Securing Implantable Medical Devices Using Ultrasound Waves

Siddiqi, Muhammad Ali; Beurskens, Robert H.S.H.; Kruizinga, Pieter; De Zeeuw, Chris I.; Strydis, Christos

DOI
10.1109/ACCESS.2021.3083576

Publication date
2021

Document Version
Final published version

Published in
IEEE Access

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 3, 2021, accepted May 11, 2021, date of publication May 25, 2021, date of current version June 8, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3083576

Securing Implantable Medical Devices Using Ultrasound Waves

MUHAMMAD ALI SIDDIQI[1,2], ROBERT H. S. H. BEURSKENS[3], PIETER KRUIZINGA[1], CHRIS I. DE ZEEUW[1], AND CHRISTOS STRYDIS[1,2], (Senior Member, IEEE)

[1]Department of Neuroscience, Erasmus Medical Center, 3015 GD Rotterdam, The Netherlands
[2]Quantum and Computer Engineering Department, Delft University of Technology, 2628 CD Delft, The Netherlands
[3]Department of Biomedical Engineering, Erasmus Medical Center, 3015 GD Rotterdam, The Netherlands

Corresponding author: Muhammad Ali Siddiqi (m.a.siddiqi@tudelft.nl)

This work was supported by the EU-Funded Project SDK4ED under Grant 780572.

ABSTRACT Modern Implantable Medical Devices (IMDs) are vulnerable to security attacks because of their wireless connectivity to the outside world. One of the main security challenges is establishing trust between the IMD and an external reader/programmer in order to facilitate secure communication. Numerous device-pairing schemes have been proposed to address this specific challenge. However, they alone cannot protect against a battery-depletion attack in which the adversary is able to keep the IMD occupied with continuous authentication requests until the battery empties. As a result, energy harvesting has been employed as an ancillary mechanism for implementing Zero-Power Defense (ZPD) functionality in order to protect against such a low-cost attack. In this paper, we propose SecureEcho, a device-pairing scheme based on MHz-range ultrasound that establishes trust between the IMD and an external reader. In addition, SecureEcho achieves ZPD without requiring any energy harvesting, which significantly reduces the design complexity. We also provide a proof-of-concept implementation and a first ever security evaluation of the ultrasound channel, which proves that it is infeasible for the attacker to eavesdrop or insert messages even from a range of a few millimeters.

INDEX TERMS Authentication protocol, battery-depletion attack, body-coupled communication, denial-of-service attack, IMD, implantable medical device, ultrasound, zero-power defense.

I. INTRODUCTION

Efforts on securing implantable medical devices (IMDs) have intensified over the past few years in the wake of successful ethical-hacking attempts [1]–[3]. Most of the focus has been on establishing trust between the IMD and the external reader/programmer (see Figure 1), or in other words, securely pairing the two devices. This involves making use of an additional channel or mechanism for authenticating the reader (by proving physical proximity) and agreeing on a cryptographic key so that the reader can securely access the IMD via the wireless channel to send commands or read out data. These solutions are mostly based on the *touch-to-access* policy [4], which assumes that entities that can come in close proximity to the patient for a *prolonged* period of time are considered trusted, and are allowed access. This is because a patient would reject any physical contact from a stranger or an attacker. Moreover, in close proximity, the attacker would have far easier means of harming the patient instead of pursuing a cybersecurity attack [5].

However, these schemes rely on the authenticator, i.e., the IMD, periodically polling for the requester over the untrusted wireless channel to kick-start the pairing process *before* proximity is established. This makes the IMD susceptible to battery Denial-of-Service (DoS) (or battery-depletion) attacks, which are among the simplest attacks to mount: the attacker continuously sends connection requests to the IMD with the aim of draining the IMD battery. Even though the messages are bogus, the IMD has to spend some energy to process or authenticate each request message. With a significantly large number of such requests, the attacker can successfully drain the battery and thus force device shutdown [6].

Traditionally, energy harvesting[1] has been employed to protect against such attacks. In such a strategy, which is a so-called *zero-power defense* (ZPD) mechanism, the IMD first harvests energy from wireless messages received from the external entity and then performs the authentication operation using this *free* energy. The IMD does not switch to its

The associate editor coordinating the review of this manuscript and approving it for publication was Cihun-Siyong Gong.

[1]We will use the term *energy harvesting* for both RF- and inductive-coupling-based harvesting techniques available in literature [7].

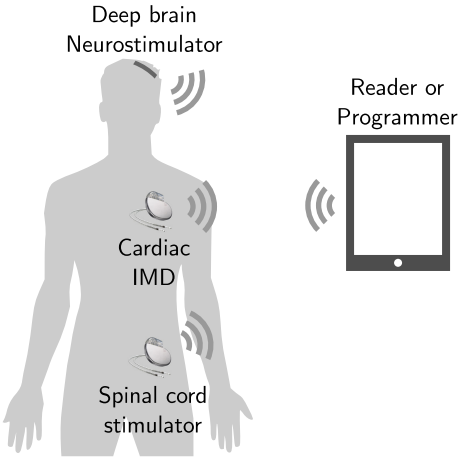


FIGURE 1. Typical commercial IMDs.

main battery for subsequent operations *until and unless* the external entity is authenticated.

Based on the above, the existing device-pairing schemes still require the use of energy-harvesting-based ZPD (EH-ZPD) to protect against battery DoS. However, energy harvesting requires additional components next to the transceiver, such as a harvesting circuit, power management and an energy reservoir (see Figure 2), which increase design complexity. It also has to satisfy additional frequency-band and medical-safety constraints in order to be used in an IMD.

In this work, we propose SecureEcho,[2] an ultrasound-based device-pairing scheme that protects against battery DoS without actually implementing energy harvesting, which reduces the associated design complexity. SecureEcho achieves secure pairing by using ultrasound as a body-coupled-communication (BCC) channel for sharing a cryptographic key. The completely passive nature of the proposed circuit allows the IMD communication interface to remain asleep before any access is made via the BCC channel, which enables ZPD. To the best of our knowledge, ultrasound has never been used for key transport in *plaintext* before. This is because of the absence of an in-depth security evaluation of this channel, as inferred from the various works in literature [8]–[10]. Therefore, in this work, we also provide a comprehensive security evaluation of this channel in order to prove its robustness against eavesdropping and message-insertion attacks.

This work, thus, makes the following novel contributions:

- A lightweight device-pairing security protocol that utilizes ultrasound in order to protect against battery-depletion attacks.
- A comprehensive security evaluation of ultrasound as an *inherently secure* BCC channel.
- A proof-of-concept implementation and validation of the SecureEcho approach.
- A detailed comparison of SecureEcho and the traditional energy-harvesting-based ZPD method.

[2]The SecureEcho device-pairing scheme described in this paper is part of a patent application that was filed in Greece on May 19, 2021, with e-filing No. 244-0004268198.

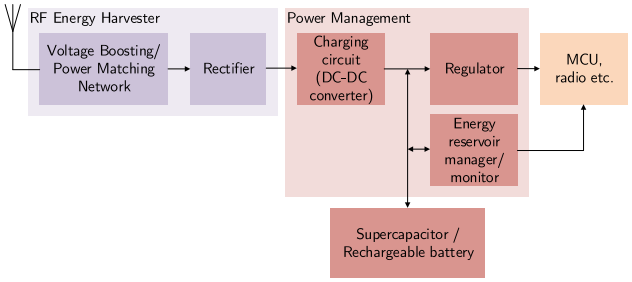


FIGURE 2. A generic RF energy harvesting system [6].

The rest of the paper is organized as follows. Section II reviews the related work. We explain our proposed reader-IMD device-pairing scheme, SecureEcho, in Section III. In Section IV, we mount a comprehensive security evaluation of the ultrasound BCC channel and, in Section V, we provide the proof-of-concept implementation of our approach. A detailed comparison of SecureEcho and the EH-ZPD approach is provided in Section VI. We draw overall conclusions in Section VII.

II. RELATED WORK

Over the past decade, numerous touch-to-access schemes have been proposed to securely pair the reader and the IMD. These schemes can be categorized as follows: **Biometric-based** schemes [4], [11] rely on the reader-IMD pair to measure a biometric/physiological signal from the patient's body. Access is allowed based on the similarity of these measurements. **Proxy-based** schemes use an additional device, such as a smart phone, watch, etc. [12], [13], which is paired with the IMD and is used to authenticate the reader. In an emergency, the device can be physically distanced from the patient in order to grant the reader unsecured access to the IMD. **Token-based** schemes rely on the patients having the IMD-access key or password with them, which is stored e.g., on a bracelet. **Distance-based** schemes [9], [14] employ weak or out-of-band (OOB) signals to exchange secrets or keys, or determine the distance between the devices in order to be sure of proximity.

Please note that in this paper, we will use the term *direct (or plaintext) key transport* when a symmetric key is sent in plaintext from one entity to another over an OOB channel. We will use the term *key agreement* when both entities exchange public-key material over the OOB channel, which is then used to compute the symmetric key.

A. BODY-COUPLED COMMUNICATION

There is an emerging trend of using the human body as an OOB channel (i.e., a distance-based scheme) not only for reader-IMD pairing, but also for pairing devices within a wireless body area network (WBAN) [15]. Three general body-coupled communication (BCC) techniques are capacitive coupling, galvanic coupling and ultrasound communication, respectively, as shown in Figure 3. In capacitive coupling, the signal propagates through the body from a

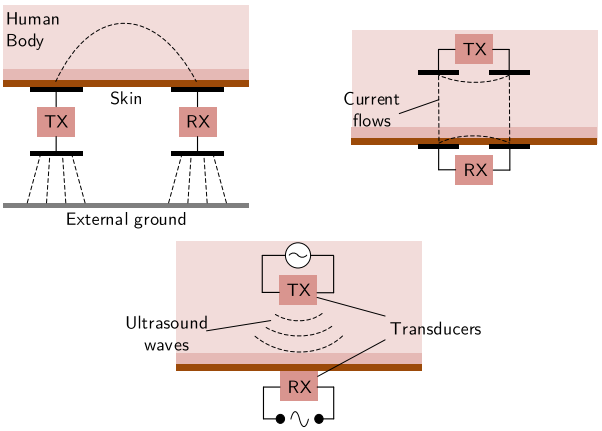


FIGURE 3. General types of BCC: Capacitive coupling (top left), Galvanic coupling (top right) and ultrasound communication (bottom).

transmitter electrode to the receiver in the form of electromagnetic waves while the return path between the two nodes is formed by electrostatic coupling between their second electrodes and an external ground [16]. In the case of galvanic coupling, the transmitter sends the signal through the body by inducing alternating current into the tissue, which is received by the two receiver electrodes [16], [17]. In ultrasound, a piezoelectric or a capacitive transducer at the transmitter side converts an electrical signal into acoustic waves (at frequencies > 20 kHz), which are detected by a similar transducer at the receiver and converted back into the original electrical signal [18].

The external return path of capacitive coupling results in electromagnetic leakage, which can be sniffed by an attacker [15], [16]. As a result, it can only be used for *key agreement*, i.e., exchanging the *public* keys, and not for key *transport* in plaintext. Galvanic coupling, is more localized and has been used for direct key transport in [3]. A preliminary security evaluation of this channel in [19] indicates that it is secure against attacks from distances > 0.5 m. However, its authors still recommend a comprehensive analysis that also takes into account different transmit powers and antenna gains of the attacker device.

Ultrasound can also potentially be used for direct key transport. However, to the best of our knowledge, such a work does not exist in literature. This will be discussed in detail in Section II-B.

It should be noted that the use of BCC for the whole reader-IMD communication session, instead of just the key establishment, is *impractical* due to its very nature. For example, it is not possible to have regular communication with a bedside reader that is a few feet away from the patient. Hence, switching to an RF transceiver is necessary in order to support long-range telemetry.

B. ULTRASOUND COMMUNICATION

Ultrasound has been proposed as a BCC channel for data transfer in quite a few recent works, such as [18], [20]–[22]. It has also been proposed as a wireless-power-transfer (WPT) channel for recharging IMDs [23], [24]. Furthermore, it is being touted as an in-body communication and WPT channel for the next-generation mm-sized neural implants for both the Central (CNS) and Peripheral Nervous Systems (PNS) [25], [26]. This is because the size of ultrasound transceivers can be several orders smaller than their electromagnetic (EM) counterparts, which is ideal for scaling-down of IMDs. Moreover, the power attenuation of ultrasound waves in soft tissue is significantly smaller than that of EM waves, leading to deeper tissue penetration and relaxed medical-safety constraints [24], [25]. However, to the best of our knowledge, its applicability in secure data transfer (e.g., direct key transport) has not been pursued. This is mainly due to the lack of evaluating the security of this channel.

Mayrhofer and Gellersen [10] performed a high-level threat analysis for ultrasound communication. They assumed that an attacker can eavesdrop on this channel if they are in the same room, and that a line of sight is not required when using this channel. Such an assumption had had to be made since a comprehensive security analysis was not available at the time. In Section IV, we will show that for high (MHz-range) resonant frequencies, the ultrasound channel can be considered safe against both eavesdropping and active attacks beyond a few millimeters. Mayrhofer *et al.* also proposed a method for secretly sending nonces via the ultrasound channel: First, a user ensures that the devices to be paired are aware of the distance between each other. The sender device first sends an RF synchronization message, and then, after a delay, sends an ultrasound pulse. This delay represents the value of the secret (or nonce). The receiving device extracts the message by calculating the delay between the received RF synchronization message and the ultrasound pulse, and subtracting the known distance. In the case of reader-IMD communication, however, the absence of the user interface on the IMD prevents the user from verifying that the two devices have agreed on a correct distance.

Besides, acoustic waves within the *audible* frequency range were employed for direct key transport by Halperin *et al.* [1]. In this scheme, the IMD sends a random key using this channel and the reader listens to this transmission at a very short range. However, this scheme was soon found to be vulnerable to passive eavesdropping from 5-6 feet away [27].

Rasmussen *et al.* [9] also proposed an acoustic-channel-based device pairing. However, instead of direct key transport, a distance-bounding scheme was employed. In such a scheme, the IMD calculates the delay between the sent and received transmissions in order to determine the physical distance between the reader-IMD pair. The IMD allows access if the reader is in very close proximity. Its security depends on the fact that an attacker cannot send a message to the acoustic interface faster than the speed of sound in air. One of the main differences of the above solution with SecureEcho is that its acoustic interface is not fully passive, which rules out its use as a ZPD scheme (when not using energy harvesting). Another issue is that this interface employs a band-pass filter,

amplifier and a phase-locked loop, which results in a (much) more complex design compared to SecureEcho.

The latest work from Putz *et al.* [8] proposes an acoustic-channel-based device pairing in which the devices send their *public-key* material via an audio interface. *Integrity codes* are employed to detect whether the keys were modified while in transit. These public keys can then be used to derive a shared symmetric key, e.g., in the form of a Diffie–Hellman key exchange, in order to secure the RF communication channel. The solution is tailored for pairing devices that already have a built-in audio and user interface, such as smartphones. A user can trigger the start of the pairing process by enabling the acoustic interfaces on both the devices (via the respective applications). However, in the case of reader-IMD systems, the absence of an IMD user interface implies that the pairing startup will require an initial communication between the two devices over an untrusted channel, and for one device to periodically poll for the other. As in the above works, this is done *before* proximity has been established. As a result, the above schemes are susceptible to battery-DoS attacks *if* energy-harvesting-based ZPD is not in place. SecureEcho, on the other hand, provides an elegant solution of inherently providing ZPD without requiring any energy harvesting, as will be shown in Section III.

III. SECUREECHO DEVICE PAIRING

In this section, we present our reader-IMD device-pairing scheme, SecureEcho, which is tailored to protect IMDs against battery-depletion attacks in addition to establishing trust.

SecureEcho employs ultrasound as a BCC channel. Although this scheme can work with *either* ultrasound or galvanic coupling, we prefer the former. This is because the ultrasound transducers offer highly directional and very-short-range communication depending on the frequency of operation and transducer width, which is ideal for secure key transport. The security evaluation of this channel will be discussed in detail in Section IV.

A. SYSTEM AND ATTACKER MODEL

We consider an IMD, such as a cardiac implant, which can communicate wirelessly with an external programming device or reader. This wireless interface is employed to change IMD configuration, retrieve private patient data, perform a firmware update, and so on (see Figure 4).

We assume an attacker whose aim could be to (1) steal private patient data, (2) tamper with patient data, and/or (3) modify treatment configuration or prevent treatment in order to physically harm the patient. Moreover, the attacker is assumed to have full control of the wireless (RF) channel between the reader and IMD, i.e., they can eavesdrop, insert, modify, block or replay messages between the two entities at will. Furthermore, we assume that the ultrasound-receiver circuit of the IMD is purely passive in nature, i.e., it does not consume any additional energy. This will be important for the discussion pertaining to message-insertion attacks.

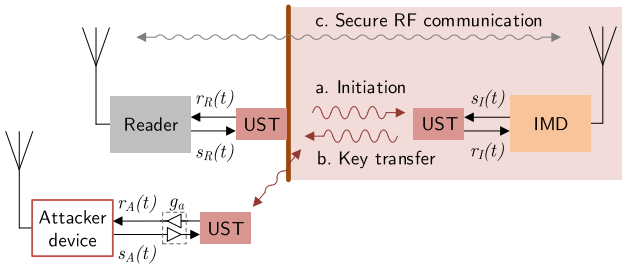


FIGURE 4. BCC-based reader-IMD pairing. UST: Ultrasound Transducer.

B. SECURITY PROTOCOL

The idea behind our scheme is briefly summarized in Figure 4. To pair a reader with an IMD, the ultrasound probe of the reader is first placed on the patient skin surface at a point closest to the implant. This is because the ultrasound propagation range is very short for MHz-range transducers and the acoustic absorption in air is very high. Since only a trusted person is able to come this close to the patient, which involves touching the skin for a prolonged period of time, this type of access can be considered strongly in line with the touch-to-access principle. The IMD can, thus, now safely assume that the message received from the ultrasound channel is from a trusted entity. Assuming that this channel is secure from eavesdropping, which we will discuss in detail in Section IV, the IMD can securely transport a symmetric key, which can be used to secure the subsequent RF communication.

The above secure device pairing can be achieved by following the protocol in Figure 5. The notation $\{\cdot\}_K$ denotes *authenticated encryption* using a key K, such as the standardized Galois Counter Mode (GCM) block-cipher mode of operation, which, in addition to confidentiality, also provides message authentication and data integrity by computing a message authentication code (MAC).

The reader sends an initiation message via the ultrasound channel in order to wake up the implant and start a communication session. This message contains a randomly-generated nonce (N_R) and the reader identifier (ID_R). The IMD responds with its own identifier (ID_I), nonce (N_I) and most importantly, a fresh and random long-term key (K). The IMD then turns on the RF transceiver for data communication. Both entities calculate a short-term session key $K' = \mathsf{kdf}(K, N_I, N_R)$ to be used for encrypting subsequent messages, where $\mathsf{kdf}()$ can be any secure key-derivation function. The reader then sends the nonces and ID_I as an encrypted message over the RF channel. The IMD decrypts and verifies the received message to be certain that the other entity is authentic and is in possession of K'. If the verification fails, the IMD turns off the RF transceiver and aborts the protocol. Otherwise, it sends the nonces and ID_R as an encrypted message to the reader.

The reader decrypts the message received from the IMD and verifies its contents. At this point, both entities have mutually authenticated each other. A secure communication channel between the two entities has been established, and

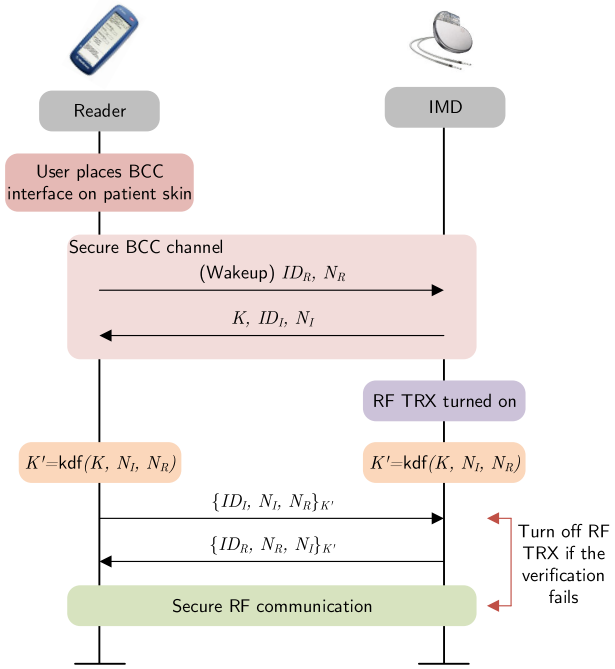


FIGURE 5. Reader-IMD protocol for initial pairing.

hence, they can now proceed with encrypting the subsequent messages using K'.

The key point during this pairing process is that the RF transceiver can *only* be woken up by the IMD MCU/processor. Since the attacker is unable to use the ultrasound BCC channel without the patient noticing, RF communication can never happen, and hence, battery DoS cannot be launched.

For the subsequent sessions, i.e., when both the devices already share a long-term key, the initial pairing is *not* required. In this case, the protocol from Figure 6 is executed over the RF channel using fresh nonces (N'_I and N'_R), which is based on the three-pass mutual authentication protocol specified in ISO/IEC 9798-2. In case a MAC check fails at the IMD side or when the received nonces and identifier do not match, e.g., in the case of a battery-DoS attack using bogus messages, the IMD turns off its RF transceiver and exits the protocol. For the next legitimate access, the devices would then again be required to undergo the pairing of Figure 5.

C. SYSTEM ARCHITECTURE

Figure 7 shows the overview of the proposed system architecture. There is a separate MCU/processor for executing the medical application (*medical MCU*), and for handling communication packets and running the security protocol (*security MCU*). This dual-processor architecture, which is based on [28], is a first step in protecting against DoS attacks in general: If an attacker sends continuous packets to prevent the IMD from running its main application, only the security MCU will be kept busy entertaining those messages, whereas the medical MCU will remain unaffected. However, in order

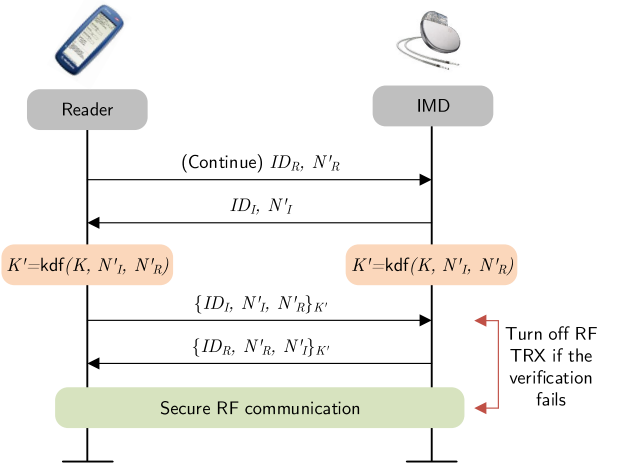


FIGURE 6. Secure communication protocol over the RF channel based on a pre-shared long-term key K.

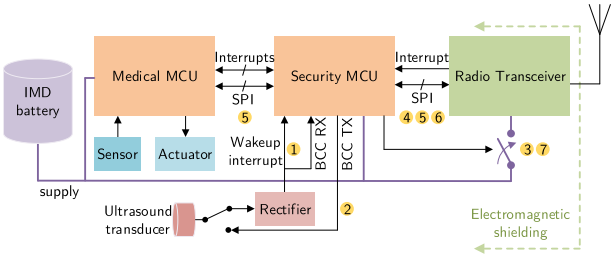


FIGURE 7. SecureEcho system schematic with FSM steps numbered according to figure 8.

to protect against battery DoS specifically, additional measures are required, as explained below.

In the default (unpaired) state, the RF transceiver is *powered off* and the security MCU is in its lowest power or *deep-sleep* state. The finite state machine (FSM) of this MCU is shown in Figure 8. It is important to note that, during this unpaired state, the RF transceiver does not wake up periodically to check the presence of an incoming RF signal. The security MCU is first woken up from its deep sleep via the ultrasound interface. In order to achieve *true* ZPD, this interface is required to operate passively, i.e., without consuming any additional energy. Fortunately, an ultrasound transducer can do just that; it can passively convert incident waves into an electrical signal so that it can be used to wake up the security MCU. This will also be demonstrated in Section V.

The IMD will use this interface to transport the long-term key K, as previously shown in Figure 5. The security MCU will then signal to power up the RF transceiver. The IMD is now ready to receive encrypted RF packets. When the communication session is over, the RF transceiver will go to sleep (instead of getting powered off) and, similarly to commercial IMDs, it will periodically wake up to check (or *sniff*) for an external entity trying to communicate with the IMD. In the above or any of the future sessions, if a packet authentication fails, the security MCU will reset the pairing by turning off the RF transceiver. Hence, in order to start

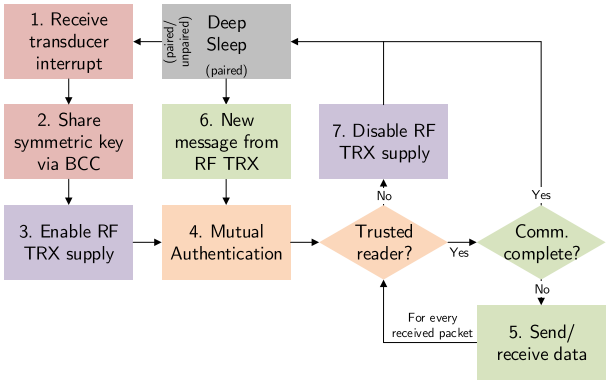


FIGURE 8. State machine of the secondary, security MCU.

the communication with the IMD again, the reader would be required to repeat the ultrasound BCC pairing.

The system architecture also includes an electromagnetic-shielding cage, which protects against side-channel attacks (to be discussed in Section IV-C). The RF antenna lies outside this cage so that (secure) RF communication is not affected.

IV. SECURITY ANALYSIS OF ULTRASOUND COMMUNICATION

To perform a comprehensive security evaluation of the ultrasound communication channel, which we employ in SecureEcho, two ways exist: (1) Physical-setup based and (2) simulation based. Regarding the first approach, it would be too cumbersome and impractical to perform the security analysis on an actual setup while taking into account the different variables, such as the transducer frequency, attacker distance, directivity etc. As a result, we follow the second approach instead, in which we employ acoustic simulations using the open-source *k-Wave toolbox* [29] built in MATLAB. k-Wave is an increasingly popular and well-studied simulation tool for modeling acoustic wave-field propagation in heterogeneous media. k-Wave efficiently solves a system of first-order, coupled equations that accounts for phenomena such as acoustic absorption and complex tissue-wave interactions that play a part when waves are transmitted through the skin and other layers. Moreover, k-Wave has been validated experimentally and it has become one of the standards for accurate and fast ultrasound simulations [30], [31].

The acoustic properties of the media encountered in an IMD setting and employed in k-Wave simulations are taken from [32], [33] and are summarized in Table 1. The acoustic impedance ($Z = \rho c$) and absorption coefficient (α) values significantly contribute to the attenuation of the ultrasound signal. When the signal travels from one medium (medium 1) to the next (medium 2), then the *transmission coefficient* (i.e., the ratio of the transmitted-signal amplitude and the incident-signal amplitude) is $2Z_2/(Z_1 + Z_2)$ [34]. For $Z_1 \gg Z_2$, the signal will experience a very-high attenuation. In addition, these waves suffer absorption at a rate of α dB/m, which increases with frequency.

TABLE 1. Acoustic properties for different media encountered in an IMD scenario.

Medium	Speed of sound, c (m/s)	Density, ρ (kg/m^3)	Acoustic impedance, Z (kg/m^{2}s $\times 10^6$)	Absorption coefficient, α (dB/m)[§]
Air	346	1.2	0.0004	161
Gel*	1480	1000	1.48	0.16
Skin	1624	1109	1.801	129.95
Fat**	1477	911	1.345	42.99

[§] At 1 MHz
* It acts as a coupling medium between the skin and the external probe.
** Subcutaneous Adipose Tissue (SAT)

The transducer efficiency for the simulations is set to 3.8 kPa/V (1 kPa = 1000 Pascals [N/m^2]) in order to match the one used in our proof-of-concept design (see Section V). The resulting acoustic intensities in W/m^2 (based on the employed signal voltages in our study) are well within the FDA safety limits for ultrasound operation [35]. For the digital data transfer over the ultrasound channel, ASK modulation (on-off keying) with non-return-to-zero (NRZ) data encoding is employed. These schemes are used to simplify the analysis without loss of generality. We ran the simulations using three different transmit frequencies, 0.5, 1 and 2 MHz, which are used in WPT schemes and ultrasonography, to find a secure range of operation.

A. PASSIVE (EAVESDROPPING) ATTACK

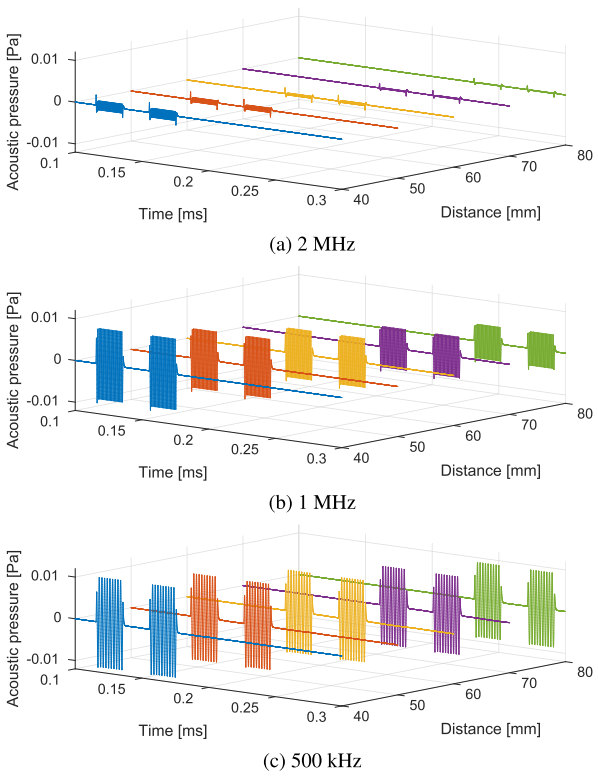
We first investigate whether an attacker can successfully eavesdrop on the key K, which is transported via the ultrasound channel. For this test, we assume that the IMD applies a 3.3 V (amplitude) signal to its transducer. This voltage level is consistent with the batteries used in such devices.

Figure 9 shows the acoustic attenuation of ASK-modulated bits (1, 0, 1, 0) with respect to transducers of different resonant frequencies, at a bit rate of 50 kbps. We notice a significant attenuation with the increase in the transducer resonant frequency. This is mainly because the acoustic absorption increases with frequency. This already gives us an indication of the improbability of retrieving the signal correctly after a few centimeters at frequencies $\geq$ 2 MHz.

To analyze this concretely, we perform a bit-error ratio (BER) analysis of the ASK-demodulated signal with respect to the attacker's distance and the employed transducer (frequency). The received signal $r_A(t)$ at the input of the attacker's demodulator is given in (1), where $s_I(t)$ is the source (modulated) waveform that drives the transducer at the IMD side (see Figure 4). $h(t)$ is the overall impulse response of the acoustic medium and g_a is the voltage gain of the attacker's receiving amplifier. $n_t(t)$ is the thermal noise due to the transducer and $n_a(t)$ is the noise introduced by the receiving amplifier.

$$r_A(t) = g_a \cdot \{h(t) * s_I(t) + n_t(t)\} + n_a(t) \tag{1}$$

The RMS value ($\bar{n}_t$) of $n_t(t)$ is shown in (2), where k_B is the Boltzmann constant, R is the transducer resistance tuned to the amplifier's input resistance, T is the temperature, and

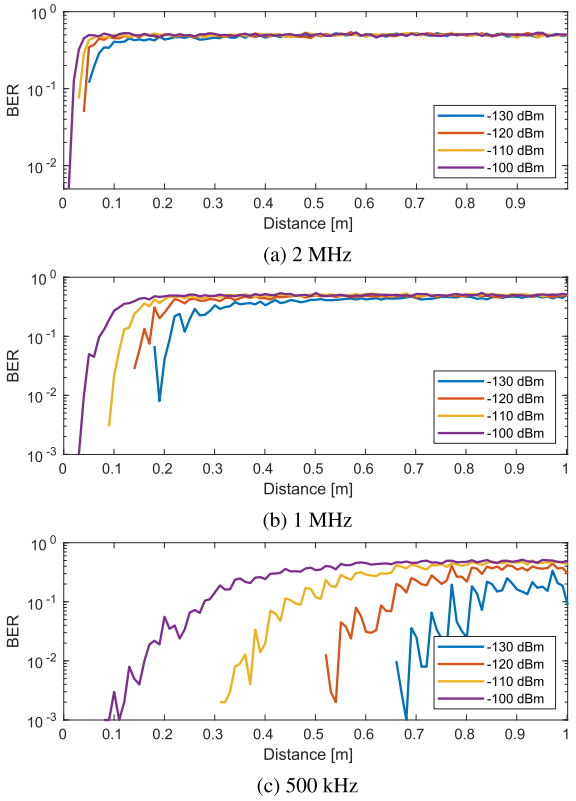


(a) 2 MHz

(b) 1 MHz

(c) 500 kHz

FIGURE 9. Acoustic-signal attenuation over distance for different transducer resonant frequencies.



(a) 2 MHz

(b) 1 MHz

(c) 500 kHz

FIGURE 10. Bit-error ratio BER over distance with respect to different noise-floor levels.

Δf is the transducer bandwidth.

$$\bar{n}_t = \sqrt{4k_B T R \Delta f} \tag{2}$$

Then, to see the effects of both the noise components ($n_t(t)$ and $n_a(t)$) on the demodulated signal, we use the overall noise floor N_{dBm}, which is calculated using (3).

$$N_{dBm} = \underbrace{10 \cdot \log_{10}\left(\frac{\bar{n}_t^2}{4R}\right)}_{\text{due to the transducer}} + \underbrace{10 \cdot \log_{10}\left(1 + \left(\frac{\bar{n}_a}{\bar{n}_t g_a}\right)^2\right)}_{\text{amplifier noise figure}} + \underbrace{10 \cdot \log_{10}(1000)}_{\text{dB to dBm conversion}} \tag{3}$$

We assume that the attacker is using an advanced, very-high-gain and very-low-noise receiver. Since the N_{dBm} of the receive chain depends on the exact implementation, we provide the BER plots with respect to a range of noise floors (see Figure 10). As a reference, for a 2-MHz ultrasound transducer with a 1-MHz bandwidth and its resistance tuned to 50 Ω, and an example advanced amplifier [36] having a 50-Ω input resistance, an input noise of 2.3 nV/$\sqrt{\text{Hz}}$ and a 60 dB gain, the overall noise floor ≈ -114 dBm at 20 °C. From Figure 10, it can be observed that for a digital acoustic signal originating from the IMD, successfully demodulating it over the air medium for a 2-MHz transducer is not possible beyond 5 cm. For a 500-kHz transducer, the eavesdropping range increases to around 60 cm for an extremely-low −130 dBm noise floor. This analysis indicates that the eavesdropping attack is physically unrealistic to launch when using a transducer with a resonant frequency in the MHz range.

We now perform the eavesdropping analysis from a different perspective, i.e., by considering the impact of the ultrasound-wave directivity, which primarily depends on the transducer frequency and width. This analysis allows us to confirm that even if the attacker is very close by, the directivity needs to be maintained in order to successfully eavesdrop.

For a transducer 5 mm wide, which is among the typical sizes used in WPT and BCC [24], the directivity plots are shown in Figure 11. After emanating from the transducer, the signal first traverses through layers of fat (4 mm), skin (2 mm) and ultrasound gel (1 mm) before entering the air medium. Although such layers are simulated, k-Wave is used by professionals in the ultrasound field to accurately assess material attenuation due to its advanced numerical model. We can observe that the transducers of MHz-range frequencies are highly directional. This is also supported by the BER plots with respect to the distance along the skin, i.e., along the direction parallel to the face of the IMD transducer, as shown in Figure 12. The BER worsens if the alignment is disturbed by even a couple of centimeters. These tests show that, in addition to being *very* close, the attacker also has to maintain a strict line-of-sight alignment with the IMD transducer. Even a subtle movement of the patient, e.g., when they are breathing, will cause disruption in the eavesdropping.

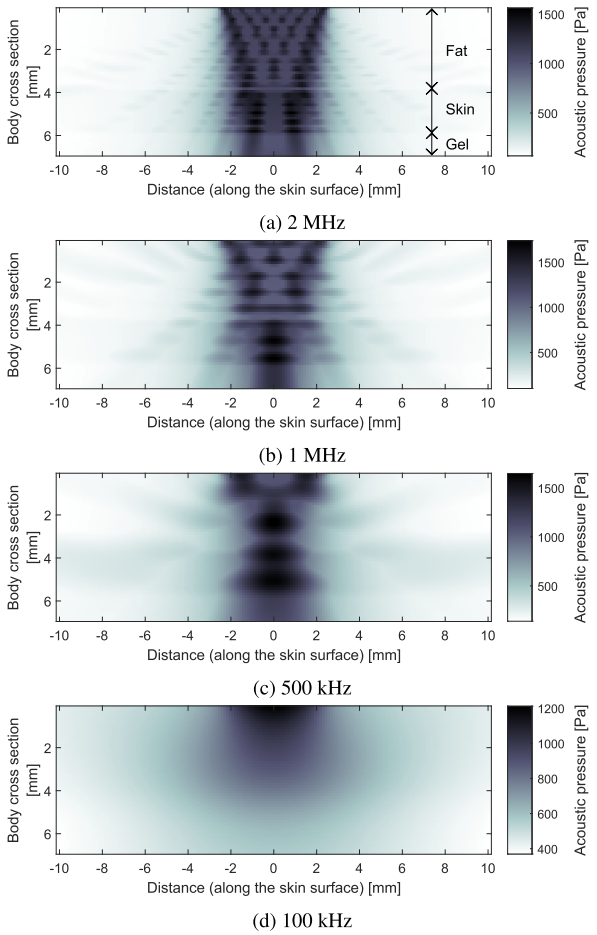


FIGURE 11. Directivity tests for 5-mm width transducers.

B. BATTERY-DoS AND ACTIVE ATTACKS

Since the IMD employs a passive ultrasound receiver with no amplification, the onus is on the attacker to pre-amplify (with gain g_a) the input signal, $s_A(t)$, of their transducer (see Figure 4) so that the DC level of the wakeup/received signal ($r_I(t)$) at the IMD side is greater than the logic level '1' threshold (V_{thr}) of the IMD-MCU's GPIO pin. For a worst-case approximation (best case for the attacker), we only include the effects of acoustic *attenuation* and do not consider acoustic-signal *distortion* since it is irrelevant when the aim of the attacker is to overcome V_{thr} at the IMD. As a result, $h(t) \approx g_{ch} \cdot \delta(t-\tau)$, where g_{ch} is the overall transmission coefficient of the heterogeneous acoustic medium, defined in (4), and τ is the introduced delay.

$$g_{ch} = 2^{n-1} \cdot \prod_{i=1}^{n-1} \frac{Z_{i+1}}{(Z_i + Z_{i+1})}, \quad \forall\, n \in \mathbb{Z}^+ \;\; n > 1 \tag{4}$$

Here, n is the number of medium changes the acoustic signal undergoes during transit. Based on the above approximation and (1), the attacker then has to satisfy (5) in order to successfully launch an active (message-insertion) attack.

$$|g_a \cdot g_{ch} \cdot s_A(t-\tau) + n(t)|_{max} > V_{thr} \tag{5}$$

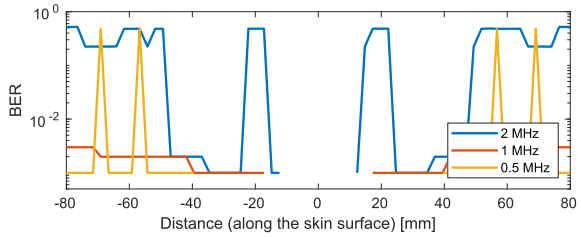


FIGURE 12. BER of the received acoustic signal along the skin with the assumed noise floor of −130 dBm.

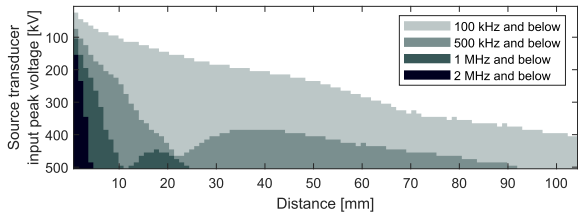


FIGURE 13. Supply voltages required by the attacker in order to successfully launch a battery-DoS attack over air with respect to different resonant frequencies and distances. A non-white grid point represents a successful attack.

However, as shown by the acoustic simulations in Figure 13, it would require an unrealistically high signal amplitude to launch a successful attack. For even a slight air gap, the attacker would need to apply a few hundreds of kilovolts at the source transducer, which is not practical at all. The reason for this is that g_{ch} from the (attacker) transducer to air is $\sim 2.6 \times 10^{-5}$ for a Lead-Zirconate-Titanate (PZT) transducer, which is insurmountable in the absence of any amplification at the IMD side. To make matters worse for the attacker, the directivity discussion from Section IV-A applies here as well.

C. SIDE-CHANNEL ATTACKS

It has been shown [9], [37] that it is possible for the acoustic circuit to get a signal from the RF receiver chain due to interference, effectively resulting in the reception of an unwanted acoustic signal. This phenomenon can lead to active signal-injection attacks from the adversary. However, this can easily be prevented by adding electromagnetic shielding over the ultrasound circuitry [9], [38], which is addressed in the system architecture (see Section III-C). This shielding also prevents the electromagnetic signals (corresponding to the signals driving the IMD transducer) to leak out of the IMD, which protects against the potential eavesdropping.

D. SUMMARY

In this section, we demonstrated through realistic simulations that ultrasound BCC is sufficiently secure when using a transducer that is sensitive to frequencies $\geq$ 1 MHz. Based on our analysis, it can be concluded with certainty that the attacker would not be able to successfully launch eavesdropping, message-insertion and battery-DoS attacks: They would need to get really close (within a few millimeters), maintain directivity, and in the case of message-insertion and battery-DoS attacks, would need to bring impractically-large-sized

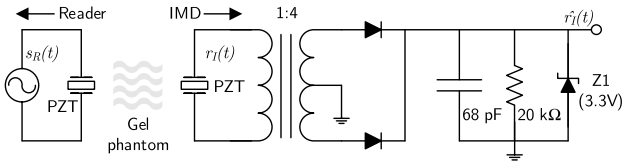


FIGURE 14. Rectification circuit for the proof-of-concept implementation.

FIGURE 15. Mediums/Phantoms employed: Standoff Gel (top left), chicken breast (top right) and human hand (bottom).

equipment on site. The analysis is also valid for even more conservative threat models [2] that assume the attacker being able to get close to the patient in a *crowded* place.

V. PROOF-OF-CONCEPT IMPLEMENTATION

In Section IV, we concluded that the ultrasound transducers of MHz frequencies are sufficiently secure. In this section, we will practically demonstrate that such transducers can be actually used for secure device pairing and ZPD.

For our proof-of-concept design, a 2.25 MHz ultrasound PZT transducer from Panametrics (model: V306) [34] with a transmit efficiency of 3.8 kPa/V is employed. A 32-bit ultra-low-power MCU from Silicon Labs, Tiny Gecko [39], is employed as the IMD security MCU.

The BCC receive path consists of a PZT and a rectification circuit (see Figure 7), which is also used for generating the wakeup signal: The high-frequency sinusoid at the output of the PZT is rectified into a digital (demodulated) signal, which is connected to the MCU BCC-RX and wakeup-interrupt pins. The transmit path, on the other hand, is much simpler: the MCU BCC-TX pin is directly connected to the PZT (similarly to [18]). In this case, the MCU performs the ASK modulation by generating a 2.25 MHz signal using its internal high-frequency-RC oscillator for a bit-period duration to represent a '1'. The absence of this signal represents a '0'.

As discussed in Section III-C, the rectification circuit has to be passive in order to achieve *true* ZPD. As a result, the amplification of both the transmit and receive signals has to be done at the reader side. However, this is not problematic since the power constraints at the reader are sufficiently relaxed compared to the IMD.

The rectifier schematic is shown in Figure 14, which is designed so that the reader can communicate and wake up the implant when the ultrasound probe is placed on the body at

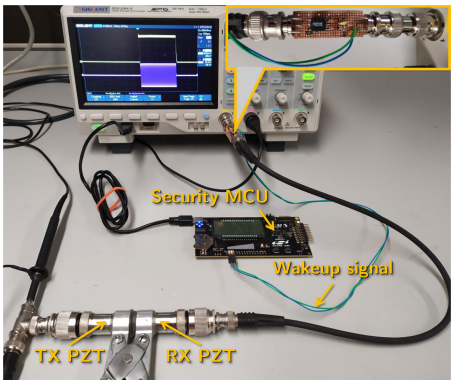


FIGURE 16. Experimental setup.

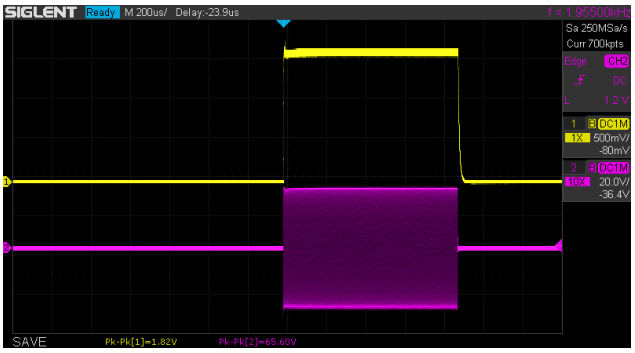


FIGURE 17. Oscilloscope snapshot of the $s_R(t)$ (magenta) and $\hat{r}_I(t)$ (yellow) signals.

the point closest to the IMD. We used four different mediums/phantoms between the source and receiver PZTs (see Figure 15 and Table 2). The best-case medium (in terms of maximum acoustic-energy transfer) was the homogeneous standoff gel, whereas the worst-case[3] mediums were the adductor-pollicis-muscle regions (between the index finger and the thumb) of two subjects. Figure 16 shows the proof-of-concept implementation setup. Figure 17 shows the oscilloscope snapshot of the input to the reader PZT, $s_R(t)$, and the resulting IMD rectifier output, $\hat{r}_I(t)$. The small number of components in the rectifier allows it to easily fit in any IMD class, along with the above-mentioned PZT. Table 2 lists the minimum required peak voltages of $s_R(t)$, which result in the $\hat{r}_I(t)$ having a DC level $\approx$ 1.8 V, which can successfully wake up the MCU and also represent a logic level '1' when receiving data. It can be seen that the TX energy transferred through the medium is small enough (i.e., less than 15 mJ) to fall within the budget of a battery-powered portable reader. It should be noted that the calculated acoustic power transferred through the medium and that too for a small duration of time, i.e., for sending ID_R and N_R (see Figure 5), is comfortably within the FDA safety limits [35].

[3]This medium has two skin layers which results in more acoustic losses compared to an actual case, such as an implanted pacemaker, in which there is one skin layer (in addition to fat) between the reader and the IMD.

TABLE 2. Measurements from the implementation setup.

Medium/Phantom	Thickness (mm)	Min. required peak $s_R(t)$ (V)	Dissipated[§] TX power (W)	Dissipated TX Energy[*] (mJ)
Standoff Gel	6	32.5	0.77	7.88
Chicken breast	5.5	34.5	0.87	8.91
Hand[**] (subject 1)	4	44	1.41	14.44
Hand (subject 2)	5	39	1.11	11.37

[§] Acoustic power transferred through the medium from the reader
[*] At a data rate of 50 kbps for a packet size of 512 bits
[**] Adductor-pollicis-muscle region (between the index finger and the thumb)

TABLE 3. Comparison of SecureEcho with EH-ZPD.

Design consideration	SecureEcho	EH-ZPD
Frequency-band constraints	+	−
Medical-safety constraints	+	−
Operating range (bedside-base-station operation)	+	−
Emergency access	+	−
Design suitability	+	−
Dependability	+	−
Secure device pairing	+	−
Device usability	−	+
Energy overheads	+	+

+/−: relatively good/poor performance

VI. COMPARISON WITH EH-ZPD

We now compare SecureEcho with the traditional energy-harvesting-based ZPD (EH-ZPD) approach. An overview of this comparison is provided in Table 3. Next, we will go over the comparison points one by one.

A. FREQUENCY-BAND AND SAFETY CONSTRAINTS

The Federal Communications Commission (FCC) does not allow an equivalent isotropically radiated power (EIRP) greater than 25 μW on the MedRadio frequency band, which is reserved for reader-IMD communication. This limit is too low for applications requiring wireless power transfer (WPT). As a result, for an EH-ZPD design, a different band should be used for energy harvesting. This requires a separate antenna, and hence, results in the increased cost and size [7]. This can be overcome by using a 13.56 MHz ISM band for *both* the data communication and WPT. However, due to the smaller bandwidth of the ISM band compared to MedRadio, this solution would result in lower supported data rates. Since SecureEcho does not require energy harvesting, it does not need a separate band for WPT, which eases up frequency-band constraints. Moreover, the medical-safety constraints imposed by the FDA are relatively easier to meet in the case of ultrasound compared to EH-ZPD since the limit for ultrasound power transmission into the tissue is higher compared to that of electromagnetic power transfer [24].

B. OPERATING RANGE

SecureEcho allows the use of a bedside base-station reader after its initial BCC pairing with the IMD. On the other hand, in the case of EH-ZPD, harvesting RF energy over the bedside range (a few feet) requires larger antennas/coils, and longer delays due to the charging of the energy reservoir, which complicates the IMD design [7].

C. EMERGENCY ACCESS

In the case of a paramedic access to the IMD in an emergency scenario, one main requirement is to provide trust establishment between the reader-IMD pair without any pre-shared secret between the two entities. This is reasonable to assume because in emergencies, the paramedic reader and the patient IMD are likely unknown to each other. SecureEcho inherently provides this feature since the secret (symmetric key) can be transported securely using the ultrasound channel. Moreover, since this transfer requires a physical contact, it satisfies the touch-to-access assumption. On the other hand, an IMD with EH-ZPD cannot establish trust on its own, and therefore, would still require a pairing mechanism.

D. DESIGN SUITABILITY

The EH-ZPD architecture has many moving parts in addition to the transceiver, such as a harvesting circuit, power management and an energy reservoir (see Figure 2). On the other hand, an ultrasound-coupling-based BCC transceiver is much simpler (as demonstrated in Section V). This gives it an advantage in terms of *design suitability*, i.e., the tedious approval cycle of such a ZPD module is likely to be much shorter than a harvesting-based design.

E. DEPENDABILITY

1) RELIABILITY

Related to the discussion in Section VI-D, since SecureEcho has a lower number of electronic components, it aids in *dependability* since each such component has an associated failure rate. This is important to consider for safety-critical systems, such as IMDs.

2) MAINTAINABILITY

In the case of EH-ZPD, since the authentication is executed using free energy, the harvesting circuit and the energy reservoir (such as a supercapacitor) have to be designed according to the required authentication energy. It is possible that, in the future, the employed cryptographic primitives may require replacing (via over-the-air firmware updates) due to newly found vulnerabilities. However, this may require the replacement of the harvesting circuitry as well, which is not possible for an already implanted device. This is not a problem for

SecureEcho since the BCC circuit is agnostic to the employed cryptographic primitives.

F. SECURE DEVICE PAIRING

In general, in the absence of a trusted-third party, for any two devices requiring key-exchange (for supporting confidentiality, integrity and authentication), they need to perform asymmetric (or public-key) cryptography. Public-key cryptography is also required if the devices need to support non-repudiation. To protect against man-in-the-middle (MITM) attack, which is a common attack against public-key cryptography, the devices require the use of certificates and a public-key infrastructure (PKI). However, when it comes to IMDs, they only have a limited on-board memory, which is problematic for storing necessary certificates, and they lack an Internet connection, which is required to track the validity of all possible reader certificates [40]. One way of getting around the need for certificates is for the IMD to verify that the reader is in close proximity, or in other words, enforce the touch-to-access principle [4], [41]. Similarly to what was discussed regarding emergency access above, SecureEcho inherently ensures proximity between the reader and the implant, which is not the case for EH-ZPD, as it would still require a touch-to-access scheme.

Related to above, SecureEcho can act as a robust pairing method (or in other words, *association model*) for existing communication standards like Bluetooth LE, which is increasingly being employed in modern reader-IMD systems. Bluetooth LE offers four association models: *Just Works*, *Passkey*, *Numeric comparison* and *OOB (out-of-band) pairing* [42]. Just Works does not offer MITM protection, whereas the passkey and numeric comparison require a user interface on the device (e.g., a touch screen), which is not possible for an implant. OOB pairing is an ideal association model for Bluetooth-LE-enabled IMDs, and SecureEcho can slot in as an OOB channel with minimal modifications.

G. DEVICE USABILITY

In terms of device usability, the main difference between SecureEcho and EH-ZPD is that the former requires a water-based ultrasound gel to be applied on the skin before the initial pairing. However, this is *not* required for subsequent accesses between the already paired devices. Moreover, the initial gel application can be considered as acceptable given that such a practice is already prevalent in ultrasonography.

H. ENERGY OVERHEADS

The SecureEcho pairing is only employed infrequently, since the devices that are already paired do not need to repeat it. As a result, the additional energy overhead introduced by SecureEcho has a negligible impact on the IMD lifetime (see Sections VI-H1 and VI-H2 for details). Also, given that EH-ZPD would still require a touch-to-access scheme (as discussed in Section VI-C), the overall solution will exhibit similar or higher energy consumption than SecureEcho.

1) DETERMINING ENERGY OVERHEADS

The total energy consumption for an IMD that provides basic security (without ZPD) is stated in (6). E_{sec} includes the energy consumed by the security computations, data handling and the RF transceiver. E_{med} includes the energy consumed by the medical application, the sensing of physiological signals, and the electrical stimulation applied on the human tissue [7].

$$E_{total} = E_{med} + E_{sec} \tag{6}$$

In the case of SecureEcho, E_{sec} is shown in (7). Here, P_{MCU} is the average active-mode power consumption of the security MCU. P_{RF} is the average active-mode power consumption of the RF transceiver. t_{auth} and t_{main} are the durations of the authentication and main (data-transfer) phases, respectively. t_{BCC} is the time taken by the BCC key-exchange. t_{total} is the duration over which the energy is being calculated. Lastly, P_{sleep} is the average sleep-mode consumption of the security MCU and the RF transceiver.

$$\begin{aligned} E_{sec}^{BCC} &= P_{MCU} \cdot t_{BCC} \\ &\quad + (P_{MCU} + P_{RF}) \cdot (t_{auth} + t_{main}) \\ &\quad + P_{sleep} \cdot (t_{total} - t_{BCC} - t_{auth} - t_{main}) \end{aligned} \tag{7}$$

For EH-ZPD, in which the authentication phase is executed on free energy, E_{sec} is shown in (8).

$$E_{sec}^{EH} = (P_{MCU} + P_{RF}) \cdot t_{main} \tag{8}$$

For $t_{total} \gg t_{BCC}, t_{auth}, t_{main}$, i.e., over a very long course of time and coupled with the fact that the pairing only has to be done when it is reset (i.e., seldom), and $t_{main} \gg t_{auth}$, the overhead introduced by SecureEcho becomes:

$$\Delta E_{sec} = E_{sec}^{BCC} - E_{sec}^{EH} \approx P_{sleep} \cdot t_{total} \tag{9}$$

With the lowest-energy-mode currents in modern MCUs getting lower than 100 nA [39], the above overhead has a negligible impact on the IMD lifetime, as discussed next.

2) IMPACT ON BATTERY LIFE

Taking the example of a typical pacemaker, we now calculate the impact of SecureEcho on the IMD battery life compared to using EH-ZPD.

We use the same MCU from Section V for this analysis. In addition, we use an implantable-grade RF transceiver, Microsemi ZL70103 [43] as an example. The specifications of this setup are shown in Table 4. The differences between the expected battery lifetimes, when using SecureEcho compared to EH-ZPD, are shown in Figure 18. It is clear that the impact of SecureEcho is hardly noticeable.

I. DISCUSSION

From the above analysis, it can be concluded that SecureEcho significantly outperforms EH-ZPD, except in the case of device usability because of the minor requirement of using a water-based medium or gel *before* the pairing process. However, this is *not* required for subsequent accesses between

TABLE 4. Specifications of a typical pacemaker.

Parameter	Value
Supply voltage	3.3 V
MCU-processor clock frequency	19 MHz (default value) [39]
RF-transceiver effective data rate	265 kbps (maximum value) [43]
Active-data-comm. duration	3 minutes per day [44]
Pacemaker stimulation energy	20 μJ per heartbeat [45]

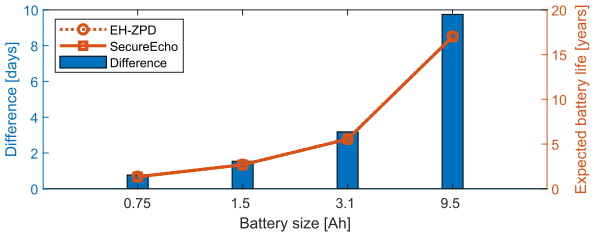


FIGURE 18. Differences between the expected battery lifetimes when using SecureEcho compared to EH-ZPD.

the already paired devices, i.e., during the normal use of the reader. Moreover, EH-ZPD is dependent on a pre-existing OOB pairing scheme (in the absence of an Internet connection). On the other hand, SecureEcho elegantly provides *both* secure device pairing and ZPD.

VII. CONCLUSION

In this work, we have presented SecureEcho, a secure device-pairing scheme for reader-IMD systems that inherently provides protection against battery-depletion attacks. We have shown that the ultrasound channel used in the pairing process is sufficiently secure at MHz-range frequencies. We have also demonstrated a proof-of-concept implementation of the passive circuit that enables the pairing process and ZPD. We conclude that SecureEcho outperforms the traditional EH-ZPD in terms of satisfying frequency-band and medical-safety constraints, operating range, emergency access, design suitability and dependability.

REFERENCES

[1] 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 Symp. Secur. Privacy (SP)*, May 2008, pp. 129–142.

[2] E. Marin, D. Singelée, F. D. Garcia, T. Chothia, R. Willems, and B. Preneel, "On the (in)security of the latest generation implantable cardiac defibrillators and how to secure them," in *Proc. 32nd Annu. Conf. Comput. Secur. Appl.*, Dec. 2016, pp. 226–236.

[3] E. Marin, D. Singelée, B. Yang, V. Volski, G. A. E. Vandenbosch, B. Nuttin, and B. Preneel, "Securing wireless neurostimulators," in *Proc. 8th ACM Conf. Data Appl. Secur. Privacy*, Mar. 2018, pp. 287–298.

[4] M. Rostami, A. Juels, and F. Koushanfar, "Heart-to-heart (H2H): Authentication for implanted medical devices," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, 2013, pp. 1099–1112.

[5] M. A. Siddiqi, C. Doerr, and C. Strydis, "IMDfence: Architecting a secure protocol for implantable medical devices," *IEEE Access*, vol. 8, pp. 147948–147964, 2020.

[6] M. A. Siddiqi and C. Strydis, "Towards realistic battery-DoS protection of implantable medical devices," in *Proc. 16th ACM Int. Conf. Comput. Frontiers*, Apr. 2019, pp. 42–49.

[7] M. A. Siddiqi, W. A. Serdijn, and C. Strydis, "Zero-power defense done right: Shielding IMDS from battery-depletion attacks," *J. Signal Process. Syst.*, vol. 93, pp. 1–17, Apr. 2020.

[8] F. Putz, F. Álvarez, and J. Classen, "Acoustic integrity codes: Secure device pairing using short-range acoustic communication," in *Proc. 13th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, Jul. 2020, pp. 31–41.

[9] K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, and S. Capkun, "Proximity-based access control for implantable medical devices," in *Proc. 16th ACM Conf. Comput. Commun. Secur. (CCS)*, 2009, pp. 410–419.

[10] R. Mayrhofer and H. Gellersen, "On the security of ultrasound as out-of-band channel," in *Proc. IEEE Int. Parallel Distrib. Process. Symp.*, Mar. 2007, pp. 1–6.

[11] R. M. Seepers, J. H. Weber, Z. Erkin, I. Sourdis, and C. Strydis, "Secure key-exchange protocol for implants using heartbeats," in *Proc. ACM Int. Conf. Comput. Frontiers*, May 2016, pp. 119–126.

[12] V. Pournaghshband, M. Sarrafzadeh, and P. Reiher, "Securing legacy mobile medical devices," in *Proc. Int. Conf. Wireless Mobile Commun. Healthcare*. Berlin, Germany: Springer, 2012, pp. 163–172.

[13] J. Sorber, M. Shin, R. Peterson, C. Cornelius, S. Mare, A. Prasad, Z. Marois, E. Smithayer, and D. Kotz, "An amulet for trustworthy wearable mhealth," in *Proc. 12th Workshop Mobile Comput. Syst. Appl.*, 2012, p. 7.

[14] Y. Kim, W. S. Lee, V. Raghunathan, N. K. Jha, and A. Raghunathan, "Vibration-based secure side channel for medical devices," in *Proc. 52nd Annu. Design Automat. Conf.*, Jun. 2015, p. 32.

[15] W. J. Tomlinson, S. Banou, C. Yu, M. Stojanovic, and K. R. Chowdhury, "Comprehensive survey of galvanic coupling and alternative intra-body communication technologies," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1145–1164, 2nd Quart., 2019.

[16] M. Roeschlin, I. Martinovic, and K. B. Rasmussen, "Device pairing at the touch of an electrode," in *Proc. NDSS*, vol. 18, 2018, pp. 18–21.

[17] M. S. Wegmüller, "Intra-body communication for biomedical sensor networks," Ph.D. dissertation, ETH Zürich, Zürich, Switzerland, 2007.

[18] G. E. Santagati and T. Melodia, "An implantable low-power ultrasonic platform for the Internet of medical things," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, May 2017, pp. 1–9.

[19] C. Li, A. Raghunathan, and N. K. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," in *Proc. IEEE 13th Int. Conf. e-Health Netw., Appl. Services*, Jun. 2011, pp. 150–156.

[20] G. E. Santagati, N. Dave, and T. Melodia, "Design and performance evaluation of an implantable ultrasonic networking platform for the Internet of medical things," *IEEE/ACM Trans. Netw.*, vol. 28, no. 1, pp. 29–42, Feb. 2020.

[21] Z. Kashani and M. Kiani, "Optimal ultrasonic pulse transmission for miniaturized biomedical implants," in *Proc. IEEE Biomed. Circuits Syst. Conf. (BioCAS)*, Oct. 2019, pp. 1–4.

[22] B. Jaafar, A. Soltan, J. Neasham, and P. Degenaar, "Wireless ultrasonic communication for biomedical injectable implantable device," in *Proc. 41st Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBC)*, Jul. 2019, pp. 4024–4027.

[23] R. V. Taalla, M. S. Arefin, A. Kaynak, and A. Z. Kouzani, "A review on miniaturized ultrasonic wireless power transfer to implantable medical devices," *IEEE Access*, vol. 7, pp. 2092–2106, 2019.

[24] H. Basaeri, D. B. Christensen, and S. Roundy, "A review of acoustic power transfer for bio-medical implants," *Smart Mater. Struct.*, vol. 25, no. 12, Dec. 2016, Art. no. 123001.

[25] K.-W. Yang, K. Oh, and S. Ha, "Challenges in scaling down of free-floating implantable neural interfaces to millimeter scale," *IEEE Access*, vol. 8, pp. 133295–133320, 2020.

[26] D. Seo, R. M. Neely, K. Shen, U. Singhal, E. Alon, J. M. Rabaey, J. M. Carmena, and M. M. Maharbiz, "Wireless recording in the peripheral nervous system with ultrasonic neural dust," *Neuron*, vol. 91, no. 3, pp. 529–539, Aug. 2016.

[27] T. Halevi and N. Saxena, "On pairing constrained wireless devices based on secrecy of auxiliary channels: The case of acoustic eavesdropping," in *Proc. 17th ACM Conf. Comput. Commun. Secur. (CCS)*, 2010, pp. 97–108.

[28] C. Strydis, R. M. Seepers, P. Peris-Lopez, D. Siskos, and I. Sourdis, "A system architecture, processor, and communication protocol for secure implants," *ACM Trans. Archit. Code Optim.*, vol. 10, no. 4, p. 57, 2013.

[29] B. E. Treeby and B. T. Cox, "K-wave: MATLAB toolbox for the simulation and reconstruction of photoacoustic wave fields," *J. Biomed. Opt.*, vol. 15, no. 2, 2010, Art. no. 021314.

[30] E. Martin, J. Jaros, and B. E. Treeby, "Experimental validation of k-wave: Nonlinear wave propagation in layered, absorbing fluid media," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 67, no. 1, pp. 81–91, Jan. 2020.

[31] A. Grisey, M. Heidmann, V. Letort, P. Lafitte, and S. Yon, "Influence of skin and subcutaneous tissue on high-intensity focused ultrasound beam: Experimental quantification and numerical modeling," *Ultrasound Med. Biol.*, vol. 42, no. 10, pp. 2457–2465, Oct. 2016.
[32] P. Hasgall, F. Di Gennaro, C. Baumgartner, E. Neufeld, B. Lloyd, M. Gosselin, D. Payne, A. Klingenböck, and N. Kuster, "IT'IS database for thermal and electromagnetic parameters of biological tissues version 4.0," IT'IS Found., Zürich, Switzerland, Database Version 4.0, May 2018, doi: 10.13099/VIP21000-04-0.
[33] A. Vladišauskas and L. Jakevičius, "Absorption of ultrasonic waves in air," *Ultragarsas*, vol. 50, no. 1, pp. 46–49, 2004.
[34] *Panametrics Ultrasonic Transducers—Wedges, Cables, Test Blocks*, Olympus, Tokyo, Japan, 2016.
[35] FDA. (2019). *Marketing Clearance of Diagnostic Ultrasound Systems and Transducers—Guidance for Industry and FDA Staff*. [Online]. Available: https://www.fda.gov/media/71100/download
[36] Femto. (2020). *100/200 MHZ Wideband Voltage Amplifier Series DHPVA*. [Online]. Available: https://www.femto.de/en/products/voltage-amplifiers/variable-gain-100-200-mhz-dhpva.html
[37] I. Giechaskiel, Y. Zhang, and K. B. Rasmussen, "A framework for evaluating security in the presence of signal injection attacks," in *Proc. Eur. Symp. Res. Comput. Secur.* Cham, Switzerland: Springer, 2019, pp. 512–532.
[38] I. Giechaskiel and K. Rasmussen, "Taxonomy and challenges of out-of-band signal injection attacks and defenses," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 645–670, 1st Quart., 2020.
[39] *EFM32 Tiny Gecko 11 Family—Reference Manual*, Silicon Labs, Austin, TX, USA, 2018.
[40] E. M. Fàbregas, "Security and privacy of implantable medical devices," Ph.D. dissertation, KU Leuven, Leuven, Belgium, 2018.
[41] M. A. Siddiqi and C. Strydis, "IMD security vs. energy: Are we tilting at windmills?: POSTER," in *Proc. 16th ACM Int. Conf. Comput. Frontiers*, Apr. 2019, pp. 283–285.
[42] M. Bon. (2016). *A Basic Introduction to BLE Security*. [Online]. Available: https://www.digikey.com/eewiki/display/Wireless/A+Basic+Introduction+to+BLE+Security
[43] *ZL70103 Medical Implantable RF Transceiver*, Microsemi, Aliso Viejo, CA, USA, 2015.
[44] *FAQs—Merlin.net Patient Care Network (PCN) 8.0 Q&A*, St. Jude Med., St. Paul, MN, USA, 2015.
[45] M. Deterre, "Toward an energy harvester for leadless pacemakers," M.S. thesis, Univ. Paris Sud, Orsay, France, Jul. 2013. [Online]. Available: https://tel.archives-ouvertes.fr/tel-00868838

MUHAMMAD ALI SIDDIQI received the B.E. degree in electrical (telecommunication) engineering from the National University of Sciences and Technology, Islamabad, Pakistan, in 2009, and the joint M.Sc. degree in embedded computing systems from the Norwegian University of Science and Technology, Trondheim, Norway, and the University of Southampton, U.K., in 2012. He is currently pursuing the Ph.D. degree with the Neuroscience Department, Erasmus Medical Center, The Netherlands.

From 2012 to 2017, he worked as a Design Engineer at Silicon Labs Norway, with a focus on the ultra-low-power MCU design. His research interests include the development of security protocols and architectures for heavily resource-constrained embedded systems, such as implantable medical devices.

ROBERT H. S. H. BEURSKENS received the B.Sc. degree in electrical engineering from Fontys Hogeschool Venlo, The Netherlands, in 1997. After pursuing his degree, he started working at Hauzer Techno Coating, Venlo, The Netherlands, as an Electrical Engineer, working on industrial scale physical vapor deposition (PVD) equipment. In 1999, he started to work at the Prins Maurits Laboratorium, Rijswijk, The Netherlands, a branch of the Dutch Organization for Applied Physics TNO. Since 2007, he has been with the Department of Biomedical Engineering, Erasmus Medical Center, Rotterdam, The Netherlands, as an Electronic Designer and an Instrumentation Technician. His research interests include design, construction and operation of high voltage pulsed power systems for all kinds of civil and defense applications varying from foodstuff sterilization, atmospheric plasmas to electric reactive armor, countermeasures, analog, and high-frequency electronics for ultrasound applications.

PIETER KRUIZINGA received the M.Sc. degree in biomedical engineering from the Delft University of Technology and the Ph.D. degree in ultrasound and photoacoustic imaging from Erasmus University Rotterdam, The Netherlands. His postdoctoral research shifted focus toward ultrasound imaging, where he developed techniques for computational ultrasound and functional ultrasound imaging. In 2018, he joined the Department of Neuroscience as an Assistant Professor. With help of a large multi-million-euro investment grant, he recently co-founded Center of Ultrasound Brain Imaging at Erasmus MC (CUBE). This new center combines imaging science, neuroscience, and neurosurgery to better understand the brain and brain diseases.

CHRIS I. DE ZEEUW received the Ph.D. degree *(cum laude)* in focus on brain and behavior and the M.D. degree *(cum laude)* from Erasmus University Rotterdam, in 1990 and 1991, respectively. He is the Chairman of the Department of Neuroscience, Erasmus Medical Center, Rotterdam, the Vice-Director at the Netherlands Institute for Neuroscience. Amsterdam, and the Director of Neurasmus BV. Soon after that he received the Fellowship Award from de Royal Dutch Academy of Sciences (KNAW) and became a Visiting Professor at NYU Med School, New York. When he returned to The Netherlands, he became a Full Professor and the Chair of the Department that he founded in Rotterdam around the turn of the new millennium. He has been the Principal Coordinator of the EU Robotics Program (SENSOPAC) and the President of Neuro-Bsik Mouse- and Pharma-Phenomics Consortia. He was received over 100 grants, including the PIONIER Award from ZonMw and the ERC Advanced Grant. In 2006, he received the Beatrix Award for Brain Research from Her Majesty the Queen, in 2014, he became an Elected Member of the Dutch Academy of Arts and Science, and in 2018, he received the international Casella Prize for Physiology.

CHRISTOS STRYDIS (Senior Member, IEEE) received the M.Sc. *(magna cum laude)* and Ph.D. degrees in computer engineering from the Delft University of Technology. He is currently a Tenured Assistant Professor in computer engineering and the Head of the NeuroComputing Laboratory, Neuroscience Department, Erasmus Medical Center, The Netherlands. He has published work in well-known international conferences and journals. He has delivered invited talks in various venues. His current research interests include brain simulations, high-performance computing, low-power embedded (implantable) systems, and functional ultrasound imaging.