They Can Hear Your Heartbeats: Non-Invasive Security for Implantable Medical Devices

Shyamnath Gollakota [†] Haitham Hassanieh[†] Benjamin Ransford[⋆] Dina Katabi[†] Kevin Fu[⋆]
[†]Massachusetts Institute of Technology
{gshyam, haithamh, dk}@mit.edu
[⋆]University of Massachusetts, Amherst
{ransford, kevinfu}@cs.umass.edu

ABSTRACT

Wireless communication has become an intrinsic part of modern implantable medical devices (IMDs). Recent work, however, has demonstrated that wireless connectivity can be exploited to compromise the confidentiality of IMDs' transmitted data or to send unauthorized commands to IMDs—even commands that cause the device to deliver an electric shock to the patient. The key challenge in addressing these attacks stems from the difficulty of modifying or replacing already-implanted IMDs. Thus, in this paper, we explore the feasibility of protecting an implantable device from such attacks without modifying the device itself. We present a physical-layer solution that delegates the security of an IMD to a personal base station called the *shield*. The shield uses a novel radio design that can act as a jammer-cum-receiver. This design allows it to jam the IMD's messages, preventing others from decoding them while being able to decode them itself. It also allows the shield to jam unauthorized commands—even those that try to alter the shield's own transmissions. We implement our design in a software radio and evaluate it with commercial IMDs. We find that it effectively provides confidentiality for private data and protects the IMD from unauthorized commands.

Categories and Subject Descriptors C.2.2 [**Computer Systems Organization**]: Computer-Communications Networks

General Terms Algorithms, Design, Performance, Security

Keywords Full-duplex, Implanted Medical Devices, Wireless

1. INTRODUCTION

The past few years have produced innovative health-oriented networking and wireless communication technologies, ranging from low-power medical radios that harvest body energy [25] to wireless sensor networks for in-home monitoring and diagnosis [49, 53]. Today, such wireless systems have become an intrinsic part of many modern medical devices [37]. In particular, implantable medical devices (IMDs), including pacemakers, cardiac defibrillators, insulin pumps, and neurostimulators all feature wireless communication [37]. Adding wireless connectivity to IMDs has enabled remote monitoring of patients' vital signs and improved care providers' ability to deliver timely treatment, leading to a better health care system [29].

Recent work, however, has shown that such wireless connectivity can be exploited to compromise the confidentiality of the IMD's transmitted data or to send the IMD unauthorized commands—even commands that cause the IMD to deliver an electric shock to the patient [19, 20]. In other systems, designers use cryptographic methods to provide confidentiality and prevent unauthorized access. However, adding cryptography *directly* to IMDs themselves is difficult for the following reasons:

- *Inalterability:* In the U.S. alone, there are millions of people who already have wireless IMDs, and about 300,000 such IMDs are implanted every year [56]. Once implanted, an IMD can last up to 10 years [12], and replacing it requires surgery that carries risks of major complications. Incorporating cryptographic mechanims into existing IMDs may be infeasible because of limited device memory and hence can only be achieved by replacing the IMDs. This is not an option for people who have IMDs or may acquire them in the near future.
- *Safety:* It is crucial to ensure that health care professionals always have immediate access to an implanted device. However, if cryptographic methods are embedded in the IMD itself, the device may deny a health care provider access unless she has the right credentials. Yet, credentials might not be available in scenarios where the patient is at a different hospital, the patient is unconscious, or the cryptographic key storage is damaged or unreachable [20, 29]. Inability to temporarily adjust or disable an IMD could prove fatal in emergency situations.[1]
- *Maintainability:* Software bugs are particularly problematic for IMDs because they can lead to device recalls. In the last eight years, about 1.5 million software-based medical devices were recalled [13]. Between 1999 and 2005, the number of recalls of software-based medical devices more than doubled; more than 11% of all medical-device recalls during this time period were attributed to software failures [13]. Such recalls are costly and could require surgery if the model is already implanted. Thus, it is desirable to limit IMDs' software to only medically necessary functions.

This paper explores the feasibility of protecting IMDs *without modifying them* by implementing security mechanisms entirely on an external device. Such an approach enhances the security of IMDs for patients who already have them, empowers medical personnel to access a protected IMD by removing the external device or powering it off, and does not in itself increase the risk of IMD recalls.

[1] Note that distributing the credentials widely beyond the patient's primary health care providers increases the probability of the key being leaked and presents a major key revocation problem.

SIGCOMM'11, August 15–19, 2011, Toronto, Ontario, Canada.

We present a design in which an external device, called the *shield*, is interposed between the IMD and potential counterparties—e.g., worn on the body near an implanted device. The shield acts as a gateway that relays messages between the IMD and authorized endpoints. It uses a novel physical-layer mechanism to secure its communication with the IMD, and it uses a standard cryptographic channel to communicate with other authorized endpoints.

The shield counters two classes of adversarial actions: passive eavesdropping that threatens the confidentiality of the IMD's transmissions, and active transmission of unauthorized radio commands to the IMD. First, to provide confidentiality for the IMD's transmissions, the shield continuously listens for those transmissions and jams them so that they cannot be decoded by eavesdroppers. The shield uses a novel radio design to simultaneously receive the IMD's signal and transmit a jamming signal. The shield then transmits the IMD's signal to an authorized endpoint using standard cryptographic techniques. Second, to protect the IMD against commands from unauthorized endpoints, the shield listens for unauthorized transmissions addressing the IMD and jams them. As a result of jamming, the IMD cannot decode the adversarial transmissions, and hence the adversary fails to make the IMD execute an unauthorized command.

A key challenge that we had to overcome to realize this architecture is to design a small wearable radio that simultaneously jams the IMD's signal and receives it. We build on prior work in the area of full-duplex radio design, which enables a single node to transmit and receive simultaneously. However, the state-of-the-art design for full-duplex radios [3] yields large devices unsuitable for our application. Specifically, it exploits the property that a signal reverses its phase every half a wavelength; it transmits the same signal from two antennas and puts a receive antenna *exactly* half a wavelength closer to one of the transmit antennas than the other. An antenna separation of half a wavelength, however, is unsuitable for our context: the IMDs we consider operate in the 400 MHz band [11] with a wavelength of about 75 cm. A shield that requires the antennas to be rigidly separated by exactly half a wavelength (37.5 cm) challenges the notion of wearability and therefore patient acceptability.

This paper presents a full-duplex radio that does not impose restrictions on antenna separation or positioning, and hence can be built as a small wearable device. Our design uses two antennas: a jamming antenna and a receive antenna. The jamming antenna transmits a random signal to prevent eavesdroppers from decoding the IMD's transmissions. However, instead of relying on a particular positioning to cancel the jamming signal at the receive antenna, we connect the receive antenna simultaneously to both a transmit and a receive chain. We then make the transmit chain send an *antidote* signal that cancels the jamming signal at the receive antenna's front end, allowing it to receive the IMD's signal and decode it. The resulting design does not restrict antenna separation and can therefore be built as a wearable radio.

Our design has additional desirable features. Specifically, because the shield can receive while jamming, it can detect adversaries who try to alter the shield's signal to convey unauthorized messages to the IMD. It can also ensure that it stops jamming the medium when an adversarial signal ends, allowing legitimate devices to communicate.

We have implemented a prototype of our design on USRP2 software radios [7]. We use 400 MHz daughterboards for compatibility with the 402–405 MHz Medical Implant Communication Services (MICS) band used by IMDs [11]. We evaluate our prototype shield against two modern IMDs, namely the Medtronic Virtuoso implantable cardiac defibrillator (ICD) [35] and the Concerto cardiac resynchronization therapy device (CRT) [34]. Our evaluation reveals the following:

- When the shield is present, it jams the IMD's messages, causing even nearby (20 cm away) eavesdroppers to experience a bit error rate of nearly 50%, which is no better than a random guess.
- When the shield jams the IMD's packets, it can still reliably decode them (the packet loss rate is 0.2%, which is negligible). We conclude that the shield and the IMD share an information channel that is inaccessible to other parties.
- When the shield is absent, the IMD replies to unauthorized commands, even if the adversary is in a non-line-of-sight location more than 14 m away, and uses a commercial device that operates in the MICS band and adheres to the FCC power limit.
- When the shield is present and has the same transmit power as the adversary, the IMD does not respond to unauthorized commands, even when the adversary is only 20 cm away.
- When the shield is absent and an adversary with 100 times the shield's power transmits unauthorized commands, the IMD responds from distances as large as 27 m. When the shield is present, however, the high-powered adversary's attempts succeed only from distances less than 5 m, and only in line-of-sight locations. The shield always detects high-powered adversarial transmissions and raises an alarm. We conclude that sufficiently high-powered adversaries present an intrinsic limitation to our physical-layer protection mechanism. However, the shield's presence reduces the adversary's success range and informs the patient, raising the bar for the adversary's attempts.

The shield is, to our knowledge, the first system that simultaneously provides confidentiality for IMDs' transmissions and protects IMDs against commands from unauthorized parties *without requiring any modification to the IMDs themselves*. Further, because it affords physical-layer protection, it may also help provide a complementary defense-in-depth solution to devices that feature cryptographic or other application-layer protection mechanisms.

Disclaimer. Operating a jamming device has legal implications that vary by jurisdiction and frequency band. The definition of jamming also depends on both context and intent. Our experiments were conducted in tightly controlled environments where no patients were present. Further, the intent of a shield is never to interfere with communications that do not involve its protected IMD. We recommend that anyone considering deployment of technology based on this research consult with their own legal counsel.

2. IMD COMMUNICATION PRIMER

Wireless communication appears in a wide range of IMDs, including those that treat heart failure, diabetes, and Parkinson's disease. Older models communicated in the 175 KHz band [20]. However, in 1999, the FCC set aside the 402–405 MHz band for medical implant communication services (MICS) [11]. The MICS band was considered well suited for IMDs because of its international availability for this purpose [8], its signal propagation characteristics in the human body, and its range of several meters that allows remote monitoring. Modern IMDs communicate medical information in the MICS band, though devices may use other bands for activation (e.g., 2.4 GHz or 175 KHz) [43]. IMDs share the MICS band with meteorological systems on a secondary basis and should ensure that their usage of it does not interfere with these systems. The FCC divides the MICS band into multiple channels of 300 KHz width [11]. A pair of communicating devices uses one of these channels.

IMDs typically communicate infrequently with a device called an IMD programmer (hereafter, *programmer*). The programmer initiates a session with the IMD during which it either queries the IMD for its data (e.g., patient name, ECG signal) or sends it commands (e.g., a treatment modification). By FCC requirement, the IMD does

not normally initiate communications; it transmits *only* in response to a transmission from a programmer [11] or if it detects a life-threatening condition [21].

A programmer and an IMD share the medium with other devices as follows [11]. Before they can use a 300 KHz channel for their session, they must "listen" for a minimum of 10 ms to ensure that the channel is unoccupied. Once they find an unoccupied channel, they establish a session and alternate between the programmer transmitting a query or command, and the IMD responding immediately without sensing the medium [22]. The programmer and IMD can keep using the channel until the end of their session, or until they encounter persistent interference, in which case they listen again to find an unoccupied channel.

3. Assumptions and Threat Model

3.1 Assumptions

We assume that IMDs and authorized programmers are honest and follow the protocols specified by the FCC and their manufacturers. We also assume the availability of a secure channel for transmissions between authorized programmers and the shield; this channel may use the MICS band or other bands. We further assume that the shield is a wearable device located close to the IMD, such as a necklace. Wearable medical devices are common in the medical industry [32, 47]. We also assume that the adversary does not physically try to remove the shield or damage it. We assume that legitimate messages sent to an IMD have a checksum and that the IMD will discard any message that fails the checksum test. This latter assumption is satisfied by all wireless protocols that we are aware of, including the ones used by the IMDs we tested (§9). Finally, we assume that the IMD does not normally initiate transmissions (in accordance with FCC rules [11]); if the IMD initiates a transmission because it detects a life-threatening condition, we make no attempt to protect the confidentiality of that transmission.

3.2 Threat Model

We address two classes of commonly considered radio-equipped adversaries: passive eavesdroppers that threaten the confidentiality of the IMD's transmissions, and active adversaries that attempt to send unauthorized radio commands to the IMD [13, 30].

(a) Passive eavesdropper: Such an adversary eavesdrops on the wireless medium and listens for an IMD's transmissions. Specifically, we consider an adversary with the following properties:

- The adversary may try different decoding strategies. It may consider the jamming signal as noise and try to decode in the presence of jamming. Alternatively, it can implement interference cancellation or joint decoding in an attempt to simultaneously decode the jamming signal and the IMD's transmission. However, basic results in multi-user information theory show that decoding multiple signals is impossible if the total information rate is outside the capacity region [51]. We ensure that the information rate at the eavesdropper exceeds the capacity region by making the shield jam at an excessively high rate; the jamming signal is random and sent without modulation or coding.
- The adversary may use standard or custom-built equipment. It may also use MIMO systems and directional antennas to try to separate the jamming signal from the IMD's signal. MIMO and directional antenna techniques, however, require the two transmitters to be separated by more than half a wavelength (see Chapter 1 in [24] and Chapter 7 in [51]). The IMDs we consider operate in the 400 MHz band with a wavelength of about 75 cm. Thus, one can defend against a MIMO eavesdropper or an eavesdropper with a directional antenna by ensuring that the shield is located significantly less than half a wavelength from the IMD. For example, if the protected IMD is a pacemaker implanted near the clavicle, the shield may be implemented as a necklace or a brooch, allowing it to sit within a few centimeters of the IMD.
- The adversary may be in any location farther away from the IMD than the shield (e.g., at distances 20 cm and greater).

(b) Active adversary: Such an adversary sends unauthorized radio commands to the IMD. These commands may be intended to modify the IMD's configuration or to trigger the IMD to transmit unnecessarily, depleting its battery. We allow this adversary the following properties:

- The adversary may use one of the following approaches to send commands: it may generate its own unauthorized messages; it may record prior messages from other sources and play them back to the IMD; or it may try to alter an authorized message on the channel, for example, by transmitting at a higher power and causing a capture effect at the IMD [44].
- The adversary may use different types of hardware. The adversary may transmit with a commercial IMD programmer acquired from a hospital or elsewhere. Such an approach does not require the adversary to know the technical specifications of the IMD's communication or to reverse-engineer its protocol. However, an adversary that simply uses an unmodified commercial IMD programmer cannot use a transmit power higher than that allowed by the FCC. Alternatively, a more sophisticated adversary might reverse-engineer the IMD's communication protocol, then modify the IMD programmer's hardware or use his own radio transmitter to send commands. In this case, the adversary can customize the hardware to transmit at a higher power than the FCC allows. Further, the adversary may use MIMO or directional antennas. Analogous to the above, however, MIMO beamforming and directional antennas require the two receivers to be separated by a minimum of half a wavelength (37 cm in the MICS band), and hence can be countered by keeping the shield in close proximity to the IMD.
- The adversary may be in any location farther away from the IMD than the shield.

4. System Overview

To achieve our design goal of protecting an IMD without modifying it, we design a device called the *shield* that sits near the IMD and acts as a proxy. An authorized programmer that wants to communicate with the IMD instead exchanges its messages with the shield, which relays them to the IMD and sends back the IMD's responses, as shown in Fig. 1. We assume the existence of an authenticated, encrypted channel between the shield and the programmer. This channel can be established using either in-band [17] or out-of-band solutions [26].

The shield actively prevents *any* device other than itself from communicating directly with the IMD. It does so by jamming messages sent to and from the IMD. Key to the shield's role is its ability to act as a jammer-cum-receiver, which enables it to jam the IMD's transmissions and prevent others from decoding them, while still being able to decode them itself. It also enables the shield to detect scenarios in which an adversary tries to overpower the shield's own transmissions to create a capture effect on the IMD and deliver an unauthorized message. By proxying IMD communications without requiring patients to interact directly with the shield, our design aligns with IMD industry trends toward wireless, time- and location-independent patient monitoring.

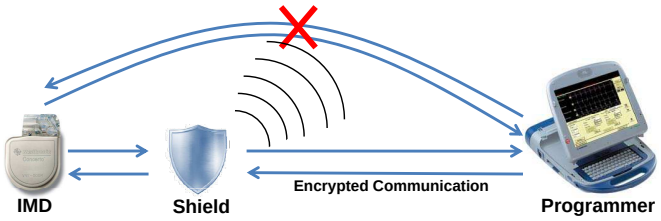


Figure 1—Protecting an IMD without modifying it: The shield jams any direct communication with the IMD. An authorized programmer communicates with the IMD only through the shield, with which it establishes a secure channel.

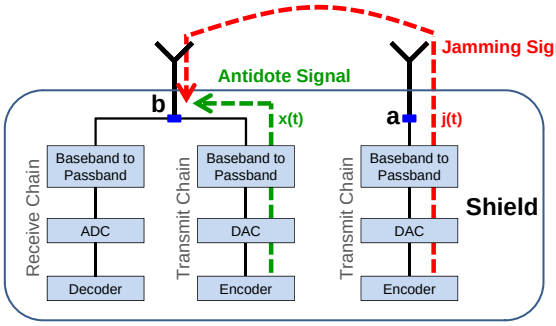


Figure 2—The jammer-cum-receiver design uses two antennas: a jamming antenna that transmits the jamming signal, and a receive antenna. The receive antenna is connected to both a transmit and receive chain. The antidote signal is transmitted from the transmit chain to cancel out the jamming signal in the receive chain.

The next sections explain the jammer-cum-receiver's design, implementation, and use against passive and active adversaries.

5. JAMMER-CUM-RECEIVER

A jammer-cum-receiver naturally needs to transmit and receive simultaneously. This section presents a design for such a full-duplex radio. Our design has two key features: First, it imposes no size restrictions and hence can be built as a small wearable device. Second, it cancels the jamming signal only at the device's receive antenna and at no other point in space—a necessary requirement for our application.

Our design, shown in Fig. 2, uses two antennas: a jamming antenna and a receive antenna. The jamming antenna transmits a random jamming signal. The receive antenna is simultaneously connected to both a transmit and a receive chain. The transmit chain sends an antidote signal that cancels the jamming signal at the receive antenna's front end, allowing the receive antenna to receive any signal without disruption from its own jamming signal.

The antidote signal can be computed as follows. Let $j(t)$ be the jamming signal and $x(t)$ be the antidote. Let H_{self} be the self-looping channel on the receive antenna (i.e., the channel from the transmit chain to the receive chain on the same antenna) and $H_{jam\to rec}$ the channel from the jamming antenna to the receive antenna. The signal received by the shield's receive antenna is:

$$y(t) = H_{jam\to rec}\, j(t) + H_{self}\, x(t). \quad (1)$$

To cancel the jamming signal at the receive antenna, the antidote must satisfy:

$$x(t) = -\frac{H_{jam\to rec}}{H_{self}}\, j(t). \quad (2)$$

Thus, by transmitting a random signal $j(t)$ on its jamming antenna and an antidote $x(t)$ on its receive antenna, the shield can receive signals transmitted by other nodes while jamming the medium.

Next, we show that the antidote cancels the jamming signal only at the shield's receive antenna, and no other location. Let $H_{jam\to l}$ and $H_{rec\to l}$ be the channels from the shield's jamming and receive antennas, respectively, to the adversary's location l. An antenna positioned at l receives the combined signal:

$$y(t) = H_{jam\to l}\, j(t) + H_{rec\to l}\, x(t) \quad (3)$$

$$= (H_{jam\to l} - H_{rec\to l}\frac{H_{jam\to rec}}{H_{self}})j(t). \quad (4)$$

For the jamming signal to be cancelled out at location l, the following must be satisfied:

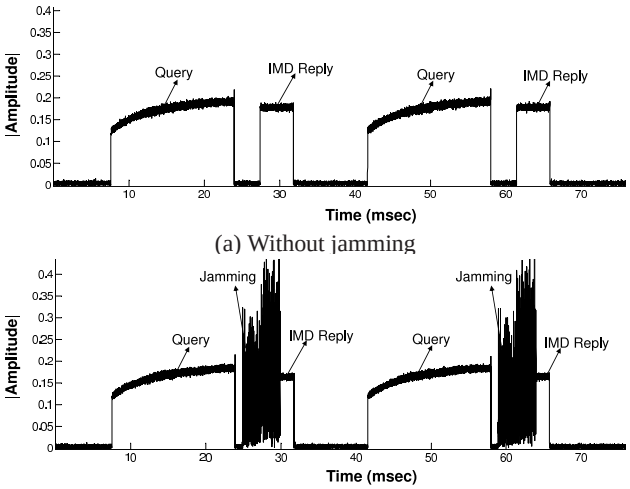
$$\frac{H_{jam\to l}}{H_{rec\to l}} = \frac{H_{jam\to rec}}{H_{self}}. \quad (5)$$

Locating the shield's two antennas very close to each other ensures that at any location l the attenuation from the two antennas is comparable, i.e., $|\frac{H_{jam\to l}}{H_{rec\to l}}| \approx 1$ (see Chapter 7 in [51] for a detailed analysis). In contrast, $|\frac{H_{jam\to rec}}{H_{self}}| \ll 1$; $|H_{self}|$ is the attenuation on the short wire between the transmit and receive chains in the receive antenna, which is significantly less than the attenuation between the two antennas that additionally have to go on the air [15]. For example, in our USRP2 prototype, the ratio $|\frac{H_{jam\to rec}}{H_{self}}| \approx -27$ dB. Thus, the above condition is physically infeasible, and cancelling the jamming signal at the shield's receive antenna does not cancel it at any other location.

We note several ancillary properties of our design:

- *Transmit and receive chains connected to the same antenna:* Off-the-shelf radios such as the USRP [7] have both a receive and a transmit chain connected to the same antenna; they can in principle transmit and receive simultaneously on the same antenna. Traditional systems cannot exploit this property, however, because the transmit signal overpowers the receive chain, preventing the antenna from decoding any signal but its own transmission. When the jamming signal and the antidote signal cancel each other, the interference is cancelled and the antenna can receive from other nodes while transmitting.
- *Antenna cancellation vs. analog and digital cancellation:* Cancelling the jamming signal with an antidote is a form of antenna cancellation. Thus, as in the antenna cancellation scheme by Choi et al. [3], one can improve performance using hardware components such as analog cancelers [41]. In this case, the input to the analog canceler will be taken from points a and b in Fig. 2; the output will be fed to the passband filter in the receive chain.
- *Channel estimation:* Computing the antidote in equation 2 requires knowing the channels H_{self} and $H_{jam\to rec}$. The shield estimates these channels using two methods. First, during a session with the IMD, the shield measures the channels immediately before it transmits to the IMD or jams the IMD's transmission. In the absence of an IMD session the shield periodically (every 200 ms in our prototype) estimates this channel by sending a probe. Since the shield's two antennas are close to each other, the probe can be sent at a low power to allow other nodes to leverage spatial reuse to concurrently access the medium.
- *Wideband channels:* Our discussion has been focused on narrowband channels. However, the same description can be extended to work with wideband channels which exhibit multipath effects. Specifically, such channels use OFDM, which divides the bandwidth into orthogonal subcarriers and treats each of the subcarriers as if it was an independent narrowband channel. Our model naturally fits in this context.[2]

[2]More generally, one could compute the multi-path channel and apply an equalizer [16] on the time-domain antidote signal that inverts the multi-path of the jamming signal.



(a) Without jamming

(b) With jamming

Figure 3—Typical interaction between the Virtuoso IMD and its programmer: Without jamming (a), the IMD transmits in response to an interrogation. The bottom graph (b) shows that the IMD transmits within a fixed interval without sensing the medium.

6. VERSUS PASSIVE EAVESDROPPERS

To preserve the confidentiality of an IMD's transmissions, the shield jams the IMD's signal on the channel. Since the wireless channel creates linear combinations of concurrently transmitted signals, jamming with a random signal provides a form of one-time pad, where only entities that know the jamming signal can decrypt the IMD's data [48]. The shield leverages its knowledge of the jamming signal and its jammer-cum-receiver capability to receive the IMD's data in the presence of jamming.

To realize our design goal, the shield must ensure that it jams every packet transmitted by the IMD. To this end, the shield leverages two properties of MICS-band IMD communications [11, 22]:

- An IMD does not transmit except in a response to a message from a programmer. The shield can listen for programmer transmissions and anticipate when the IMD may start transmitting.
- An IMD transmits in response to a message from a programmer without sensing the medium. This allows the shield to bound the interval during which the IMD replies after receiving a message.

Fig. 3 shows an example exchange between a Medtronic Virtuoso implantable cardiac defibrillator (ICD) and a programmer (in this case, a USRP). Fig. 3(a) shows that the Virtuoso transmits in response to a programmer's message after a fixed interval (3.5 ms). To check that the Virtuoso indeed does not sense the medium, we made the programmer USRP transmit a message to the Virtuoso and within 1 ms transmit another random message. Fig. 3(b) plots the resulting signal and shows that the Virtuoso still transmitted after the same fixed interval even though the medium was occupied.

Given the above properties, the shield uses the following algorithm to jam the IMD's transmissions. Let T_1 and T_2 be the lower and upper bounds on the time that the IMD takes to respond to a message, and let P be the IMD's maximum packet duration. Whenever the shield sends a message to the IMD, it starts jamming the medium exactly T_1 milliseconds after the end of its transmission. While jamming, the shield receives the signal on the medium using its receive antenna. The shield jams for $(T_2 - T_1) + P$ milliseconds.

Additionally, to deal with scenarios in which the IMD may transmit in response to an unauthorized message, the shield uses its ability to detect active adversaries that might succeed at delivering a message to the IMD (see §7(d)). Whenever such an adversary is detected, the shield uses the same algorithm above, as if the message were sent to the IMD by the shield itself.

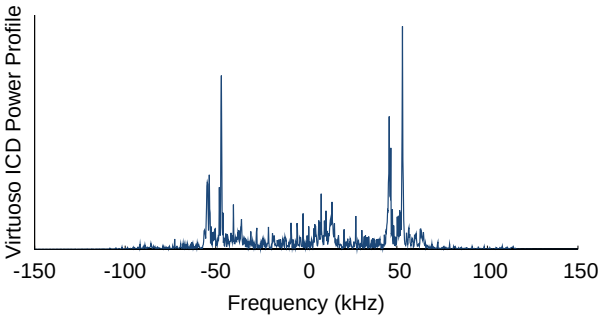


Figure 4—The frequency profile of the FSK signal captured from a Virtuoso cardiac defibrillator shows that most of the energy is concentrated around ± 50 KHz.

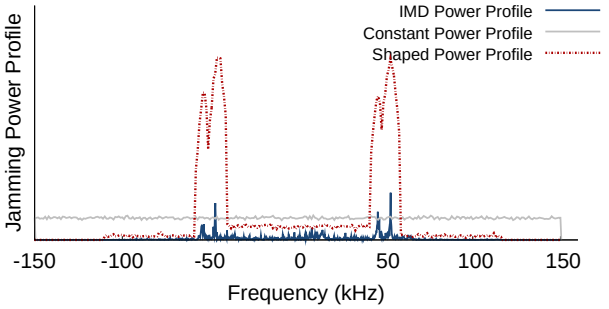


Figure 5—Shaping the jamming signal's profile to match an IMD's allows the shield to focus its jamming power on the frequencies that matter for decoding, as opposed to jamming across the entire 300 KHz channel.

We note that each shield should calibrate the above parameters for its own IMD. In particular, for the IMDs tested in this paper, the above parameters are as follows: $T_1 = 2.8$ ms, $T_2 = 3.7$ ms, and $P = 21$ ms.

Our design of the shield sets three sub-goals:

(a) Maximize jamming efficiency for a given power budget: It is important to match the frequency profile of the jamming signal to the frequency profile of the jammed signal [28]. To understand this issue, consider the example of the Virtuoso cardiac defibrillator. This device operates over a channel bandwidth of 300 KHz. However, it uses FSK modulation where a '0' bit is transmitted at one frequency f_0 and a '1' bit is transmitted at a different frequency f_1. Fig. 4 shows the frequency profile of the FSK signal captured from a Virtuoso cardiac defibrillator. A jammer might create a jamming signal over the entire 300 KHz. However, since the frequency-domain representation of the received FSK signal has most of its energy concentrated around f_0 and f_1, an adversary can eliminate most of the jamming signal by applying two band-pass filters centered on f_0 and f_1.

Therefore, an effective jammer should consider the structure of the IMD's signal when crafting the jamming signal, shaping the amount of energy it puts in each frequency according to the frequency profile of the IMD signal. Fig. 5 compares the power profile of a jamming signal that is shaped to fit the signal in Fig. 4 and an oblivious jamming signal that uses a constant power profile. The figure shows that the shaped signal has increased jamming power in frequencies that matter for decoding.

To shape its jamming signal appropriately, the shield generates the jamming signal by taking multiple random white Gaussian noise signals and assigning each of them to a particular frequency

bin in the 300 KHz MICS channel. The shield sets the variance of the white Gaussian noise in each frequency bin to match the power profile resulting from the IMD's FSK modulation in that frequency bin. We then take the IFFT of all the Gaussian signals to generate the time-domain jamming signal. This process generates a random jamming signal that has a power profile similar to the power profile generated by IMD modulation. The shield scales the amplitude of the jamming signal to match its hardware's power budget. The shield also compensates for any carrier frequency offset between its RF chain and that of the IMD.

(b) Ensure independence of eavesdropper location: To ensure confidentiality, the shield must maintain a high bit error rate (BER) at the adversary, *independent* of the adversary's location. The BER at the adversary, however, strictly depends on its signal-to-interference-and-noise ratio, SINR_A [15]. To show that the BER at the adversary is independent of its location, we show that the SINR at the adversary is independent of its location.

Suppose the IMD transmits its signal at a power P_i dB and the shield transmits the jamming signal at a power P_j dB. The IMD's signal and the jamming signal will experience a pathloss to the adversary of L_i and L_j, respectively. Thus, the SINR at the adversary can be written in dB as:

$$\text{SINR}_A = (P_i - L_i) - (P_j - L_j) - N_A, \tag{6}$$

where N_A is the noise in the adversary's hardware. Since equation 6 is written in a logarithmic scale, the pathlosses translate into subtractions.

The pathloss from the IMD to the adversary can be expressed as the sum of the pathloss that the IMD's signal experiences in the body and on the air, i.e., $L_i = L_{body} + L_{air}$ [37]. Since the shield and the IMD are close together, the pathlosses they experience on the air to the adversary are approximately the same—i.e., $L_{air} \approx L_j$ [51]. Thus, we can rewrite equation 6 as:

$$\text{SINR}_A = (P_i - L_{body}) - P_j - N_A. \tag{7}$$

The above equation shows that SINR_A is independent of the adversary's location and can be controlled by setting the jamming power P_j to an appropriate value. This directly implies that the BER at the adversary is independent of its location.

(c) SINR tradeoff between the shield and the adversary: Similarly to how we computed the SINR of an eavesdropper, we can compute the SINR of the shield (in dB) as:

$$\text{SINR}_S = (P_i - L_{body}) - (P_j - G) - N_G, \tag{8}$$

where N_G is the thermal noise on the shield and G is the reduction in the jamming signal power at the receive antenna due to the antidote. The above equation simply states that SINR_S is the IMD power after subtracting the pathloss due mainly to in-body propagation, the residual of the jamming power $(P_j - G)$, and the noise.

Note that if one ignores the noise on the shield's receive antenna and the adversary's device (which are negligible in comparison to the other terms), one can express the relation between the two SINRs using a simple equation:

$$\text{SINR}_S = \text{SINR}_A + G. \tag{9}$$

This simplified view reveals an intrinsic tradeoff between the SINR at the shield and the adversary, and hence their BERs. To increase the BER at the adversary while maintaining a low BER at the shield, one needs to increase G, which is the amount of jamming power cancelled at the shield's receive antenna. We refer to G as the *SINR gap* between the shield and the adversary.

We show in §10.1 that for the tested IMDs, an SINR gap of $G = 32$ dB suffices to provide a BER of nearly 50% at the adversary (reducing the adversary to guessing) while maintaining reliable packet delivery at the shield.

7. Versus Active Adversaries

Next, we explain our approach for countering active adversaries. At a high level, the shield detects unauthorized packets and jams them. The jamming signal combines linearly with the unauthorized signal, causing random bit flips during decoding. The IMD ignores these packets because they fail its checksum test.

The exact active jamming algorithm follows. Let S_{id} be an *identifying sequence*, i.e., a sequence of m bits that is always used to identify packets destined to the IMD. S_{id} includes the packets' physical-layer preamble and the subsequent header. When the shield is not transmitting, it constantly monitors the medium. If it detects a signal on the medium, it proceeds to decode it. For each newly decoded bit, the shield checks the last m decoded bits against the identifying sequence S_{id}. If the two sequences differ by fewer than a threshold number of bits, b_{thresh}, the shield jams the signal until the signal stops and the medium becomes idle again.

The shield also uses its receive antenna to monitor the medium while transmitting. However, in this case, if it detects a signal concurrent to its transmission, it switches from transmission to jamming and continues jamming until the medium becomes idle again. The reason the shield jams any concurrent signal without checking for S_{id} is to ensure that an adversary cannot successfully alter the shield's own message on the channel in order to send an unauthorized message to the IMD.

We note five subtle design points:

(a) Choosing identifying sequences: Our algorithm relies on the identifying sequence S_{id} in order to identify transmissions destined for the protected IMD. We therefore desire a method of choosing a per-device S_{id} based on unique device characteristics. Fortunately, IMDs already bear unique identifying characteristics. For example, the Medtronic IMDs that we tested (the Virtuoso ICD and the Concerto CRT) use FSK modulation, a known preamble, a header, and the device's ID, i.e., its 10-byte serial number. More generally, each wireless device has an FCC ID, which allows the designer to look up the device in the FCC database and verify its modulation, coding, frequency and power profile [10].[3] One can use these specifications to choose an appropriate identifying sequence. Furthermore, once in a session, the IMD locks on to a unique channel, to receive any future commands. Since other IMD–programmer pairs avoid occupied channels, this channel ID can be used to further specify the target IMD.

(b) Setting the threshold b_{thresh}: If an adversary can transmit a signal and force the shield to experience a bit error rate higher than the IMD's, it may prevent the shield from jamming an unauthorized command that the IMD successfully decodes and executes. However, we argue that such adversarial success is unlikely, for two reasons. First, because the signal goes through body tissue, the IMD experiences an additional pathloss that could be as high as 40 dB [45], and hence it naturally experiences a much weaker signal than the shield. Second, the IMD uses a harder constraint to accept a packet than the constraint the shield uses to jam a packet. Specifically, the IMD requires that all bits be correct to pass a checksum, while the shield tolerates some differences (up to b_{thresh} bits) between the identifying sequence and the received one. We describe our empirical method of choosing b_{thresh} in §10.1(c).

(c) Customizing for the MICS band: It is important to realize that the shield can listen to the entire 3 MHz MICS band, transmit in all or any subset of the channels in this band, and further continue

[3] For example, the FCC ID *LF5MICS* refers to Medtronic IMDs we tested.

to listen to the whole band as it is transmitting in any subset of the channels. It is fairly simple to build such a device by making the radio front end as wide as 3 MHz and equipping the device with per-channel filters. This enables the shield to process the signals from all channels in the MICS band simultaneously.

The shield uses this capability to monitor the entire 3 MHz MICS band because an adversary can transmit to the IMD on any channel in the band. This monitoring allows the shield to detect and counter adversarial transmissions even if the adversary uses frequency hopping or transmits in multiple channels simultaneously to try to confuse the shield. The shield jams any given 300 KHz channel if the channel contains a signal that matches the constraints described in the active jamming algorithm.

(d) Complying with FCC rules: The shield must adhere to the FCC power limit even when jamming an adversary. However, as explained in §3, a sophisticated adversary may use a transmission power much higher than the FCC limit. In such cases, the adversary will be able to deliver its packet to the IMD despite jamming. However, the shield is still useful because it can detect the high-powered adversary in real time and raise an alarm to attract the attention of the patient or a caregiver. Such alarms may be similar to a cell phone alarm, i.e., the shield may beep or vibrate. It is desirable to have a low false positive rate for such an alarm. To that end, we calibrate the shield with an IMD to find the minimum adversarial transmit power that can trigger a response from the IMD despite jamming. We call this value P_{thresh}. When the shield detects a potentially adversarial transmission, it checks whether the signal power exceeds P_{thresh}, in which case it raises an alarm.

Finally, we note that when the shield detects a high-powered active adversary, it also considers the possibility that the adversary will send a message that triggers the IMD to send its private data. In this case, the shield applies the passive jamming algorithm: in addition to jamming the adversary's high-powered message, it jams the medium afterward as detailed in §6.

(e) Battery life of the shield: Since jamming consumes power, one may wonder how often the shield needs to be charged. In the absence of attacks, the shield jams only the IMD's transmissions, and hence transmits approximately as often as the IMD. IMDs are typically nonrechargeable power-limited devices that do not transmit frequently [9]. Thus, in this mode of operation, we do not expect the battery of the shield to be an issue. When the IMD is under an active attack, the shield will have to transmit as often as the adversary. However, since the shield transmits at the FCC power limit for the MICS band, it can last for a day or longer even if transmitting continuously. For example, wearable heart rate monitors that continuously transmit ECG signals can last 24–48 hours [55].

8. IMPLEMENTATION

We implement a proof-of-concept prototype shield with GNU Radio and USRP2 hardware [7, 14]. The prototype uses the USRP's RFX400 daughterboards, which operate in the MICS band [11]. The USRP2 does not support multiple daughterboards on the same motherboard, so we implement a two-antenna shield with two USRP2 radio boards connected via an external clock so that they act as a single node. Our implementation uses the FURY GPSDO clock model [23].

Our design for a two-antenna jammer-cum-receiver requires the receive antenna to be always connected to both a transmit and a receive chain. To enable the shield's receive antenna to transmit and receive simultaneously, we turn off the USRP RX/TX switch, which leaves both the transmit and receive chains connected to the antenna all the time. Specifically, we set `atr_txval=MIX_EN` and `atr_rxval=ANT_SW` in the TX chain, and we set `atr_txval=MIX_EN` and `atr_rxval=MIX_EN` in the RX chain, in the USRP2's firmware and FPGA code. Finally, we equip the shield with FSK modulation and demodulation capabilities so that it can communicate with an IMD.

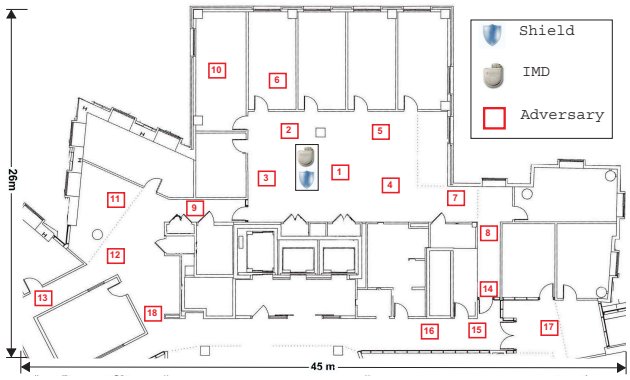


Figure 6—Testbed setup showing shield, IMD, and adversary locations. We experiment with 18 adversary locations, numbered here in descending order of received signal strength at the shield.

9. TESTING ENVIRONMENT

Our experiments use the following devices:

- Medtronic Virtuoso DR implantable cardiac defibrillators (ICDs) [35].
- A Medtronic Concerto cardiac resynchronization therapy device (CRT) [34].
- A Medtronic Vitatron Carelink 2090 Programmer [33].
- USRP2 software radio boards [7].

In our *in vitro* experiments, the ICD and CRT play the role of the protected IMD. The USRP devices play the roles of the shield, the adversary, and legitimate users of the MICS band. We use the programmer off-line with our active adversary; the adversary records the programmer's transmissions in order to replay them later. Analog replaying of these captured signals doubles their noise, reducing the adversary's probability of success, so the adversary demodulates the programmer's FSK signal into the transmitted bits to remove the channel noise. The adversary then re-modulates the bits to obtain a clean version of the signal to transmit to the IMD.

Fig. 6 depicts the testing setup. To simulate implantation in a human, we followed prior work [20] and implanted each IMD beneath 1 cm of bacon, with 4 cm of 85% lean ground beef packed underneath. We placed the shield next to the IMD on the bacon's surface to simulate a necklace. We varied the adversary's location between 20 cm and 30 m, as shown in the figure.

10. EVALUATION

We evaluate our prototype of a shield against commercially available IMDs. We show that the shield effectively protects the confidentiality of the IMD's messages and defends the IMD against commands from unauthorized parties. We experiment with both the Virtuoso ICD and the Concerto CRT. However, since the two IMDs did not show any significant difference, we combine the experimental results from both devices and present them together. Our results can be summarized as follows.

- In practice, our antenna cancellation design can cancel about 32 dB of the jamming signal at the receive antenna (§10.1(a)). This result shows that our design achieves similar performance to the antenna cancellation algorithm proposed in prior work [3], but without requiring a large antenna separation.

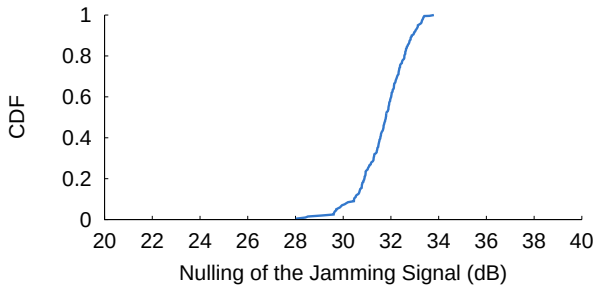


Figure 7—Antenna cancellation: The antidote signal reduces the jamming signal by 32 dB on average.

- Setting the shield's jamming power 20 dB higher than the IMD's received power allows the shield to achieve a high bit error rate at adversarial locations while still being able to reliably decode the IMD's transmissions (§10.1(b)). The shield's increased power still complies with FCC rules in the MICS band since the transmit power of implanted devices is 20 dB less than the transmit power for devices outside the body [38, 39].
- With the above setting, the bit error rate at a passive eavesdropper is nearly 50% at all tested locations—i.e., an eavesdropping adversary's decoding efforts are no more effective than random guessing. Further, even while jamming, the shield can reliably decode the IMD's packets with a packet loss rate less than 0.2%. We conclude that the shield and the IMD share an information channel inaccessible to other parties (§10.2).
- When the shield is present and active, an adversary using off-the-shelf IMD programmers cannot elicit a response from the protected IMD even from distances as small as 20 cm. A more sophisticated adversary that transmits at 100 times the shield's power successfully elicits IMD responses only at distances less than 5 meters, and only in line-of-sight locations. Further, the shield detects these high-powered transmissions and raises an alarm. We conclude that the shield significantly raises the bar for such high-powered adversarial transmissions (§10.3).

10.1 Micro-Benchmark Results

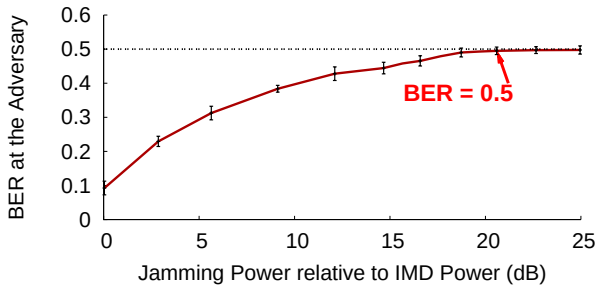
In this section, we calibrate the parameters of the shield and examine the performance of its components.

(a) Antenna cancellation: We first evaluate the performance of the antenna cancellation algorithm in §5, in which the shield sends an antidote signal to cancel the jamming signal on its receive antenna.

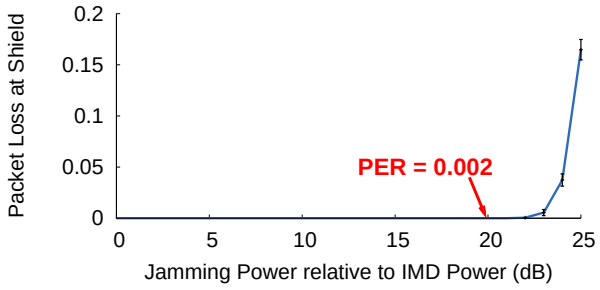
In this experiment, the shield transmits a random signal on its jamming antenna and the corresponding antidote on its receive antenna. In each run, it transmits 100 Kb without the antidote, followed by 100 Kb with the antidote. We compute the received power at the receive antenna with and without the antidote. The difference in received power between the two trials is the amount of jamming cancellation resulting from the transmission of the antidote.

Fig. 7 shows the CDF of the amount of cancellation over multiple runs of the experiment. It shows that the average reduction in jamming power is about 32 dB. The figure also shows that the variance of this value is small. This result shows that the antenna cancellation algorithm introduced in this paper achieves similar performance to the antenna cancellation algorithm proposed by Choi et al. [3], but without requiring a large antenna separation.[4]

[4] Choi et al. [3] also combine antenna cancellation with analog and digital cancellation to obtain a total cancellation of 60 dB at the receive antenna. However, we show in §10.2 that for our purposes, a cancellation of 32 dB suffices to achieve our goal of high reliability at the shield and nearly 50% BER at the adversary.



(a) Adversary's BER vs. jamming power



(b) Shield's PER vs. jamming power

Figure 8—Tradeoff between BER at the eavesdropper and reliable decoding at the shield: If the shield sets its jamming power 20 dB higher than the power it receives from the IMD, it can ensure that an eavesdropper sees a BER around 50% (a)—effectively reducing the eavesdropper to guessing—while keeping the packet loss rate (PER) at the shield as low as 0.2% (b).

(b) Tradeoffs between eavesdropper error and shield error: The aforementioned 32 dB of cancellation at the shield's receive antenna naturally sets an upper bound on the jamming power: if the residual error after jamming cancellation is too high, the shield will fail to decode the IMD's data properly.

To explore the tradeoff between the error at the shield and the error at an eavesdropper, we run the following experiment. We place the IMD and the shield at their marked locations in Fig. 6, and we place a USRP eavesdropper 20 cm away from the IMD at location 1. In each run of the experiment, the shield repeatedly triggers the IMD to transmit the same packet. The shield also uses its jammer-cum-receiver capability to simultaneously jam and decode the IMD's packets. The eavesdropper tries to decode the IMD packets, in the presence of jamming, using an optimal FSK decoder [36].

Fig. 8(a) plots the eavesdropper's BER as a function of the shield's jamming power. Since the required jamming power naturally depends on the power of the jammed IMD's signal, the x-axis reports the shield's jamming power relative to the power of the signal it receives from the IMD. The figure shows that if the shield sets its jamming power 20 dB higher than the power of the signal it receives from the IMD, the BER at an eavesdropper is 50%, which means the eavesdropper's decoding task is no more successful than random guessing.

Next, we check that the above setting allows the shield to reliably decode the IMD's packets. As above, Fig. 8(b) plots the shield's packet loss rate as a function of its jamming power relative to the power of the signal it receives from the IMD. The figure shows that if the shield's jamming power is 20 dB higher than the IMD's power, the packet loss rate is no more than 0.2%. We conclude that this jamming power achieves both a high error rate at the eavesdropper and reliable decoding at the shield.

We note that the shield's increased power, described above, still complies with FCC rules on power usage in the MICS band because

P_{thresh}: Adversary power that elicits IMD response	Minimum	−11.1 dBm
	Average	−4.5 dBm
	Standard Deviation	3.5 dBm

Table 1—Adversarial RSSI that elicits IMD responses despite the shield's jamming.

the transmit power of implanted devices is 20 dB less than the maximum allowed transmit power for devices outside the body [38, 39].

(c) Setting the jamming parameters: Next we calibrate the jamming parameters for countering active adversaries. The shield must jam unauthorized packets sent to the IMD it protects. It must jam these packets even if it receives them with some bit errors, because they might otherwise be received correctly at the IMD. We therefore empirically estimate an upper bound, b_{thresh}, on the number of bit flips an IMD accepts in an adversary's packet header. The shield uses this upper bound to identify packets that must be jammed.

To estimate b_{thresh}, we perform the following experiment. First, a USRP transmits unauthorized commands to the IMD to trigger it to send patient data. We repeat the experiment for all locations in Fig. 6. The shield stays in its marked location in Fig. 6, but its jamming capability is turned off. However, the shield logs all of the packets transmitted by the IMD as well as the adversarial packets that triggered them. We process these logs offline and, for packets that successfully triggered an IMD response despite containing bit errors, we count the number of bit flips in the packet header. Our results show that it is unlikely that a packet will have bit errors at the shield but still be received correctly by the IMD. Out of 5000 packets, only three packets showed errors at the shield but still triggered a response from an IMD. The maximum number of bit flips in those packets was 2, so we conservatively set $b_{thresh} = 4$.

Next, we measure P_{thresh}, the minimum adversary RSSI at the shield that can elicit a response from the IMD in the presence of jamming. To do so, we fix the location of the IMD and the shield as shown in Fig. 6. Again we use a USRP that repeatedly sends a command to trigger the IMD to transmit. We fix the adversary in location 1 and vary its transmit power. Table 1 reports the minimum and average RSSI at the shield's receive antenna for all packets that succeeded in triggering the IMD to transmit. We set P_{thresh} 3 dB below the minimum RSSI in the table and use that value for all subsequent experiments.

10.2 Protecting from Passive Adversaries

To evaluate the effectiveness of the shield's jamming, we run an experiment in which the shield repeatedly triggers the IMD to transmit the same packet. The shield also uses its jammer-cum-receiver capability to jam the IMD's packets while it decodes them. We set the shield's jamming power as described in §6. In each run, we position an eavesdropper at a different location shown in Fig. 6 and make the IMD send 1000 packets. The eavesdropping adversary attempts to decode the IMD's packets using an optimal FSK decoder [36]. We record the BER at the eavesdropper and the packet loss rate at the shield.

Fig. 9 plots a CDF of the eavesdropper's BER taken over all locations in Fig. 6. The CDF shows that the eavesdropper's BER is nearly 50% in all tested locations. We conclude that our design of the shield achieves the goal of protecting the confidentiality of IMD's transmissions from an eavesdropper regardless of the eavesdropper's location.

For the same experiment, Fig. 10 plots a CDF of the packet loss rate of IMD-transmitted packets at the shield. Each point on the x-axis refers to the packet loss rate over 1000 IMD packets. The average packet loss rate is about 0.2%, considered low for wireless systems [6]. Such a low loss rate is due to two factors. First, we

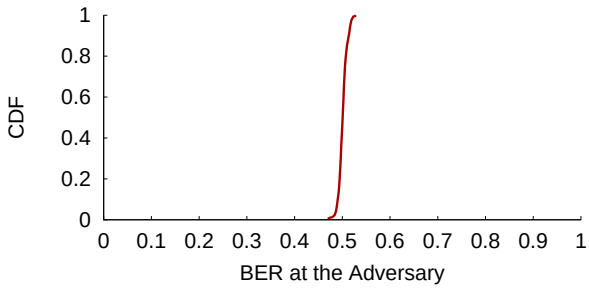


Figure 9—CDF of an eavesdropper's BER over all eavesdropper locations in Fig. 6: At all locations, the eavesdropper's BER is nearly 50%, which makes its decoding task no more successful than random guessing. The low variance in the CDF shows that an eavesdropper's BER is independent of its location.

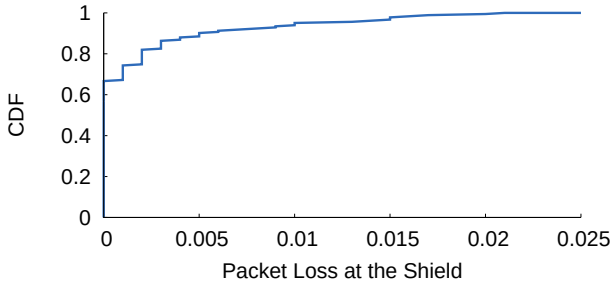


Figure 10—Packet loss at the shield: When the shield is jamming, it experiences an average packet loss rate of only 0.2% when receiving the IMD's packets. We conclude that the shield can reliably decode the IMD's transmissions despite jamming.

locate the shield fairly close to the IMD, so it receives the IMD's signal at a relatively high SNR. Second, the jamming cancellation is sufficient to maintain a high SNR that ensures a low packet loss rate. We conclude that the shield can decode the IMD's packets reliably, even while jamming.

10.3 Protecting from Active Adversaries

We distinguish between two scenarios representing different levels of adversarial sophistication. In the first, we consider scenarios in which the adversary uses an off-the-shelf IMD programmer to send unauthorized commands to the IMD. In the second, a more sophisticated adversary reverse-engineers the protocol and uses custom hardware to transmit with much higher power than is possible in the first scenario.

(a) Adversary that uses a commercial IMD programmer: The simplest way an adversary can send unauthorized commands to an IMD is to obtain a standard IMD programmer and use its built-in radio. Since commercial programmers abide by FCC rules, in this scenario, the adversary's transmission power will be comparable to that of the shield.

Using an IMD programmer we obtained via a popular auction website, we play the role of such an active adversary. We use the setup in Fig. 6, fixing the IMD's and shield's locations and transmitting unauthorized commands from all the marked locations. As shown in the figure, we experiment with both line-of-sight and non-line-of-sight locations as well as nearby (20 cm) and relatively far locations (30 m).

To test whether the shield's jamming is effective against unauthorized commands, regardless of which unauthorized command the adversary chooses to send, we experiment with two types of adversarial commands: those that trigger the IMD to transmit its data

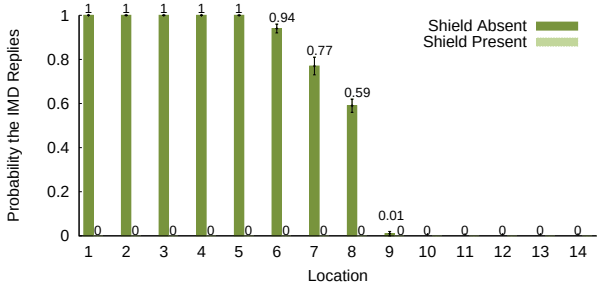


Figure 11—Without the shield, triggering an IMD to transmit and deplete its battery using an off-the-shelf IMD programmer succeeds with high probability. With the shield, such attacks fail.

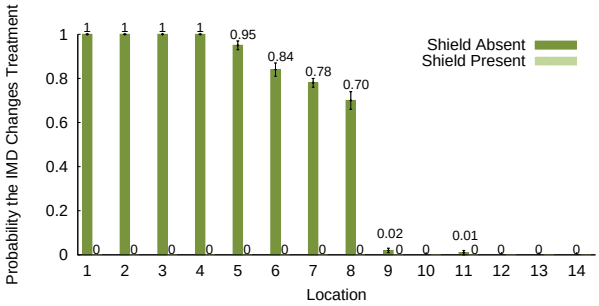


Figure 12—Without the shield, an adversary using an off-the-shelf programmer to send unauthorized commands (in this case, to modify therapy parameters) succeeds with high probability. The shield materially decreases the adversary's ability to control the IMD.

with the objective of depleting its battery, and those that change the IMD's therapy parameters. In each location, we play each command 100 times with the shield on and 100 times with the shield off. After each attempt, we check whether the command was successful. To determine whether the first type of command was successful—i.e., whether it elicited a reply—we sandwiched a USRP observer along with the IMD between the two slabs of meat. To allow the USRP observer to easily check whether the IMD transmitted in response to the adversary's command, we configure the shield to jam only the adversary's packets, not the packets transmitted by the IMD. To determine whether a therapy modification command was successful, we use the IMD programmer to read the therapy parameters before and after the attempt.

Fig. 11 and Fig. 12 show the results of these experiments. They plot the probability that adversarial commands succeed with the shield off (absent) and on (present), each as a function of adversary locations. The locations are ordered by decreasing SNR at the USRP observer. The figures show the following:

- When the shield is off, adversaries located up to 14 meters away (location 8) from the IMD—including non-line-of-sight locations—can change the IMD's therapy parameters or cause the IMD to transmit its private data using precious battery energy, in contrast to past work in which the adversarial range is limited to a few centimeters [20]. We attribute this increased adversarial range to recent changes in IMD design that enable longer-range radio communication (MICS band) meant to support remote monitoring and a larger sterile field during surgery.
- When the shield is on, it successfully prevents the IMD from receiving adversarial commands as long as the adversary uses a device that obeys FCC rules on transmission power—even when the adversary is as close as 20 cm.
- There is no statistical difference in success rate between commands that modify the patient's treatment and commands that trigger the IMD to transmit private data and deplete its battery.

(b) High-powered active adversary: Next, we experiment with scenarios in which the adversary uses custom hardware to transmit at 100 times the shield's transmit power. The experimental setup is similar to those discussed above; specifically, we fix the locations of the IMD and the shield and vary the high-powered adversary's position among the numbered locations in Fig. 6. Each run has two phases: one with the shield off and another with the shield on. Since we found no statistical difference in success rate between unauthorized commands that trigger the IMD to transmit and those that change its therapy parameters, we show results only for the therapy modification command.

Fig. 13 shows the results of this experiment in terms of the observed probability of adversarial success, with the shield both on and off. It also shows the observed probability that the shield raises an alarm, which is how the shield responds to a high-powered (above P_{thresh}) adversarial transmission. The figure further shows:

- When the shield is off, the adversary's increased transmission power allows it to elicit IMD responses from as far as 27 meters (location 13) and from non-line-of-sight locations.
- When the shield is on, the adversary elicits IMD responses only from nearby, line-of-sight locations. Thus, the shield's presence raises the bar even for high-powered adversaries.
- Whenever the adversary elicits a response from the IMD in the presence of the shield, the shield raises an alarm. The shield also raises an alarm in response to *unsuccessful* adversarial transmissions that are high powered and emanate from nearby locations (e.g., location 6). While this conservative alert results in false positives, we believe it is reasonable to alert the patient that an adversary is nearby and may succeed at controlling the IMD.

11. COEXISTENCE

We investigate how the presence of a shield affects other legitimate users of the medium. As explained in §2, the FCC rules for medical devices in the MICS band require such devices to monitor a candidate channel for 10 ms and avoid using occupied channels. As a result, two pairs of honest medical devices are unlikely to share the same 300 KHz channel. We focus our evaluation on coexistence with the meteorological devices that are the primary users of the MICS band (and hence can transmit even on occupied channels).

In this experiment, we position the IMD and the shield in the locations marked on Fig. 6. We make a USRP board alternate between sending unauthorized commands to the IMD and transmitting cross-traffic unintended for the IMD. The cross-traffic is modeled after the transmissions of meteorological devices, in particular a Vaisala digital radiosonde RS92-AGP [1] that uses GMSK modulation. For each of the adversary positions in Fig 6, we make the USRP alternate between one packet to the IMD and one cross-traffic packet. The shield logs all packets it detects and reports which of them it jammed.

Post-processing of the shield's log showed that the shield did not jam any of the cross-traffic packets, regardless of the transmitter's location. In contrast, the shield jammed all of the packets that it detected were addressed to the IMD; see Table 2. Further, our software radio implementation of the shield takes 270 ± 23 μs after an adversary stops transmitting to turn around and stop its own transmissions. This delay is mainly due to the shield's being implemented in software. A hardware implementation would have a more efficient turn-around time of tens of microseconds. (Note, for example, that a 802.11 card can turn around in a SIFS duration of 10 μs.) The low turn-around time shows that the shield does not continuously jam the medium (thereby denying others access to it).

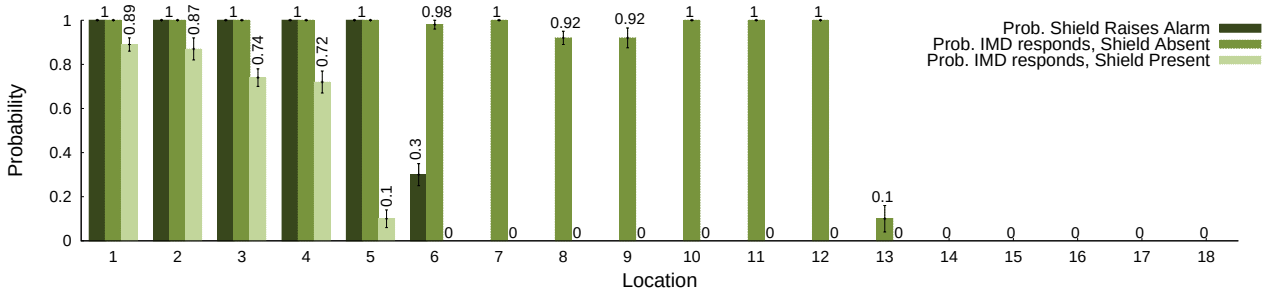


Figure 13—High-powered adversary: Without the shield, an adversary transmitting at 100 times the shield's power can change the IMD's therapy parameters even from non-line-of-sight locations up to 27 m away. With the shield, the adversary is successful only from line-of-sight locations less than 5 m away, and the shield raises an alarm.

Probability of Jamming	Cross-Traffic	0
	Packets that trigger IMD	1
Turn-around Time	Average	270 μs
	Standard Deviation	23 μs

Table 2—Coexistence results: Jamming behavior and turn-around time in the presence of simulated meteorological cross-traffic.

12. Related Work

Recent innovations in health-related communication and networking technologies range from low-power implantable radios that harvest body energy [25] to medical sensor networks for in-home monitoring and diagnosis [49, 53]. Past work has also studied the vulnerabilities of these systems and proposed new designs that could improve their security [19, 20]. Our work builds on this foundation, but it differs from all past works in that it presents the first system that defends existing commercial IMDs against adversaries who eavesdrop on transmissions or send unauthorized commands.

Our design is motivated by the work of Halperin et al., who analyzed the security properties of an implantable cardiac device and demonstrated its vulnerability to adversarial actions that compromise data confidentiality or induce potentially harmful heart rhythms [19, 20]. They also suggested adding passively powered elements to implantable devices to allow them to authenticate their interlocutors. Along similar lines, Denning et al. propose a class of devices called *cloakers* that would share secret keys with IMDs [5]; an IMD would attempt to detect an associated cloaker's presence either periodically or when presented with an unknown programmer. Unlike these three proposals, our technique does not require cryptographic methods and is directly applicable to IMDs that are already implanted.

Other work has focused on the problem of key distribution for cryptographic security. Cherukuri et al. propose using consistent human biometric information to generate identical secret keys at different places on a single body [2]. Schechter suggests that key material could be tattooed onto patients using ultraviolet micropigmentation [46].

Our work also builds on a rich literature in wireless communication. Past work on physical-layer information-theoretic security has shown that if the channel to the receiver is better than the channel to an eavesdropper, the sender-receiver pair can securely communicate [4, 50, 52].

Most of the past work on jamming focuses on enabling wireless communication in the presence of adversarial jamming [27, 40]. Some past work, however, has proposed to use friendly jamming to prevent adversarial access to RFID tags, sensor nodes, and IMDs [31, 42, 54]. Our work is complementary to this past work but differs from it in that our jammer can transmit and receive at the same time; this allows it to decode IMD messages while protecting their confidentiality.

Our work is related to prior work by Gollakota et al., who propose iJam, an OFDM-based technique to jam while receiving to prevent unauthorized receivers from obtaining a protected signal [18]. iJam, however, is not applicable to IMDs because it relies on the intrinsic characteristics of OFDM signals, which differ greatly from IMDs' FSK signals. Furthermore, iJam requires changes to both the transmitter and receiver, and hence does not immediately apply to IMDs that are already implanted.

Finally, our design of a jammer-cum-receiver builds on the full-duplex radio design by Choi et al. [3]. However, our design does not require an antenna separation of half a wavelength, or 37 cm in the MICS band. Hence our design can be incorporated in a small portable device that a patient could wear or carry.

13. Conclusion

The influx of wireless communication in medical devices brings a number of domain-specific problems that require the expertise of both the wireless and security communities. This paper addresses the problem of communication security for implantable medical devices. The key challenge in addressing this problem stems from the difficulty of modifying or replacing implanted devices. We present the design and implementation of a wireless physical-layer solution that delegates the task of protecting IMD communication to an external device called the shield. Our evaluation shows that the shield effectively provides confidentiality for IMDs' transmitted data and shields IMDs from unauthorized commands, both without requiring any changes to the IMDs themselves.

Acknowledgments: We thank Arthur Berger, Ramesh Chandra, Rick Hampton, Steve Hanna, Dr. Daniel Kramer, Swarun Kumar, Nate Kushman, Kate Lin, Hariharan Rahul, Stefan Savage, Keith Winstein, and Nickolai Zeldovich for their insightful comments. The authors acknowledge the financial support of the Interconnect Focus Center, one of the six research centers funded under the Focus Center Research Program, a Semiconductor Research Corporation program. This research is also supported by NFS CNS-0831244, an NSF Graduate Research Fellowship, a Sloan Research Fellowship, the Armstrong Fund for Science, and Cooperative Agreement No. 90TR0003/01 from the Department of Health and Human Services. Its contents are solely the responsibility of the authors and do not necessarily represent the official views of the DHHS or NSF. K. Fu is listed as an inventor on patent applications pertaining to zero-power security and low-power flash memory both with assignee UMass.

14. References

[1] J. Åkerberg. State-of-the-art radiosonde telemetry. In *Proc. Symp. Integrated Observing and Assimilation Systems for Atmosphere, Oceans, and Land Surface*. American Meterological Society, 2004.

[2] S. Cherukuri, K. K. Venkatasubramanian, and S. K. S. Gupta. Biosec: A biometric based approach for securing communication in wireless

networks of biosensors implanted in the human body. In *International Conference on Parallel Processing Workshops*, 2003.
[3] J. Choi, M. Jain, K. Srinivasan, P. Levis, and S. Katti. Achieving single channel, full duplex wireless communication. In *Proc. ACM MobiCom*, 2010.
[4] I. Csiszar and J. Korner. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, 24(3):339–348, 1978.
[5] T. Denning, K. Fu, and T. Kohno. Absence makes the heart grow fonder: New directions for implantable medical device security. In *Proc. USENIX Workshop on Hot Topics in Security (HotSec)*, 2008.
[6] D. Eckhardt and P. Steenkiste. Measurement and analysis of the error characteristics of an in-building wireless network. In *Proc. ACM SIGCOMM*, 1996.
[7] Ettus Inc. Universal Software Radio Peripheral. http://ettus.com/.
[8] European Telecommunications Standard Institute. ETSI EN 301 839-1 V1.3.1, 2009.
[9] C. Falcon. Inside implantable devices. *Medical Design Tech.*, 2004.
[10] Federal Communications Commission. FCC ID number search. http://www.fcc.gov/searchtools.html.
[11] Federal Communications Commission. MICS Medical Implant Communication Services, FCC 47CFR95.601-95.673 Subpart E/I Rules for MedRadio Services.
[12] K. Fu. Inside risks: Reducing the risks of implantable medical devices: A prescription to improve security and privacy of pervasive health care. *Communications of the ACM*, 52(6):25–27, 2009.
[13] K. Fu. Trustworthy medical device software. In *Public Health Effectiveness of the FDA 510(k) Clearance Process: Measuring Postmarket Performance and Other Select Topics: Workshop Report*. IOM (Institute of Medicine), National Academies Press, 2011.
[14] GNU Radio. http://gnuradio.org/.
[15] A. Goldsmith. *Wireless Communications*. Cambridge University Press, 2005.
[16] S. Gollakota, F. Adib, D. Katabi, and S. Seshan. Clearing the rf smog: Making 802.11n robust to cross-technology interference. In *ACM SIGCOMM*, 2011.
[17] S. Gollakota, N. Ahmed, N. Zeldovich, and D. Katabi. Secure in-band wireless pairing. In *Usenix security symposium*, 2011.
[18] S. Gollakota and D. Katabi. Physical layer security made fast and channel-independent. In *Proc. IEEE INFOCOM*, 2011.
[19] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel. Security and privacy for implantable medical devices. *IEEE Pervasive Computing*, 7(1), 2008.
[20] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In *Proc. IEEE Symposium on Security and Privacy*, 2008.
[21] Industry Canada. Radio Standards Specification RSS-243: Medical Devices Operating in the 401–406 MHz Frequency Band. Spectrum Management and Telecommunications, 2010.
[22] International Telecommunications Union. ITU-R Recommendation RS.1346: Sharing between the meteorological aids service and medical implant communication systems (MICS) operating in the mobile service in the frequency band 401–406 MHz, 1998.
[23] Jackson Labs. Fury GPSDO. http://www.jackson-labs.com/.
[24] W. C. Jakes. *Microwave Mobile Communications*. Wiley, 1974.
[25] M. Koplow, A. Chen, D. Steingart, P. Wright, and J. Evans. Thick film thermoelectric energy harvesting systems for biomedical applications. In *Proc. Symp. Medical Devices and Biosensors*, 2008.
[26] C. Kuo, J. Walker, and A. Perrig. Low-cost manufacturing, usability and security: An analysis of bluetooth simple pairing and wi-fi protected setup. In *Usable Security Workshop*, 2007.
[27] Y. Liu, P. Ning, H. Dai, and A. Liu. Randomized differential DSSS: Jamming-resistant wireless broadcast communication. In *Proc. IEEE INFOCOM*, 2010.
[28] J. Lopatka. Adaptive generating of the jamming signal. In *Proc. IEEE Military Communications Conference (MILCOM)*, 1995.
[29] W. H. Maisel. Safety issues involving medical devices: Implications of recent implantable cardioverter-defibrillator malfunctions. *Journal of the American Medical Association*, 2005.
[30] W. H. Maisel and T. Kohno. Improving the security and privacy of implantable medical devices. *New England Journal of Medicine*, 362(13):1164–1166, 2010.
[31] I. Martinovic, P. Pichota, and J. Schmitt. Jamming for good: A fresh approach to authentic communication in WSNs. In *Proc. ACM Conf. on Wireless Network Security (WiSec)*, 2009.
[32] Medtronic's Paradigm Veo wireless insulin pump helps prevent hypoglycemia. *MedGadget—Internet Journal for emerging medical technologies*, 2009.
[33] Medtronic Inc. CareLink Programmer. http://www.medtronic.com/for-healthcare-professionals/products-therapies/cardiac-rhythm/patient-management-carelink/medtronic-carelink-programmer/index.htm.
[34] Medtronic Inc. Concerto II CRT-D digital implantable cardioverter defibrillator with cardiac resynchronization therapy. http://www.medtronic.com/for-healthcare-professionals/products-therapies/cardiac-rhythm/cardiac-resynchronization-therapy-devices/historical-crt-devices/index.htm.
[35] Medtronic Inc. Virtuoso DR/VR implantable cardioverter defibrillator systems. http://www.medtronic.com/your-health/sudden-cardiac-arrest/device/our-implantable-defibrillators/virtuoso/index.htm.
[36] H. Meyr, M. Moeneclaey, and S. A. Fechtel. *Digital Communication Receivers: Synchronization, Channel Estimation, and Signal Processing*. Wiley, 1998.
[37] D. Panescu. Wireless communication systems for implantable medical devices. *IEEE Eng. in Medicine and Biology Mag.*, 2008.
[38] PCTest Engineering Labs, Inc. Certificate of compliance, fcc part 95 certification, test report number: 95.220719375.lf5, 2002.
[39] PCTest Engineering Labs, Inc. Certificate of compliance, fcc part 95 and en 301 839-2, test report number: 0703090168.med, 2007.
[40] C. Pöpper, M. Strasser, and S. Capkun. Jamming-resistant broadcast communication without shared keys. In *USENIX Security Sym.*, 2009.
[41] B. Radunovic, D. Gunawardena, P. Key, A. Proutiere, N. Singh, H. V. Balan, and G. Dejean. Rethinking indoor wireless: Low power, low frequency, full-duplex. Technical report, Microsoft Research, 2009.
[42] M. Rieback, B. Crispo, and A. Tanenbaum. RFID Guardian: A battery-powered mobile device for RFID privacy management. In *Proc. Australasian Conf. on Information Security and Privacy*, 2005.
[43] D. Sagan. Rf integrated circuits for medical applications: Meeting the challenge of ultra low power communication. Zarlink Semiconductor. http://stf.ucsd.edu/presentations.
[44] N. Santhapuri, R. R. Choudhury, J. Manweiler, S. Nelakuduti, S. Sen, and K. Munagala. Message in message mim: A case for reordering transmissions in wireless networks. In *ACM HotNets-VII*, 2008.
[45] K. Sayrafian-Pour, W. Yang, J. Hagedorn, J. Terrill, K. Yazdandoost, and K. Hamaguchi. Channel models for medical implant communication. *Inter. Journal of Wireless Info. Networks*, 2010.
[46] S. Schechter. Security that is meant to be skin deep: Using ultraviolet micropigmentation to store emergency-access keys for implantable medical devices. In *USENIX Workshop HealthSec*, 2010.
[47] M. Scheffler, E. Hirt, and A. Caduff. Wrist-wearable medical devices: Technologies and applications. *Medical Device Technology*, 2003.
[48] C. E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4):656–715, 1949.
[49] V. Shnayder, B. Chen, K. Lorincz, T. R. F. Fulford-Jones, and M. Welsh. Sensor networks for medical care. Technical Report TR-08-05, Harvard University, 2005.
[50] M. J. Siavoshani, U. Pulleti, E. Atsan, I. Safaka, C. Fragoulia, K. Argyraki, and S. Diggavi. Exchanging secrets without using cryptography. *arXiv:1105.4991v1*, 2011.
[51] D. Tse and P. Vishwanath. *Fundamentals of Wireless Communications*. Cambridge University Press, 2005.
[52] A. Wyner. The wire-tap channel. *Bell Sys. Technical Journal*, 1975.
[53] S. Xiao, A. Dhamdhere, V. Sivaraman, and A. Burdett. Transmission power control in body area sensor networks for healthcare monitoring. *IEEE Journal on Selected Areas in Comm.*, 2009.
[54] 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*, 2011.
[55] Zephyr Inc. BioHarness BT. http://www.zephyr-technology.com.
[56] C. Zhan, W. B. Baine, A. Sedrakyan, and S. Claudia. Cardiac device implantation in the US from 1997 through 2004: A population-based analysis. *Journal of General Internal Medicine*, 2007.