vector which expresses the channel coefficients between the IMD and all sensors, x is the symbol transmitted by IMD, H_J is the channel matrix which considers the channel coefficients between the sensors, $\bar{s}_J$ is the jamming vector which considers on-off switched jamming signals transmitted by all the sensors and $\bar{n}$ is the noise vector which expresses the additive noises on all sensors. Expressing the received signal detailed, it is

$$\begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_k \end{bmatrix} = \begin{bmatrix} h_{IMD1} \\ h_{IMD2} \\ \vdots \\ h_{IMDk} \end{bmatrix} x + \begin{bmatrix} 1 & h_{j12} & \dots & h_{j1k} \\ h_{j21} & 1 & \dots & h_{j2k} \\ \vdots & \vdots & \ddots & \vdots \\ h_{jk1} & h_{jk2} & \dots & 1 \end{bmatrix} \begin{bmatrix} s_{j1} \\ s_{j2} \\ \vdots \\ s_{jk} \end{bmatrix} + \begin{bmatrix} n_1 \\ n_2 \\ \vdots \\ n_k \end{bmatrix} \quad (7)$$

Each element of column vector $\bar{s}_J$ is switched to zero or jamming signal randomly in each time interval. Diagonal channel coefficients have been taken '1' because the received

jamming signal produced by the same sensor. The jamming based noise or distortion vector is shown more clearly below.

$$\begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_k \end{bmatrix} = \begin{bmatrix} h_{IMD1} \\ h_{IMD2} \\ \vdots \\ h_{IMDk} \end{bmatrix} x + \begin{bmatrix} s_{j1} + h_{j12}s_{j2} + \dots + h_{j1k}s_{jk} \\ h_{j21}s_{j1} + s_{j2} + \dots + h_{j2k}s_{jk} \\ \vdots \\ h_{jk1}s_{j1} + h_{jk2}s_{j2} + \dots + s_{jk} \end{bmatrix} + \begin{bmatrix} n_1 \\ n_2 \\ \vdots \\ n_k \end{bmatrix} \quad (8)$$

and the received signal in the eavesdropper is obtained similarly as

$$y_{eve} = h_{imd_{eve}}x + h_{j1_{eve}}s_{j1} + h_{j2_{eve}}s_{j2} + \dots + h_{jk_{eve}}s_{jk} + n_{eve} \quad (9)$$

Using Eq. 5, it is possible to obtain the combined and equalized symbol by the equation below by the main processor.

$$\tilde{x} = \frac{\bar{h}_{IMD}^H (\bar{y} - H_J \bar{s}_J)}{\|\bar{h}_{IMD}\|^2} \quad (10)$$

B. SECURE TRANSMISSION TO IMD-MISO STRUCTURE

When transmitting from sensors to the IMD, communication takes place in the MISO structure. In the Fig. 4, there is a 2-dimensional cross-sectional view (only one layer) of security jacket with the sensors. On this cross-section, it is shown that all the sensors transmit to the IMD. Eavesdropper also receives the signals of all sensors.

To ensure security, sensors have the ability to switch transmit beamforming and spoofing mode randomly. When transmission occurs to IMD at each time interval, each sensor switches to transmit beamforming or spoofing

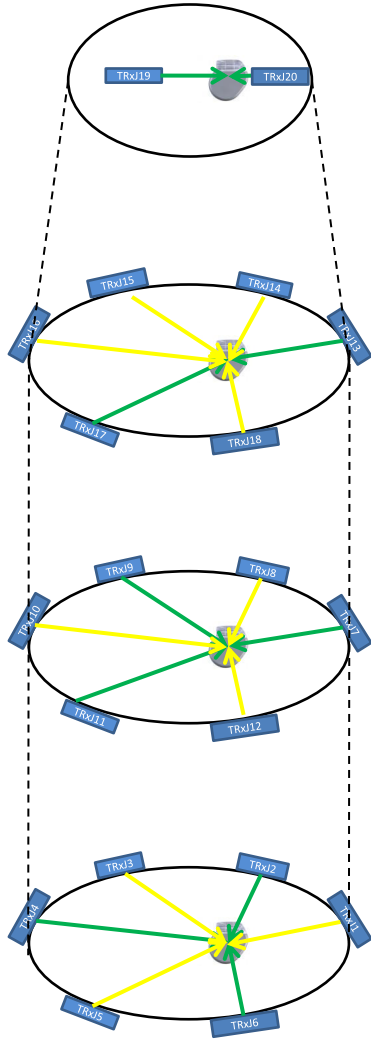


FIGURE 5. A scenario of IMD reception with randomized transmit beamforming.

mode randomly. In Fig.5, it is seen an example of a MISO transmission scenario on security jacket which is horizontally sliced. Some of the sensors on transmit beamforming mode and the others are in spoofing mode and IMD reception in a time interval occurs.

In wireless communication, transmit beamforming is a form of space diversity, where there are multiple antennas at the transmitter and one antenna at the receiver. The received signal can be defined as follows,

$$y = \bar{h}^H \bar{x} + n \quad (11)$$

where y is the received signal which expresses the symbol obtained on receive antenna, $\bar{h}^H$ is the Hermitian of the channel vector which expresses the channel coefficients for all branches to receive antenna, $\bar{x}$ is the transmitted vector considering the symbols for all branches and n is the noise signal which expresses the additive noise on receive antenna.

The detailed received signal on receiver antenna is

$$y = [h_1 \ h_2 \ \dots \ h_k] \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{bmatrix} + n \quad (12)$$

where k is the total number of the antennas on transmitter. It is assumed that all elements of channel vector and noise is independent. The received signal can be redefined as

$$y = h_1 x_1 + h_2 x_2 + \dots + h_k x_k + n \quad (13)$$

Transmit beamformed signal is as in [26]

$$\bar{x} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{bmatrix} = \frac{\bar{h}^H x}{\|\bar{h}\|} = \frac{1}{\|\bar{h}\|} \begin{bmatrix} h_1^* \\ h_2^* \\ \vdots \\ h_k^* \end{bmatrix} x \quad (14)$$

where x is the transmitted symbol and $\|\cdot\|$ denotes norm of the vector. Transmit beamformed signal is again

$$\bar{x} = \frac{1}{\sqrt{|h_1|^2 + |h_2|^2 + \dots + |h_k|^2}} \begin{bmatrix} h_1^* \\ h_2^* \\ \vdots \\ h_k^* \end{bmatrix} x$$

$$= \begin{bmatrix} \frac{h_1^* x}{\sqrt{|h_1|^2 + |h_2|^2 + \dots + |h_k|^2}} \\ \frac{h_2^* x}{\sqrt{|h_1|^2 + |h_2|^2 + \dots + |h_k|^2}} \\ \vdots \\ \frac{h_k^* x}{\sqrt{|h_1|^2 + |h_2|^2 + \dots + |h_k|^2}} \end{bmatrix} \quad (15)$$

Using Equ. 13, 14 and 15, the detailed received signal on receiver antenna is again

$$y = h_1 \frac{h_1^* x}{\sqrt{|h_1|^2 + |h_2|^2 + \dots + |h_k|^2}} + h_2 \frac{h_2^* x}{\sqrt{|h_1|^2 + |h_2|^2 + \dots + |h_k|^2}} + \dots + h_k \frac{h_k^* x}{\sqrt{|h_1|^2 + |h_2|^2 + \dots + |h_k|^2}} + n$$

$$= \frac{|h_1|^2 x}{\sqrt{|h_1|^2 + |h_2|^2 + \dots + |h_k|^2}} + \frac{|h_2|^2 x}{\sqrt{|h_1|^2 + |h_2|^2 + \dots + |h_k|^2}} + \dots + \frac{|h_k|^2 x}{\sqrt{|h_1|^2 + |h_2|^2 + \dots + |h_k|^2}} + n \quad (16)$$

Equation is as follows in the simplest form.

$$y = \left(\sqrt{|h_1|^2 + |h_2|^2 + \dots + |h_k|^2} \right) x + n$$

$$= \|\bar{h}\| x + n \quad (17)$$

The equalized symbol is finally obtained by the equation below.

$$\tilde{x} = \frac{y}{\|\bar{h}\|} \quad (18)$$

Taking into account the above theoretical background, for example, randomized spoofing-based transmit beamformed signal vector by all sensors can be given below similar to Equ. 15.

$$\tilde{x} = \begin{bmatrix} x_1 \\ \frac{h_2^* x}{\sqrt{|h_2|^2 + |h_3|^2 + |h_6|^2 + \dots + |h_k|^2}} \\ \frac{h_3^* x}{\sqrt{|h_2|^2 + |h_3|^2 + |h_6|^2 + \dots + |h_k|^2}} \\ x_4 \\ x_5 \\ \frac{h_6^* x}{\sqrt{|h_2|^2 + |h_3|^2 + |h_6|^2 + \dots + |h_k|^2}} \\ \vdots \\ \frac{h_k^* x}{\sqrt{|h_2|^2 + |h_3|^2 + |h_6|^2 + \dots + |h_k|^2}} \end{bmatrix} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ \vdots \\ x_k \end{bmatrix} \quad (19)$$

where x_1 , x_4 and x_5 are determined as artificial noise by verifying the following equation. The equation below can be obtained in order to spoof eavesdropper according to this example.

$$h_1 x_1 + h_4 x_4 + h_5 x_5 = 0 \quad (20)$$

The received signal on IMD is

$$y_{IMD} = h_1 x_1 + h_2 x_2 + h_3 x_3 + h_4 x_4$$

$$+ h_5 x_5 + h_6 x_6 + \dots + h_k x_k + n$$

$$= h_2 x_2 + h_3 x_3 + h_6 x_6 + \dots + h_k x_k + n \quad (21)$$

The detailed received signal on IMD is

$$y_{IMD} = \frac{|h_2|^2 x}{\sqrt{|h_2|^2 + |h_3|^2 + |h_6|^2 + \dots + |h_k|^2}}$$

$$+ \frac{|h_3|^2 x}{\sqrt{|h_2|^2 + |h_3|^2 + |h_6|^2 + \dots + |h_k|^2}}$$

$$+ \frac{|h_6|^2 x}{\sqrt{|h_2|^2 + |h_3|^2 + |h_6|^2 + \dots + |h_k|^2}} + \dots$$

$$+ \frac{|h_k|^2 x}{\sqrt{|h_2|^2 + |h_3|^2 + |h_6|^2 + \dots + |h_k|^2}} + n \quad (22)$$

Equation is as follows in the simplest form for this example.

$$y_{IMD} = \left(\sqrt{|h_2|^2 + |h_3|^2 + |h_6|^2 + \dots + |h_k|^2} \right) x + n \quad (23)$$

The equalized symbol can be obtained by the equation below if the IMD could be touched. But BER calculation is done by IMD according to the received signal as in Equ. 23.

$$\tilde{x} = \frac{y_{IMD}}{\sqrt{|h_2|^2 + |h_3|^2 + |h_6|^2 + \dots + |h_k|^2}} \quad (24)$$

The received signal in the eavesdropper is obtained using spoofed signal x_1 , x_4 and x_5 , for this example, similarly as

$$y_{eve} = \bar{h}_{eve}^H \tilde{x} + n$$

$$= [h_{eve1} h_{eve2} \dots h_{evek}] \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{bmatrix} + n$$

$$= h_{eve1} x_1$$

$$+ h_{eve2} \frac{h_2^* x}{\sqrt{|h_2|^2 + |h_3|^2 + |h_6|^2 + \dots + |h_k|^2}}$$

$$+ h_{eve3} \frac{h_3^* x}{\sqrt{|h_2|^2 + |h_3|^2 + |h_6|^2 + \dots + |h_k|^2}}$$

$$+ h_{eve4} x_4$$

$$+ h_{eve5} x_5$$

$$+ h_{eve6} \frac{h_6^* x}{\sqrt{|h_2|^2 + |h_3|^2 + |h_6|^2 + \dots + |h_k|^2}} + \dots$$

$$+ h_{evek} \frac{h_k^* x}{\sqrt{|h_2|^2 + |h_3|^2 + |h_6|^2 + \dots + |h_k|^2}} + n \quad (25)$$

III. PERFORMANCE EVALUATION

Performance results of the proposed solution are given in this section. According to the proposed technique, bit error ratio (BER) performance is shown in terms of signal to noise ratio (SNR) according to the simulations.

In this solution, it is assumed that sensors on the jacket are very close to IMD. But sensors on the jacket or IMD are far away from eavesdropper. Because of distance and faraday structure, it is also shown that the attenuation on signals reaching eavesdropper is too much. FSK modulation is also used because it is the most preferred modulation type in IMD communication.

Typical materials used for electromagnetic shielding include sheet metal, metal screen, and metal foam. The texture of the security jacket is assumed to be flexible, thin and lightweight as metal foam. It is also assumed that from outside of the jacket it is not possible to understand which sensor or sensors in active transmission mode (transmitting symbol or jamming signal) or not. Furthermore, the main purpose assumed in this study is to create a reflective environment for sensors and IMD signals in the jacket, while reducing electromagnetic emissions by implementing electromagnetic shielding. Thus, it will not be possible to separate the signals reflected from the arm and head holes.

Fig. 6 shows the BER performance of randomly selected some sensors and eavesdropper when transmission takes

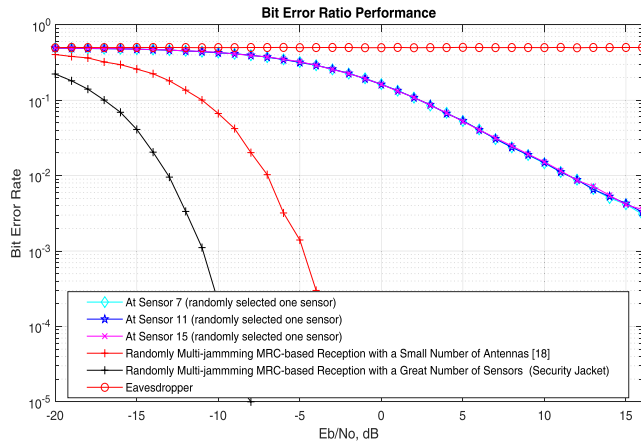


FIGURE 6. BER performance of some individual sensors, randomly multi-jamming/extraction with MRC-based reception, and eavesdropper when transmissions occur from the IMD.

place from the IMD. Because eavesdropper does not have knowledge which sensor or sensors jam transmissions by IMD in each time interval and also has no way to discard jamming signals, even his or her SNR is high, BER is still very high, i.e., around 0.5. But all the sensors have the capability to decode and discard jamming signal coming from any sensor. Therefore, all the sensors discard the jamming signal or signals and get unblended transmitted signals of IMD in each time interval. When SNR increases in the individual sensors, BER decreases as in Fig. 6. But when randomly multi-jamming and MRC-based reception is performed, BER performance is getting better. There are three jamming and six receiver antennas in the proposed solution in [18], but security jacket solution has 20 sensors and all the sensors have the capability of jamming and receiving synchronously in this solution. Therefore, when compared to [18], the BER performance of the security jacket is outperforms the previous one. It can also be understood that the IMD's transmission power could be reduced tremendously with the large number of sensors.

In wireless communication, the meaning of the SNR is the signal power to noise power ratio. Reducing SNR also means reducing the transmission power. Reducing transmission power means longer battery life. Figure 6 also shows that a lower SNR value is sufficient for the same BER value with Security Jacket solution and this means that lower transmission signal power is needed. Lower transmission signal power also means longer battery life for IMD. Due to the limited battery life, the average time to change of IMDs is about ten years and this change requires patients to be operated every ten years. This solution offers longer battery life and less rare surgery.

Fig. 7 shows the BER performance of IMD and eavesdropper positioned anywhere around the patient when transmissions occur to the IMD. Eavesdropper does not have knowledge which sensor or sensors are in transmitting (beamforming based) or spoofing mode in each time interval and he or she has no knowledge of channel coefficients between

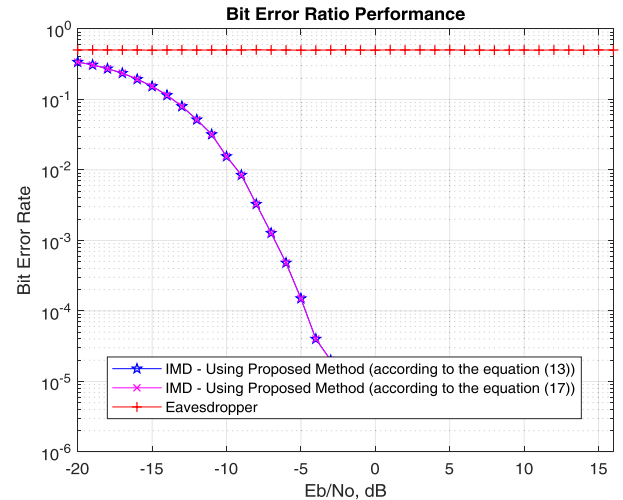


FIGURE 7. BER performance of randomized spoofing-based transmit beamforming reception and eavesdropper when transmissions occur to the IMD.

the sensors and IMD. Therefore, even its SNR is high, BER is still very high, i.e., around 0.5. But when SNR increases in IMD, BER decreases with randomized spoofing-based transmit beamforming.

IV. CONCLUSION

In this paper, a new protector compatible with already implanted unsecure systems has been proposed by providing full-duplex secure communication of wireless IMDs. This new protector is externally worn jacket and, therefore, called Security Jacket. However, in order to provide physical layer security, some advanced sensors have been placed on the jacket. In this method, randomly multi-jamming and extraction with a great number of sensors and MRC reception by all the sensors are employed when transmissions coming from the IMD occur. Randomized spoofing-based transmit beamforming technique is applied when reception by IMD is performed. This protector also provides power efficiency and supports extended battery life. The number of sensors may be increased when they are optimum positioned with a different placement by adding arm areas. This would be future work.

REFERENCES

- [1] J. Choi, J. Ha, and H. Jeon, "Physical layer security for wireless sensor networks," in *Proc. IEEE 24th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Sep. 2013, pp. 1–6.
- [2] T. Pecorella, L. Brilli, and L. Mucchi, "The role of physical layer security in IoT: A novel perspective," *Information*, vol. 7, no. 3, p. 49, 2016.
- [3] S. Soderi, L. Mucchi, M. Hämäläinen, A. Piva, and J. Iinatti, "Physical layer security based on spread-spectrum watermarking and jamming receiver," *Trans. Emerg. Telecommun. Technol.*, vol. 28, no. 7, p. e3142, 2017.
- [4] N. Zhao *et al.*, "Authentication in millimeter-wave body-centric networks through wireless channel characterization," *IEEE Trans. Antennas Propag.*, vol. 65, no. 12, pp. 6616–6623, Dec. 2017.
- [5] N. Zhao *et al.*, "Double threshold authentication using body area radio channel characteristics," *IEEE Commun. Lett.*, vol. 20, no. 10, pp. 2099–2102, Oct. 2016.
- [6] S. Kulaç, M. H. Sazli, and H. G. Ilk, "External relaying based security solutions for wireless implantable medical devices: A review," in *Proc. 11th IFIP Wireless Mobile Netw. Conf. (WMNC)*, Sep. 2018, pp. 1–4.

- [7] G. Zheng, R. Shankaran, M. A. Orgun, L. Qiao, and K. Saleem, "Ideas and challenges for securing wireless implantable medical devices: A review," *IEEE Sensors J.*, vol. 17, no. 3, pp. 562–576, Feb. 2017.
- [8] H. Rathore, A. Mohamed, A. Al-Ali, X. Du, and M. Guizani, "A review of security challenges, attacks and resolutions for wireless medical devices," in *Proc. 13th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2017, pp. 1495–1501.
- [9] R. Altawy and A. M. Youssef, "Security tradeoffs in cyber physical systems: A case study survey on implantable medical devices," *IEEE Access*, vol. 4, pp. 959–979, 2016.
- [10] T. Denning, K. Fu, and T. Kohno, "Absence makes the heart grow fonder: New directions for implantable medical device security," in *Proc. 3rd Conf. Hot Topics Secur. (HOTSEC)*, Berkeley, CA, USA, 2008, pp. 5:1–5:7.
- [11] F. Xu, Z. Qin, C. C. Tan, B. Wang, and Q. Li, "Imdguard: Securing implantable medical devices with the external wearable guardian," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 1862–1870.
- [12] M. Zhang, A. Raghunathan, and N. Jha, "MedMon: Securing medical devices through wireless monitoring and anomaly detection," *IEEE Trans. Biomed. Circuits Syst.*, vol. 7, no. 6, pp. 871–881, Dec. 2013.
- [13] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They can hear your heartbeats: Non-invasive security for implantable medical devices," *SIGCOMM Comput. Commun. Rev.*, vol. 41, no. 4, pp. 2–13, Aug. 2011.
- [14] D. Halperin *et al.*, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2008, pp. 129–142.
- [15] M. Zhang, A. Raghunathan, and N. K. Jha, "Trustworthiness of medical devices and body area networks," *Proc. IEEE*, vol. 102, no. 8, pp. 1174–1188, Aug. 2014.
- [16] S. Kulaç, M. H. Yilmaz, and H. Arslan, "Secure transmission of commands using multicarrier structure for wireless implantable medical devices," in *Proc. 24th Signal Process. Commun. Appl. Conf. (SIU)*, May 2016, pp. 737–740.
- [17] S. Kulaç, "Medikal implant haberleşme sistemleri için bandgenişliği verimli örtüşmeli fsk kodlamalı güvenli komut iletimi," *Gazi Üniversitesi Fen Bilimleri Dergisi C, Tasarım Ve Teknoloji*, vol. 6, no. 2, p. 250–258, 2018.
- [18] S. Kulaç, "Security belt for wireless implantable medical devices," *J. Med. Syst.*, vol. 41, no. 11, p. 172, Sep. 2017.
- [19] Y.-H. Liu, C.-J. Tung, and T.-H. Lin, "A low-power asymmetrical mics wireless interface and transceiver design for medical imaging," in *Proc. IEEE Biomed. Circuits Syst. Conf. (BioCAS)*, Nov./Dec. 2006, pp. 162–165.
- [20] K. Zhu, M. R. Haider, S. Yuan, and S. K. Islam, "A Sub-1 μ A low-power FSK modulator for biomedical sensor circuits," in *Proc. IEEE Comput. Soc. Annu. Symp. VLSI (ISVLSI)*, Jul. 2010, pp. 265–268.
- [21] *MICS Medical Implant Communication Services, FCC 47 CFR 95.601–95.673 Subpart E/I Rules for Medradio Services*, Federal Communications Commission, Washington, DC, USA, 1999.
- [22] *Sharing Between the Meteorological Aids Services and Medical Implant Communication Systems (MICS) Operating in the Mobile Service in the Frequency Band 401–406 MHz*, document ITU-R Rec. RS.1346, 1998.
- [23] A. F. Demir *et al.*, "Anatomical region-specific *in vivo* wireless communication channel characterization," *IEEE J. Biomed. Health Inform.*, vol. 21, no. 5, pp. 1254–1262, Sep. 2017.
- [24] C. He, Y. Liu, T. P. Ketterl, G. E. Arrobo, and R. D. Gitlin, "MIMO *in vivo*," in *Proc. WAMICON*, Jun. 2014, pp. 1–4.
- [25] T. S. Rappaport, *Wireless Communications: Principles and Practice*, 2nd ed. Upper Saddle River, NJ, USA: Prentice-Hall, 2001.
- [26] J. R. Barry, E. A. Lee, and D. G. Messerschmitt, *MIMO Communications*. Boston, MA, USA: Springer, 2004, pp. 461–536.



SELMAN KULAÇ was born in Düzce, Turkey, in 1980. He received the bachelors' degree, the master's degree, and the Ph.D. degree from the Electronics Engineering Department, Ankara University, in 2002, 2004, and 2012, respectively. He has been an Assistant Professor with the Electrical Electronics Engineering Department, Düzce University, since 2012. His research interests include cognitive radio, wireless implantable medical devices, and massive MIMO.

...