

**Zero-Power Defense Done Right
Shielding IMDs from Battery-Depletion Attacks**

Siddiqi, Muhammad Ali; Serdijn, Wouter A.; Strydis, Christos

DOI

[10.1007/s11265-020-01530-5](https://doi.org/10.1007/s11265-020-01530-5)

Publication date

2020

Document Version

Final published version

Published in

Journal of Signal Processing Systems

Citation (APA)

Siddiqi, M. A., Serdijn, W. A., & Strydis, C. (2020). Zero-Power Defense Done Right: Shielding IMDs from Battery-Depletion Attacks. *Journal of Signal Processing Systems*, 93 (2021)(4), 421–437.
<https://doi.org/10.1007/s11265-020-01530-5>

Important note

To cite this publication, please use the final published version (if applicable).
Please check the document version above.

Copyright

Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy

Please contact us and provide details if you believe this document breaches copyrights.
We will remove access to the work immediately and investigate your claim.



Zero-Power Defense Done Right: Shielding IMDs from Battery-Depletion Attacks

Muhammad Ali Siddiqi¹ · Wouter A. Serdijn² · Christos Strydis¹

Received: 14 October 2019 / Revised: 27 February 2020 / Accepted: 5 March 2020 / Published online: 8 April 2020
© The Author(s) 2020

Abstract

The wireless capabilities of modern Implantable Medical Devices (IMDs) make them vulnerable to security attacks. One prominent attack, which has disastrous consequences for the patient's wellbeing, is the battery Denial-of-Service attack whereby the IMD is occupied with continuous authentication requests from an adversary with the aim of depleting its battery. Zero-Power Defense (ZPD), based on energy harvesting, is known to be an excellent protection against these attacks. This paper raises essential design considerations for employing ZPD techniques in commercial IMDs, offers a critical review of ZPD techniques found in literature and, subsequently, gives crucial recommendations for developing comprehensive ZPD solutions.

Keywords Implantable medical device · IMD · Energy harvesting · Wireless power transfer · Zero-power defense · Authentication protocol · Denial-of-service attack · Battery DoS · Battery-depletion attack

1 Introduction

Implantable medical devices (IMDs) such as cardiac pacemakers and defibrillators, neurostimulators, infusion pumps and more, are battery-powered devices with extremely high

safety, reliability and availability constraints. The typical operational lifetime of these autonomous devices is around a decade or so while implanted in the patient's body. Almost all of these devices are nowadays equipped with wireless connectivity via a transceiver in order to support and complement their treatment capabilities. They can communicate with an external reader (Fig. 1) for, e.g., monitoring patient health, updating IMD settings, and so on. However, and despite their benefits, such communication capabilities open the door to malicious use for stealing private patient data, effecting mis-diagnosis, or even causing physical harm. An attacker can cause physical harm either by changing the IMD functionality (e.g., by managing to send incorrect commands) or through a Denial-of-Service (DoS) attack. One such attack is the *battery-depletion* (or *battery-DoS*) attack where the attacker can force the IMD to continuously run an energy-consuming operation, which ultimately results in power loss and IMD shutdown. As indicated in an exhaustive IMD-threat-modeling analysis in [47], battery DoS is one of the easiest to mount and highly effective attacks. This is also backed by the majority of the ethical-hacking efforts in which the batteries of commercial IMDs were depleted using black-box approaches [16, 32].

It is considered that the only robust way of protecting an IMD against a battery DoS is by running the above-mentioned (energy-consuming) authentication operation using only *free* harvested energy. It can be argued that

This work is an extended version of [49], which was presented at the 16th ACM International Conference on Computing Frontiers. This paper improves the original article by (1) introducing additional design considerations in Section 4, (2) adding non-harvestingbased- ZPD works in Section 5, (3) discussing the impact of electromagnetic-noise attacks on IMDs in Section 6.2, and (4) proposing the novel concept of a standalone ZPD module along with the taxonomy of ZPD implementations in Section 6. This work has been supported by the EU-funded project SDK4ED (Grant Agreement No. 780572).

✉ Muhammad Ali Siddiqi
m.siddiqi@erasmusmc.nl

Wouter A. Serdijn
w.a.serdijn@tudelft.nl

Christos Strydis
c.strydis@erasmusmc.nl

¹ Neuroscience Department, Erasmus MC, Rotterdam, The Netherlands

² Section Bioelectronics, Delft University of Technology, Delft, The Netherlands

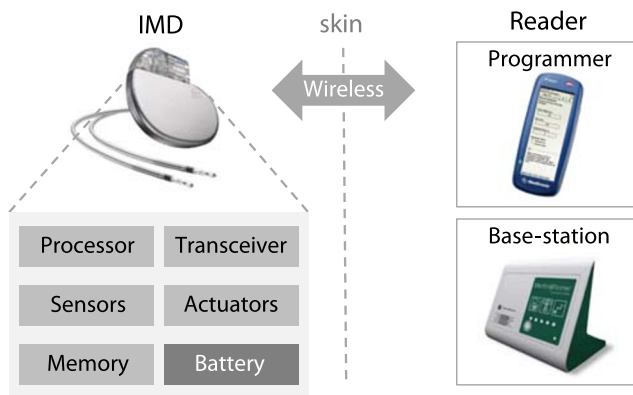


Figure 1 A Reader/IMD system.

there is no necessity for this zero-power defense (ZPD) mechanism since technology exists to wirelessly charge IMD batteries when they are running low (as discussed in Section 2, next). However, this recharging feature is only available in less critical IMDs, such as spinal-cord stimulators [1, 36]. For critical devices such as pacemakers, there is a reluctance among the medical community to give recharging responsibility to the patients, in order to avoid patient errors. Moreover, the physicians prefer to replace the whole IMD after a certain period to get the latest technology [25]. Besides, even by assuming that all IMDs have this capability, the attacker can still drain the battery before the patient or doctor has a chance to recharge it.

Energy harvesting is a widely used concept employed in a variety of devices including RFIDs. However, ZPD for IMDs introduces new challenges that do not apply in other domains. Even though there are quite a few ZPD implementations proposed in literature, to the best of our knowledge this paper is the first to facilitate the transition from *concept* to *industry-compliant* ZPD designs for IMDs. Based on a clear-cut set of design considerations, we survey and evaluate the current state of the art and proceed to propose specific recommendations for enhancing existing IMDs. Essentially, this work makes the following novel contributions:

- We consolidate ZPD design considerations for the specific domain of IMDs.
- We perform a survey of existing systems and highlight their limitations based on the above considerations.
- We provide recommendations in order to develop comprehensive protection of IMDs against battery-DoS attacks.

The rest of the paper is organized as follows. We provide a brief background on the use of energy harvesting in IMDs in Section 2, and then provide motivation for using it to enhance IMD security in Section 3. In Section 4, we provide detailed ZPD design considerations. Based on these considerations, we review and evaluate state-of-the-art ZPD solutions in Section 5. In Section 6, we provide

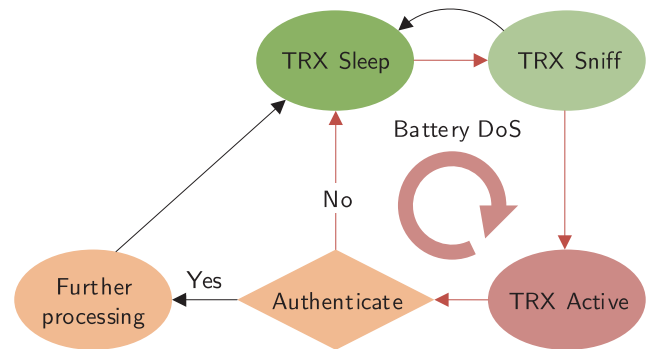


Figure 2 Battery-DoS attack: continuous traversal of the different transceiver modes and the authentication protocol.

recommendations for improving ZPD designs. We conclude the discussion in Section 7.

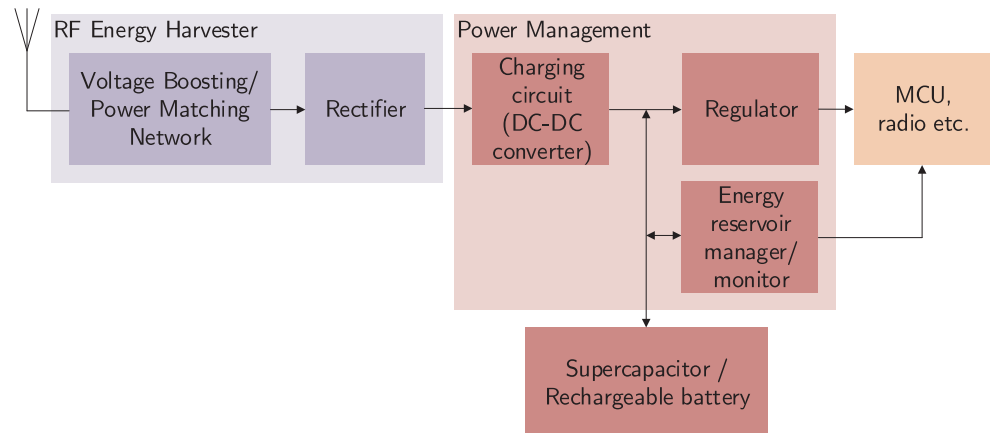
2 Energy Harvesting in IMDs

The use of energy harvesting in IMDs is not new. The application of this concept, however, has been very narrow in this domain, i.e., in wireless power transfer (WPT)¹ to recharge IMD batteries. For instance, there are several rechargeable neurostimulators that are commercially available [1, 36]. In this specific category of implants there is a rising trend towards increased IMD-power requirements due to recent advances in neuromodulation-related pain relief. For such power-hungry devices, a non-rechargeable battery would result in a very short IMD lifespan and subsequently require expensive surgeries in order to replace the battery-depleted implants. One way of avoiding this is to use larger battery sizes, which can quickly become impractical to implant. Hence, the natural solution is to use rechargeable systems, which can prevent the need for frequent surgeries and would result in smaller battery sizes and implants as a whole [37].

3 Energy Harvesting for Battery-DoS Protection

During normal IMD operation, the RF transceiver usually polls for an external entity by cycling through *sleep* and *sniff* modes [38]. The (short-duration) sniff mode consumes relatively little power compared to active transceiver operation. If the transceiver detects RF energy, it switches to its active mode in order to receive data. Battery-DoS attacks

¹The term *energy harvesting* generally refers to harvesting energy from ambient sources, whereas *WPT* refers to the intentional transfer of energy from a dedicated charging device [5]. In this paper, we use the terms interchangeably.

Figure 3 A typical WPT System (RF Energy Harvesting).

basically change the sleep-awake periods of both the IMD transceiver and the internal processor, as shown in Fig. 2.

Battery-DoS attacks can generally happen in two ways [13]: (1) They can increase the IMD activity by sending bogus communication packets. As an example, the attacker can repeatedly request the IMD to establish a secure channel using incorrect credentials. Consequently, the IMD will run part of an energy-consuming authentication protocol for analyzing every request, which will drain the battery. (2) The attacker can also generate electromagnetic (EM) noise in order to cause high error rates at the IMD transceiver, which in turn increases its energy consumption due to increased number of retransmissions. This increased noise may also force the IMD to increase the transmission power, which also reduces battery life.

In light of the fact that energy harvesting has already been employed by some classes of IMDs, the use of this concept, in the form of ZPD, has now become quintessential to protecting all IMDs against battery DoS. In this scheme, the IMD, while authenticating the external entity that is trying to communicate, can run the energy-consuming security primitives using the RF energy harvested from the incoming communication messages. The IMD is allowed to use the battery for subsequent operations *only* after the entity is authenticated. This prevents the IMD from depleting its battery to entertain continuous bogus messages from a malicious entity.

4 Design Considerations

In this section, we enumerate and discuss various considerations that should be taken into account when approaching the design of an IMD-specific ZPD system.

4.1 Choice of WPT Technique

Since ZPD is based on the concept of wireless energy harvesting, it is important to briefly discuss the WPT

techniques that enable such strategies. A typical WPT setup is shown in Fig. 3 [22, 29]. State-of-the-art IMD-specific WPT techniques can be broadly categorized into three types² [2]:

4.1.1 Inductive Coupling (IC)

Near-field or magnetostatic WPT is usually categorized as inductive coupling or inductive power transfer (IPT). IPT usually involves the use of two coupled coils that have the same inductance. The transmitter coil is placed outside the body. When an AC current passes through it, voltage is induced due to electromagnetic induction in the receiver coil, which is located inside the body. IPT is the dominant method that is used to wirelessly recharge commercial IMDs, specifically neurostimulators [1, 36].

4.1.2 Radio Frequency (RF)

If the transfer is in the transition region (mid field) [18] or far field, then the WPT system is usually categorized as RF or electromagnetic power transfer (RFPT). Here, antennas are not just limited to coils for the transmission of power. A typical RFPT system is shown in Fig. 3.

4.1.3 Acoustic/Ultrasound

This WPT category harvests acoustic waves, which are usually at ultrasound frequencies. In acoustic power transfer (APT), the transmitter node, while in contact with the skin, generates these waves using a piezoelectric transducer. These waves induce charge differences on a piezoelectric device in the receiver node, which is located inside the body along with the IMD.

The advantages and drawbacks of the three WPT techniques are summarized in Table 1 in terms of operating range, potential biological effects, amount of transferred

²Note that this classification is not universal.

Table 1 Comparison of WPT techniques.

Technique	Range	Biological effects	Transferred power	Receiver size
IPT	—	—	+	—
RFPT	+	—	—	+
APT	—*	+	+	+

+ / —: relatively good/poor performance, *: requires (non-air) medium

power and receiver area. The choice of WPT scheme and associated transferred-power amount has an impact on the real-time IMD *performance*, and also on the *size* of the energy reservoir and, subsequently, the IMD as a whole. This is further discussed in the subsequent sections.

4.2 Medical-Safety Constraints

The ZPD technique should satisfy the various requirements by the FDA, FCC, IEEE, etc., in order to prevent any adverse biological effects on human tissue due to excess electromagnetic-energy exposure. IEEE puts constraints on the intensity of RF signals and defines maximum-permissible-exposure (MPE) limits for magnetic and electric fields [21]. In addition to RF-signal intensity, the signal frequency has a significant impact on the amount of energy absorbed in the human tissue and the resulting potential to cause harm. This absorption is characterized by the *specific absorption rate* (SAR), which is expressed in $\frac{W}{kg}$ or $\frac{mW}{kg}$. The peak-spatial-average SAR values for exposure of the public and controlled environments are $2 \frac{W}{kg}$ and $10 \frac{W}{kg}$, respectively (over 10 g of tissue) [21]. The FDA also has guidelines regarding intensity of acoustic signals in $\frac{W}{cm^2}$, namely *spatial peak temporal average intensity* (I_{SPTA}) and *spatial peak pulse average intensity* (I_{SPPA}) [12]. Satisfying these constraints impacts the choice of WPT scheme (as discussed in Section 4.1).

4.3 Frequency-Band Constraints

Certain FCC constraints also need to be met in order to avoid IMD-radio interference with other devices operating in the same frequency band. For example, the MedRadio band, which is reserved for IMD communication, does not allow an equivalent isotropically radiated power (EIRP) of more than $25 \mu W$ [11]. Since this amount of power is too small for WPT (as will be discussed in Section 6.3), a separate band should be used for power transfer, whereas the MedRadio band can be used for data communication. This implies increased cost and size due to the use of

two antennas. One solution could be to use a single ISM-band (13.56 MHz) antenna for both WPT and data communication, however this would result in lower data rates due to smaller allowed bandwidth than that of MedRadio [33].

4.4 Real-time Behavior

Harvested power needs to stay above the consumed power in order for the energy consumers to work seamlessly. Otherwise, an energy reservoir must be employed so as to collect sufficient energy before the IMD can use it. Technically, due to this reservoir, the ZPD scheme should always work, but the charging delay limits usability and real-time behavior, which can be critical in the case of emergencies. The ZPD scheme should never slow down a paramedic access and jeopardize patient safety as a result.

4.5 Choice of Energy Reservoir

Either a supercapacitor (supercap) or a rechargeable battery can be employed as the energy reservoir. Supercaps in general have a longer lifespan and support more recharge cycles than batteries [30], and thus are more suitable for IMDs. Employing a supercap, can limit the range of applied charging voltage, since these components have low operating-voltage limits. Also, as indicated in [23], the capacitor size has to incorporate the losses due to the decoupling capacitors connected to the energy consumers.

4.6 Passive Wireless Communication

Passive communication relies on WPT schemes in order to function without the need of an on-board power supply. This concept forms the basis of ZPD strategies, which will be discussed in Section 5. The most critical component of these passive devices is the wireless transceiver that can lead to significant peak power consumption based on the design choice. Based on the choice of transmitter, which subsequently impacts the receiver implementation, we categorize these devices into four schemes, as depicted in Fig. 4. The different schemes at the leaf nodes of the tree are numbered accordingly and are subsequently explained. The first part of the scheme name indicates the type of wireless communication whereas the suffix indicates whether the communication shares the power-transfer-signal frequency band (PB) or uses an independent band (IB).

4.6.1 ActiveTX-IB

The passive device has an *active* transceiver, i.e., it actively transmits (using supply from the energy reservoir) instead of

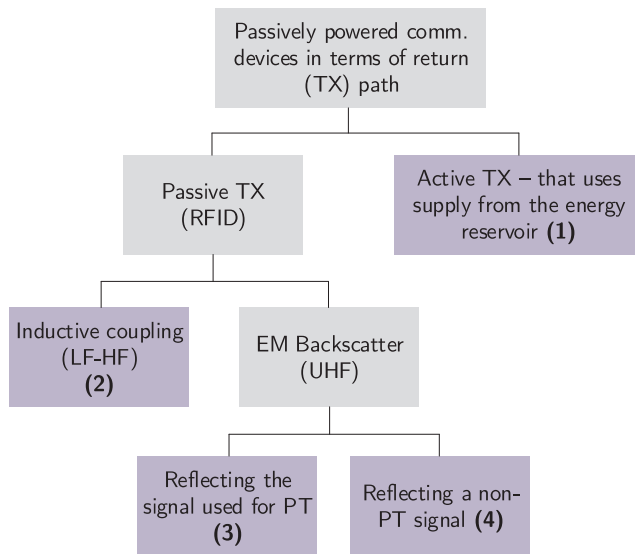


Figure 4 Classification of passive communication devices in terms of transmitter implementation.

reflecting the incident RF signal, as shown in Fig. 5a. This scheme is employed by the design in [46].

4.6.2 IC-PB

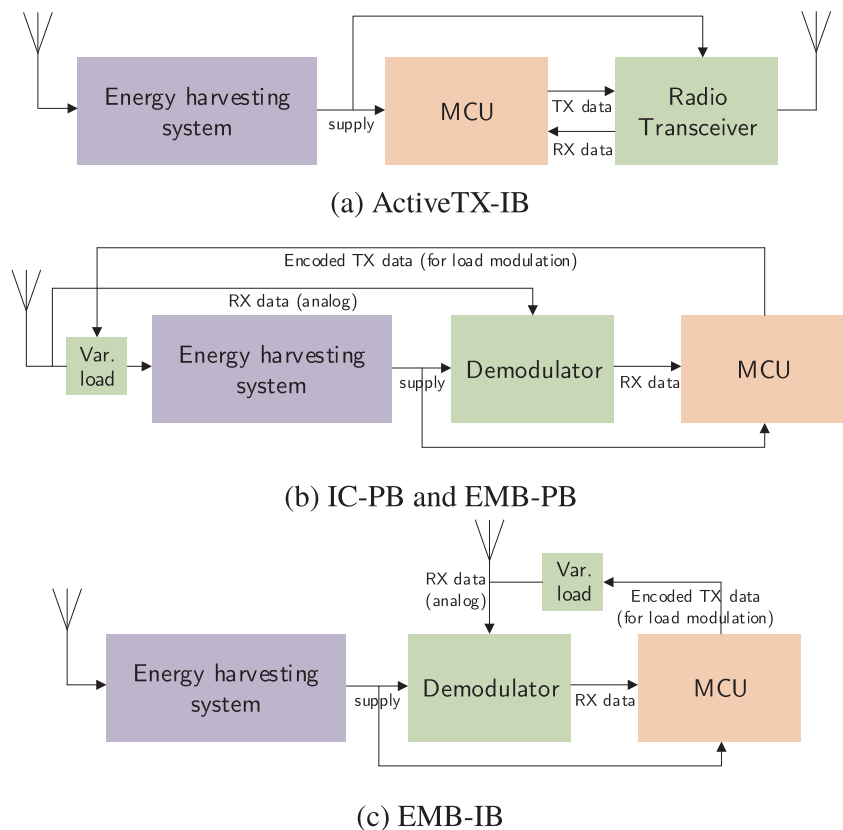
The downlink (reader to passive device) communication uses the same signal that is used for inductive power

transfer, which lies in the low- or high-frequency band (LF-HF). For the uplink, the electrical properties of the inductive coil are changed (by load modulation; in this case, *Load Shift Keying*), which affects the same inductive-coupling field, and is thus detected by the reader (see Fig. 5b). The design in [3] employs this scheme.

4.6.3 EMB-PB

Compared to the previous scheme, RF/Electromagnetic backscattering (EMB), which reflects the incident RF, is used for data transmission instead of inductive coupling. Here, the incident RF is used for both energy harvesting and data communication (see Fig. 5b). The RF is reflected if the load across the antenna feed-point is minimum, and vice versa. One of the works that employ this scheme is [45]. The use of EMB helps eliminate the high peak power consumption of a conventional RF transmitter. This is important for passive devices because, even to transmit just a few bits of data, the peak power may exceed the incoming power, which will result in device malfunction in the absence of a reservoir. Note that the use of EMB for transmission is fully beneficial only if a simple and low-power circuit is used for the receive path, such as an Amplitude-Shift-Keying (ASK) envelope detector.

Figure 5 Schematics of different passive communication schemes for ZPD.



4.6.4 EMB-IB

Compared to EMB-PB, here the difference is that the WPT signal is different from the one used for EMB (as shown in Fig. 5c). The design in [29] uses this scheme.

ActiveTX-IB and EMB-IB offer the most flexibility since they use separate antennas for WPT and data communication. As discussed in Section 4.3, these configurations are helpful in meeting the FCC constraints while maintaining both the sufficient power transfer and data rates. On the other hand, IC-PB and EMB-PB are more economical in terms of resources since they only employ one antenna [33]. This comes, however, at the cost of reduced flexibility in terms of data rate.

4.7 Fundamental Security Services

ZPD schemes primarily address *Availability* from the CIANA security services [47]: *Confidentiality*, *Integrity*, *Authentication*, *Non-repudiation* and *Availability*. Ensuring the first four services can have an indirect impact on *Availability*. As an example, if the IMD has a dedicated processor that is responsible for authenticating an external entity, the peak-power consumption of the implant will increase when this peripheral is active. As a result, the bogus messages sent by an attacker will draw more energy from the battery than in the case of a less-secure IMD. Hence, ensuring one service should not be at the expense of the other.

The choice of cryptographic primitives, which are needed to provide these services, plays a critical role in the design of the energy-harvesting circuit. For example, lightweight block ciphers are preferred candidates for achieving data confidentiality because of their low energy profile. Moreover, in order to achieve integrity and authentication, a cipher-based Message Authentication Code (MAC) should be used instead of a hash-based MAC (HMAC) because of lower energy consumption in software implementations. For dedicated hardware implementations, however, this is not always the case [40]. Furthermore, for these systems, *mutual* authentication should be employed instead of just authenticating the reader unilaterally. This is required to prevent spoofing attacks on the reader [50]. This implies that the harvested energy should be able to support *both* transmission and reception of data.

In addition to battery DoS, satisfying availability also implies providing protection against a second class of DoS attack on IMDs, which we call function DoS [50]. This type of DoS floods the IMD with communication requests in order to prevent it in performing its main medical functionality. It follows that a security architecture that ensures implant availability should protect against both battery and function DoS.

4.8 Device Usability

The ZPD design should not result in an awkward usage or programming of the IMD. For instance, a (short range) IPT-based access does not result in patient inconvenience in case of a pacemaker. However, such a close-range access may not be acceptable to the patient in case of a neurostimulator implanted within the skull. For instance, a patient may avoid frequent IMD access in public if it requires placing the reader interface on their head. This can significantly impact the patient's social life and can lead to social segregation.

4.9 Maintainability

The ZPD design involves executing cryptographic mechanisms in order to authenticate the external entities. In the event of discovering a security loophole or an implementation bug, the cryptographic primitives and/or the security protocol require replacement or an update. In the case of IMDs, the first requirement is that such updates should be possible at the firmware level using the wireless interface, otherwise hardware updates or modifications imply device explantation via surgery. Another requirement is that such firmwares should be decoupled from the main IMD functionality. This expedites the firmware-certification cycle. Updating a monolithic IMD firmware, which includes both the medical application and the security functionality, is highly likely to result in a longer certification cycle compared to a decoupled firmware.

4.10 Dependability

IMDs are safety-critical systems, which have extreme safety and reliability (cumulatively; *dependability*) constraints. A ZPD design introduces additional electronic components to the IMD system, and each component (e.g., a transistor) has an associated failure rate. Hence, ZPD protection should not significantly impact the overall implant dependability. Analysis of IMD dependability is further discussed in Section 6.6.

4.11 Emergency Access

In the case of emergencies, the paramedics or first responders should have unhindered and fast access to the IMD, without compromising patient safety and security. Hence, an appropriate balance should be attained between usability, safety and security. For instance, the authentication protocol running on harvested energy should not require a *pre-shared* secret (or key) between the reader and the IMD. Otherwise, it will not work in the case of the paramedic reader, which will most likely not have the same key as the implant [47]. Moreover, as discussed in Section 4.4, it is of

paramount importance that the choice of WPT and the associated energy reservoir results in acceptable charging delay in order to ensure real-time performance. Otherwise, it will block legitimate access to the IMD in emergency scenarios.

4.12 Design Suitability

Existing IMD designs take a long time from concept to market due to rigorous certification cycles. Therefore, any new ZPD solution should fit in seamlessly in the existing designs resulting in minimal changes and short review cycles. For example, technically speaking, a large energy reservoir enables ZPD but this increases the size of the design and introduces unnecessary delay, which impacts suitability.

4.13 Conformity to Touch-to-access Principle

Any ZPD scheme shall ensure that only the entity in close proximity to the patient for a prolonged period of time is allowed to access the IMD. This *touch-to-access* principle assumes that it is infeasible for the attacker to get in close proximity since the patient would reject physical contact with untrusted entities [43, 47].

4.14 Range of Operation

The ZPD solution shall be able to work correctly independently of the implantation depth. Appropriate balance should be attained between the WPT and the associated thermal effects and energy absorption in the human tissue. Also, the ZPD solution shall allow the provision of bedside-base-station operation for the convenience of the patient (see Fig. 1). This device by definition can be less than 10 feet away from the patient [34]. However, in order to conform to the touch-to-access principle, this communication should be strictly limited to the bedside range (less than 5 feet away).

5 A Survey of Existing ZPD Techniques

In light of the design considerations discussed in Section 4, we now survey works from literature and discuss their limitations. We hope that this survey will help us reflect on and validate the design considerations. These works are presented in chronological order, and to the best of our knowledge, are the only works pertaining to ZPD for IMDs.

5.1 Harvesting-Based Techniques

Halperin et al. [16] presented the pioneering work of RFID-style energy harvesting for zero-power defense of IMDs. They use an RFID module called WISP [45], which

employs EMB for the data transmission from the implant to the reader, and simple ASK-envelope detection in the reverse direction, while using RFPT for wireless power transfer. Their scheme, however, does not perform mutual authentication and its acoustic-communication-based key transport is susceptible to attacks, as shown in [15].

The scheme from Liu et al. [28] is the only ZPD work that takes FCC regulations into consideration. They employ the ISM band for RFPT and the MedRadio band for data communication. It employs a dedicated passive RFID wake-up module, which performs RF-energy harvesting from the incoming signal in order to authenticate the other entity. Upon successful authentication, the main module is woken up. This scheme uses pre-shared keys between the reader and the IMD, which makes emergency access impossible. This is because in emergencies, the IMD and the paramedic reader are likely unknown to each other and therefore do not share a key.

Strydis et al. [50] propose an IMD architecture that isolates the implant functionality from the security tasks by using dedicated processing cores for the respective applications. They designed the security co-processor from scratch, which was optimized for executing the MISTY1 cipher in terms of energy and performance. The choice of this dual-core architecture helps in dealing with repeated communication requests that may prevent the implant from performing its primary task. Thus it effectively protects against function DoS. Battery DoS is tackled by ensuring that the security core and the transceiver run on harvested RF energy before mutual authentication of reader/IMD. After successful authentication, these modules are allowed to use battery power for subsequent communication. However, they did not present a full system implementation.

Ellouze et al. [8, 9] propose an RFID-based, energy-harvesting solution, that uses the same WISP module as employed by [16]. In contrast to [16], their solution additionally provides mutual authentication. They use cardiac-signal-based biometrics for authentication and the generation of session keys. However, the fuzzy-vault-inspired protocol (OPFKA) [19] employed in their scheme is vulnerable to attacks as demonstrated in [42].

Yang et al. [53] use IPT, and employ the same coil for power transfer and data communication. Their scheme provides mutual authentication. However, it employs pre-shared keys, and is thus unable to support emergency access. Moreover, they did not implement a unified ZPD system since the hash-based authentication was verified separately on an FPGA.

Chang et al. [3] propose a generic ZPD solution that is not specific to IMDs per se, however, it covers a spectrum of devices that have more or less the same profile. They propose IPT for the power transfer from the reader. This signal is also used for bi-directional communication.

However, they do not give any description of the employed security protocol.

5.2 Non-harvesting-Based Techniques

Denning et al. [6] propose a class of defensive mechanisms, which uses an external device, called the communication *cloaker*. This device shares a secret key with the IMD, which allows secure communication between the pair. The defensive mechanisms vary in terms of whether the IMD checks the presence of a cloaker *periodically* or if it contacts the cloaker only when an external entity tries to access the implant. In case the cloaker is absent, the IMD allows fail-open access to any reader. Otherwise, the cloaker performs the authentication of the external entity, and allows it to communicate with the IMD in case it is authentic. Although the proposed class provides emergency access, the authors acknowledge that it is susceptible to jamming attacks, in which the attacker selectively jams packets between the cloaker-IMD pair in order to convince the IMD of the cloaker's absence. Additional mitigation schemes against these attacks are briefly discussed. Another drawback of this scheme is that it introduces an additional single point of failure. This is because the IMD becomes unsecured in case the patient forgets to wear the cloaker, or loses it.

Hei et al. [17] utilize the concept of *anomaly detection* [44] in which the system automatically detects abnormal events, such as malicious access. Their scheme is based on supervised learning in which the normal access patterns of IMDs are used as training data. The result is then used to classify abnormal IMD accesses in real time. Their scheme uses an additional device (a cellphone) that performs this real-time classification. Moreover, their scheme is designed to block anomalous access attempts *before* the expensive authentication-related computations are performed by the IMD. When the IMD is contacted by an external device, it asks the cellphone to classify this connection attempt. Based on the verdict from the cellphone, the IMD either proceeds with the authentication, or goes to sleep. One main drawback of their scheme is that they have neither provided a security protocol between the IMD and the cellphone, nor any security analysis. One highly probable attack against this scheme is for an attacker to spoof cellphone messages to the IMD. Moreover, this scheme is not designed to work in an emergency scenario.

Similarly to [6], Gollakota et al. [14] propose an external wearable device, called the *shield*, which listens and jams all IMD accesses. With this *friendly* jamming, the scheme tries to protect against both active and passive (eavesdropping) attacks. In case a legitimate reader access is required, the shield is simply removed from the patient's proximity. The main advantage of this solution is that it can be readily employed in existing IMD systems. However, similar to [6],

this scheme introduces an additional single point of failure. Moreover, they assume that the distance between the IMD and the shield is less than the distance between the attacker and the IMD, and hence the attacker would be unable to perform eavesdrop attack. However, it is shown in [52] that MIMO-based eavesdropping attacks are possible if the attacker uses two antennas within 3 meters of the patient [44].

5.3 Summary

Table 2 compares the above ZPD techniques based on the various parameters and design considerations highlighted in Section 4. We can see that all harvesting-based works lack the evaluation of hazardous biological effects of the employed WPT schemes. Moreover, all the techniques do not consider the possibility of a bedside-base-station operation, which is a rising trend in the reader/IMD systems. They also offer insufficient security services and/or have security vulnerabilities in one form or another.

6 Discussion and Recommendations

We, next, provide recommendations on how existing solutions can be improved in order to better meet the design constraints highlighted in Section 4.

6.1 Adaptive ZPD

In modern IMD setups, in addition to the doctor's programmer, we also have a bedside base-station, as shown in Fig. 1. For the convenience of the patients, these wireless devices are required to communicate with the IMD from a few feet away [34]. With this constraint, IPT- and APT-based ZPD cannot be used for the base-station/IMD authentication. Hence, with this setup, it is advantageous to employ RFPT for energy harvesting, since it is more flexible compared to IPT and APT in terms of range. Though the amount of power transferred through RFPT is significantly smaller compared to IPT/APT, it is not an issue in this specific case since the base-station communication is only used for non-critical daily monitoring. As a result, this setup can afford long delays due to energy-reservoir charging. In light of the above, an *adaptive ZPD* approach should be considered, that e.g., uses IPT/APT for doctor-programmer/IMD communication, and switches to RFPT for base-station/IMD communication. In terms of implementation cost, it is more economical to use IPT for programmer/IMD communication instead of APT. This is because the same coils can potentially be employed for near-field (programmer communication) and far-field (base-station communication). On the other hand, the use

Table 2 Summary of ZPD strategies.

Design considerations	Harvesting-based techniques					Non-Harvesting-based techniques			
	Halperin et al. [16]	Liu et al. [28]	Strydis et al. [50]	Ellouze et al. [8, 9]	Yang et al. [53]	Chang et al. [3]	Denning et al. [6]	Hei et al. [17]	Gollakota et al. [14]
-	-	-	-	-	-	-	N/A	N/A	N/A
Satisfy freq. band req.	-	Yes	-	Yes	Yes	-	Yes	Yes	Yes
Real-time performance	Yes	-	-	-	-	Yes	-	-	Yes
Energy reservoir	Not used	Not used	-	Not used	Not used	-	N/A	N/A	N/A
Type of WPT technique	RFPT	RFPT (ISM)	-	RFPT	IPT	IPT	N/A	N/A	N/A
Passive wireless comm.:							N/A	N/A	N/A
<i>Scheme</i>	EMB-PB	-	-	EMB-PB	IC-PB	IC-PB			
<i>ZPD Receive path</i>	ASK	-	-	ASK	IC (ASK)	IC (FM)			
<i>ZPD Transmit path</i>	EMB	No	-	EMB	IC (ASK)	IC (ASK)			
Security services related:									
<i>Employed primitives</i>	DE	-	DE, CMAC	DE, HMAC	Hash function	DE	-	-	None
<i>Mutual authentication</i>	No	No	Yes	Yes	Yes	-	No	No	No
<i>Avoids pre-shared keys</i>	Yes	No	No	Yes	No	-	Yes	-	Yes
<i>Function-DoS protection</i>	Yes	Yes	Yes	Yes	Yes	-	-	-	Yes
<i>vulnerabilities</i>	[15]	-	-	[42]	-	-	SJ	-	[52]
Device usability	-	-	-	-	-	-	-	-	Yes
Dependability	-	-	-	-	-	-	SPF	SPF	SPF
Maintainability	Yes	-	Yes	Yes	No	-	-	-	Yes
Emergency access	Yes	No	No	Yes	No	-	Yes	No	Yes
Touch-to-access	Yes	-	No	Yes	-	Yes	Yes	No	Yes
Operating distance:									
<i>Max. implantation depth</i>	1 cm (animal tissue)	-	-	-	-	2.5 cm (air)	N/A	N/A	N/A
<i>Bedside-base-station</i>	No	No	No	No	No	No	No	-	No
Design suitability (size, additional hardware etc.)	WISP and piezoelectric transd.	RFID module	Co-processor for security	WISP	-	-	ED	ED	ED

‘-’: Lacking information, DE: Data Encryption, Not used: Advantageous avoidance of an additional component, Yes/No: Satisfies requirement (or not), N/A: Not applicable, ED: The scheme employs an external mobile/wearable device, SJ: Selective-jamming attack, SPF: ZPD design adds an additional single point of failure

of APT (for programmer communication) would require the use of piezoelectric transducers in addition to the RF antenna (needed for base-station communication).

6.2 Main-Implant-Battery Size

We now discuss how realistic it is to achieve battery DoS when considering actual IMD battery sizes. The generic components of the total IMD energy consumption are summarized in (1) [7].

$$E_{total} = E_{comp} + E_{sense} + E_{stim} + E_{TRX} \quad (1)$$

E_{comp} is the computational energy which includes the energy spent by the IMD processor or MCU for medical-related processing, and the energy spent for handling the incoming or outgoing communication messages. E_{sense} is the energy consumed during the sensing of a physiological signal from the human body. E_{stim} is the energy spent for electrical stimulation via the electrodes applied by the IMD on the human tissue. Finally, E_{TRX} is the energy consumed by the RF transceiver.

For the calculations, it is assumed that the IMD has a state-of-the-art ultra-low-power ARM Cortex-M0+ based 32-bit MCU [24], running at 19 MHz, and an implantable-grade radio transceiver [38], with an effective data rate of 265 kbps. The supply voltage is set at 3.3 V. The IMD-battery-lifetime trends with respect to example processor duty cycles, which contribute to E_{comp} and E_{sense} , are shown in Fig. 6. For instance, the pacemaker design in [27] has a processor duty cycle of 5%. Moreover, the worst-case E_{stim} of a pacemaker is 25 μ J per heartbeat, based on reported figures of commercial devices [7]. The duty cycle of the transceiver is estimated at 0.21%, which corresponds to 3 minutes of active data communication per 24 hours with a bedside base-station [34]. The data points correspond to actual implantable-grade battery sizes [51].

The time required to completely deplete the IMD battery by continuously sending bogus communication packets is illustrated in Fig. 7. On average, we assume half the charge available in the batteries due to normal use. As a worst-case

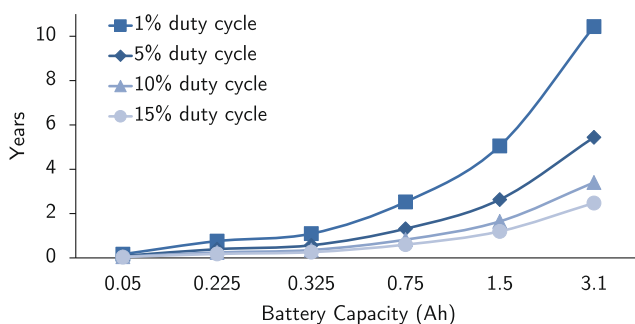


Figure 6 IMD-battery lifetime with respect to example processor duty cycles while the transceiver is active for 3 minutes per 24 hours.

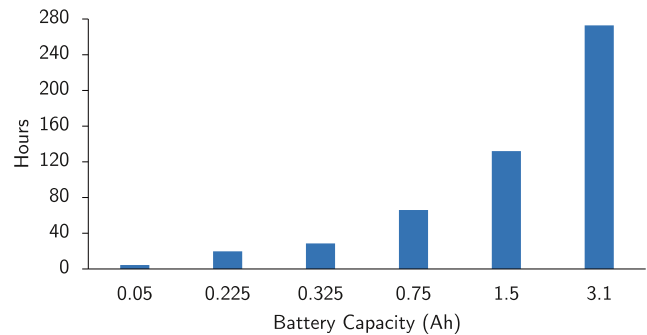


Figure 7 Time required to completely deplete a half-full IMD battery through battery DoS.

scenario, we also assume that the authentication steps are executed *continuously* on *active* modes of the MCU and the transceiver with the current consumption of 0.78 mA and 4.9 mA, respectively. It can be deduced from these plots that, as a first level of defense, the battery sizes for critical applications, such as pacemakers, should be as large as possible.

We now analyze the effect of the EM-noise attack, in which the attacker's aim is to cause IMD retransmissions due to high error rates at the IMD transceiver. Based on the analysis from Gelenbe et al. [13] of battery-DoS attacks on sensor nodes, the IMD current consumption under an EM-noise attack can be represented by (2).

$$I_a = I_n + rI_a = \frac{I_n}{1-r} \quad (2)$$

Here, I_n is the average current consumption in a normal scenario, I_a is the total average current consumption in an attack scenario, and r is the retransmission probability ($0 \leq r < 1$). Increase in the EM-noise level is reflected by an increase in r . Figure 8 shows the expected lifetime of an IMD operating under realistic processor and transceiver duty cycles of 5% and 0.21% respectively (as discussed above). From this, we can conclude that, although the EM-noise attack significantly affects the IMD lifetime, its impact is less critical compared to continuously making

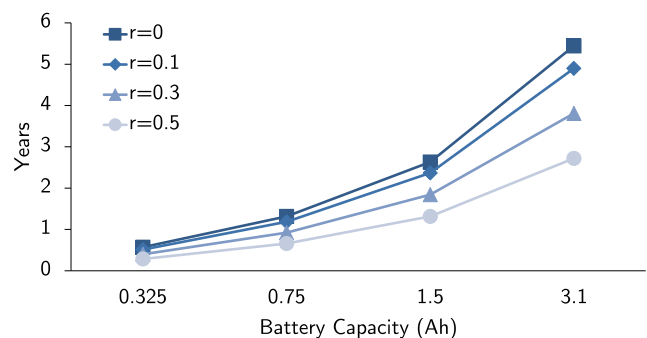


Figure 8 IMD-battery lifetime in the presence of an EM-noise attack resulting in the retransmission probability r .

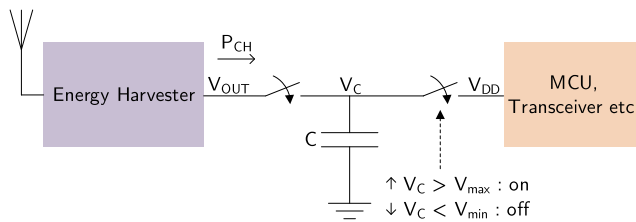


Figure 9 Simple ZPD configuration.

bogus authentication attempts. This is because the amount of RF traffic generated by the IMDs in realistic scenarios is very low, e.g., 3 minutes per day for the above-mentioned reader [34].

6.3 Reservoir Size and Charging Delay

If the peak power of the load is always less than the harvested power, then we do not need a reservoir. Otherwise, the size of the reservoir is determined by looking at the required energy consumption of all the consumers during the authentication operation. Moreover, if a reservoir is required, then it may seem that any ZPD scheme might work. However, this is not true since it can become impractical for high-energy-consumption solutions due to the long delay, which is required to store sufficient energy.

For capacitor reservoirs, in order to determine the required capacitance, the energy available in the capacitor (E_{cap}), should be greater than the authentication energy (E_{auth}). The capacitance can be calculated using (3) [4], where V_{max} is the capacitor voltage when it is sufficiently charged and V_{min} is when it has been used by the application or authentication process (see Fig. 9).

$$E_{cap} = \frac{1}{2} C (V_{max}^2 - V_{min}^2) > E_{auth} \quad (3)$$

RF-energy harvesters in general output *constant power* instead of constant voltage [39]. In this type of capacitor charging, the supplied voltage increases (instead of staying fixed) and current decreases with increasing capacitor voltage. The capacitor charging time³ (t_{ch}) for this type of charging is calculated using (4) [39]. Here, P_{ch} is the charging power supplied by the energy harvester to the capacitor (C), R is the capacitor's equivalent series resistance (ESR) and Q is the amount of coulombs stored during this time. Here $A = \sqrt{Q^2 + 4C^2RP_{ch}}$.

$$t_{ch} = \frac{Q^2 + QA + 4C^2RP_{ch} \ln\left(\frac{A+Q}{\sqrt{4C^2RP_{ch}}}\right)}{4CP_{ch}} \quad (4)$$

If the authentication-energy consumption is reduced, then the required reservoir capacitance can be reduced as

³The capacitor charging time for constant voltage charging is $5RC$.

a result. If this value is between $0.1 \mu\text{F}$ and $470 \mu\text{F}$, then ceramic capacitors can be employed, which are ideal for energy harvesting because of their low leakage current, small size and low cost [4]. These capacitors also have a very low ESR [10], which allows us to ignore the effect of the time constant (RC). Hence, (4) can be simplified to (5), which is also equivalent to (6). Here, E is the energy stored in the capacitor.

$$t_{ch} = \frac{Q^2}{2CP_{ch}} \quad (5)$$

$$t_{ch} = \frac{E}{P_{ch}} \quad (6)$$

The time it takes to charge an empty capacitor ($t_{ch_{initial}}$), and in the case of subsequent charging operations ($t_{ch_{repeat}}$) when a capacitor has a residue voltage of V_{min} can be calculated by (7) [4]. Here, $E_{initial} = \frac{1}{2}CV_{max}^2$, which is the energy attained by an empty capacitor when charged from 0 V to V_{max} .

$$\begin{aligned} t_{ch_{initial}} &= \frac{E_{initial}}{P_{ch}} \\ t_{ch_{repeat}} &= \frac{E_{cap}}{P_{ch}} \end{aligned} \quad (7)$$

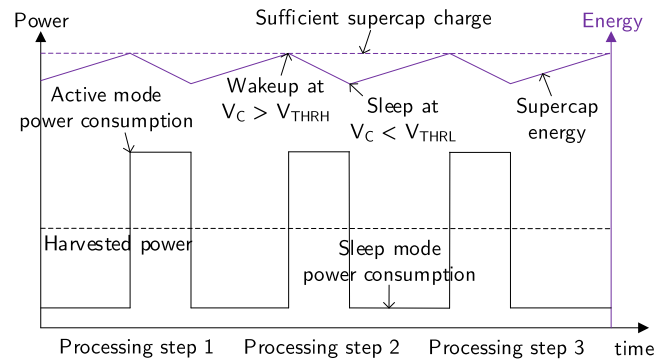
As an example, we use the evaluation setup from Section 6.2 and take the ISO/IEC 9798-2-based mutual authentication protocol from the ZPD solution in [50]. We use AES-128 for data confidentiality and cipher-based MAC. For WPT, we look at the IPT scheme from [26], which is specifically designed for IMDs and delivers $P_{ch} = 6.15 \text{ mW}$. Using $V_{max} = 3.3 \text{ V}$ and $V_{min} = 2.1 \text{ V}$, which are within the operating supply voltage range of this setup (i.e., 2.05 V to 3.5 V), we see that C for the resulting scheme turns out to be $6.19 \mu\text{F}$ (since the measured $E_{auth} = 20.07 \mu\text{J}$). Using a standard ceramic capacitor of size greater than this value e.g., $10 \mu\text{F}$, $t_{ch_{initial}}$ and $t_{ch_{repeat}}$ turn out to be 8.85 ms and 5.27 ms respectively, which are very reasonable in terms of real-time behavior.

In general, the simplest solution is always to choose a reservoir capacitance that is much larger than the required value (as long as the charging delay is reasonable). This margin is important since the authentication protocol or the employed cryptographic primitives can change in the future, e.g., due to security updates. However, in case C turns out to be outside the ceramic-capacitor range due to large E_{auth} , we can employ the following schemes to reduce it, and thereby the charging delay.

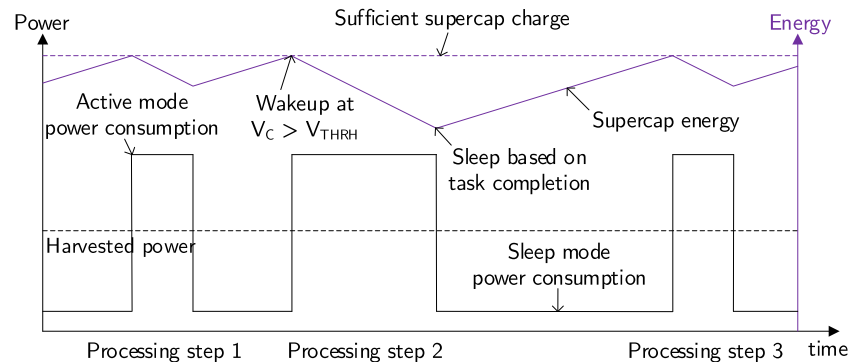
6.3.1 Use of Sleep Modes

The capacitor-charging delay can be minimized by using sleep modes and interrupts, instead of sizing the capacitor

Figure 10 Supercapacitor characteristics in relation to application duty cycle (active mode vs. sleep mode).



(a) Entering sleep based on voltage-comparator interrupt



(b) Entering sleep after protocol-step completion

for the whole authentication, resulting in reduced required capacitance. One way of achieving this could be to achieve a minimum required voltage (V_{THR_H}) using a voltage-controlled switch, before the capacitor energy is used by the rest of the IMD (Fig. 10a). After some processing, the implant MCU can then enter sleep mode based on a voltage-comparator-based interrupt when the capacitor voltage (V_C) falls below a lower threshold (V_{THR_L}). Subsequently, the MCU can wake up⁴ again if another such interrupt is set at $V_C > V_{THR_H}$ [23]. In this case, a *protocol step*, such as a MAC calculation, can have multiple *processing steps*.

Another way could be to go to sleep *after* each protocol step in order to reduce the number of wakeups and the associated delay at the cost of a larger capacitor. Here, the protocol step is the same as the processing step (Fig. 10b). In this case, the supercap size should be chosen based on the most energy-consuming protocol step. However, this can be problematic if such a step is changed in the future due to the reprogramming of the IMD with a different authentication protocol. Note that in this scheme as well the comparator interrupt will be required to wake up the device, indicating that the capacitor has been sufficiently charged.

6.3.2 Gradual Switch to Harvested Energy

In another approach, the implant can use the battery for the first authentication request and if it fails, it can switch to harvested energy for subsequent accesses within a specified time-frame. This can allow for smaller reservoir sizes since we can afford the resulting delay due to frequent charge/discharge cycles in case of an illegal entity.

6.4 Timeouts

It can be argued that timeouts can be employed as a simpler alternative to ZPD. For instance, after a certain number of incorrect attempts, the IMD can be made to not accept further messages for a certain duration. For domains other than IMDs this can be a natural choice. However, for IMDs, these timeouts can significantly compromise patient safety. For instance, any timeout after a malicious access can subsequently block a valid authentication attempt, which impacts *availability*.

6.5 Standalone ZPD Module

As discussed in Section 4.12, the ZPD circuitry should not impact the already-constrained design choices from the

⁴The plots in Fig. 10 do not show the wakeup-time durations for clarity.

manufacturer's perspective. When incorporating ZPD, it is likely that the manufacturer's preferable course of action would be to retain most of the existing IMD design in order to expedite regulatory approval. A solution to this problem is to design a ZPD module that sits externally to the main IMD core next to the antenna and is minimally invasive from the IMD design perspective. This is shown in Fig. 11.

This module decouples the antenna from the rest of the IMD with the help of a switch. The antenna is initially disconnected from the IMD transceiver. Upon receiving the incoming RF, the ZPD module is powered up using the harvested energy and executes the authentication protocol. When the external entity/reader is authenticated, the ZPD module turns on the switch so that the IMD is able to communicate with the reader in a secure manner. Upon completion of the communication session, the ZPD module turns off the switch. This configuration, however, poses two new constraints: (1) There should be enough space inside the casing for the placement of this standalone module. (2) The antenna (or coil) used by the ZPD module should not be obstructed by the metallic casing. Otherwise, it can negatively impact energy harvesting and wireless communication.

Regarding the first constraint, we observe that it is quite common for the IMDs (e.g., [35]) to have sufficient vacant space inside the metal casing. Regarding the second constraint as well, we have examples of rechargeable IMDs such as [41], which have unusually large charging coils compared to non-rechargeable IMDs. Here, the coil is embedded within an elastomeric plate, which is placed outside the IMD's titanium casing. This allows unobstructed WPT. Hence, it is reasonable to assume that the IMDs currently in the field can accommodate a standalone ZPD module.

As discussed in Section 3, the IMD transceiver usually polls for an external entity by cycling through sleep and sniff modes. Employing the above-discussed standalone ZPD module alleviates the need for such polling, and thus, the transceiver can completely stay asleep. However, this implies modifying the transceiver functionality, which was

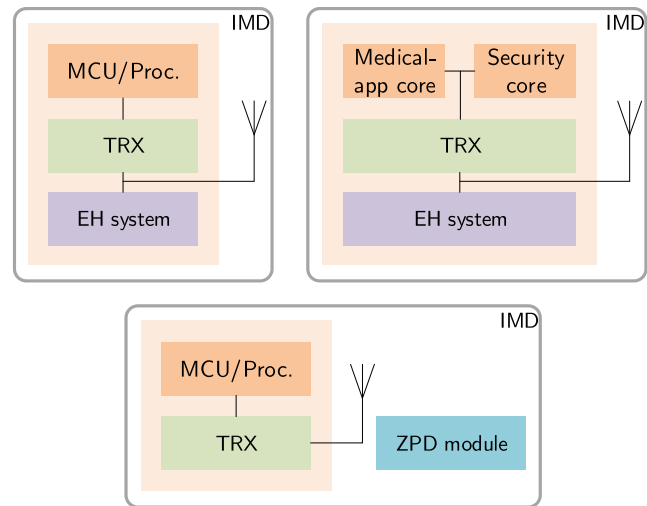


Figure 12 Taxonomy of ZPD implementations. Top left: single-processor implementation. Top right: dual-processor implementation. Bottom: standalone ZPD module with the internal IMD design unchanged.

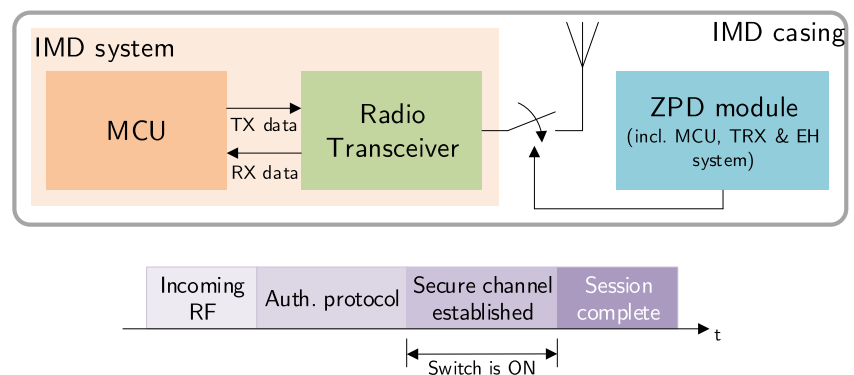
intended to be avoided in the first place. Thankfully, such changes can be performed at the firmware level, which are far less invasive than changing the transceiver circuitry.

6.6 Taxonomy of ZPD Implementations

In terms of implementing ZPD, we can have three possible schemes, as shown in Fig. 12.

1. **Single-processor ZPD (1P-ZPD):** This is the most basic implementation in which a dedicated energy-harvesting system is added to a reference single-processor IMD; see Fig. 3. This processor is responsible for both executing the medical application and for receiving/sending data packets from/to the transceiver. This handling of data includes running the crypto primitives in order to authenticate the external device (using harvested energy).
2. **Dual-processor ZPD (2P-ZPD):** This scheme was originally proposed in [50], in which a dedicated

Figure 11 Standalone ZPD module.



processor is added (within the IMD system) for handling the communication data and executing the security primitives. This helps protect the IMD against function-DoS.

3. Standalone ZPD (S-ZPD): This type of ZPD implementation is the scheme introduced in Section 6.5. Note that similar to 2P-ZPD, this scheme has a second processor as well, which is inside the standalone module.

These implementations are compared in Table 3 against a reference, non-ZPD design. Only 2P-ZPD and S-ZPD provide protection against *function-DoS* since the medical and security tasks are decoupled and executed on separate processors. In addition, S-ZPD provides the fastest time to market because of a significantly shorter approval cycle of the standalone module. On the other hand, as evident from Fig. 12, 1P-ZPD results in the lowest area overheads compared to the other two schemes. Note, however, that 2P-ZPD and S-ZPD do not introduce significant energy and power costs since the authentication is performed by the additional processors using only harvested energy and, after authentication, these processors can enter their deepest sleep modes, as shown in [48].

In terms of *maintainability*, both 2P-ZPD and S-ZPD decouple the security-related processing from the main implant functionality. This makes it straightforward to update the security firmware, without the need for touching the medical application. Hence, the potential maintainability cost of 1P-ZPD is considerably higher than the other two schemes.

In order to evaluate the schemes in terms of *dependability*, we consider *functional safety*, which is based on the industry-established meta-standard IEC 61508 [20] and has been increasingly used for a diverse number of application domains, ranging from cars, and planes to IMDs.

Functional safety can be calculated via such techniques as Failure Mode and Effect Analysis (FMEA). More

Table 3 Comparison of ZPD-enabled IMD designs with respect to a base, single-processor, non-ZPD system.

	1P-ZPD	2P-ZPD	S-ZPD
Function-DoS protection	0	+	+
Design suitability			
<i>Certification effort</i>	--	--	--
<i>Area cost</i>	--	--	--
<i>Power/Energy cost</i>	--	--	--
Maintainability	--	+	+
Dependability	0	0	0

(+) stands for a benefit, (–) for a drawback and (0) for no perceptible change compared to the base design

Table 4 High-demand probability of failure per hour (PFH) for an 18-nm technology node.

PFH	FITs
$< 10^{-5}/h$	10000
$< 10^{-6}/h$	1000
$< 10^{-7}/h$	100
$< 10^{-8}/h$	10

specifically and without loss of generality, we consider here an IMD processor comprising three critical subparts: the core, the instruction memory (FLASH) and the data memory (SRAM). We, then, proceed to perform an FMEA on the *safety functions* included in the IMD safety-critical systems; in this case the aforementioned three subparts. The objective is to calculate the Probability of Failure per Hour (PFH), an absolute metric for the overall system. For constant failure rates, PFH is given by (8):

$$PFH = \sum \lambda_{DU} \quad (8)$$

Here, λ_{DU} is the rate of dangerous undetected failures observed. PFH encompasses a λ_{DU} per each of the sub-components (i.e. here, IMD subparts) of the analyzed safety function and accounts for both permanent and transient faults. Here, we draw the λ_{DU} values of all such components from confidential industrial data [31] in the possession of YogiTech S.p.A., now an Intel company. This dataset is empirically collected and pertains to an 18-nm process technology and, hence, is relevant for future IMDs, as well. Considering a *high-demand* application scenario – since we focus on IMDs –, we can use calculated PFH figures to also derive the well-known FIT metric (Failures In Time) based on well-known values (see Table 4).

Based on the above, the dependability findings for the three implementations are collected in Table 5. Since the S-ZPD module is standalone, it must contain its own processor (or MCU). Then, the amount of processing logic and memory footprint of this scheme is similar to that of 2P-ZPD, which is roughly double to that of 1P-ZPD. Hence, 1P-ZPD should have a lower PFH compared to the other two schemes (assuming same processor architecture and memories are used in all the schemes). We take as an example a 16-bit 5-stage RISC processor with a separate 16-kB instruction (FLASH) memory and a 16-kB data memory

Table 5 Dependability evaluation of ZPD-enabled IMD designs.

	PFH	FIT
1P-ZPD	4.86×10^{-8}	100
2P-ZPD & S-ZPD	9.70×10^{-8}	100

(SRAM). Incorporating an additional processor (i.e., in schemes 2P-ZPD and S-ZPD) doubles the PFH value to that of 1P-ZPD. However, there is no change in FIT value, due to the trivial silicon overhead involved in moving from a single to two tiny implant processors due to the lightweight processor designs used [50]. Hence, 2P-ZPD and S-ZPD do not impact the IMD dependability perceptibly.

7 Conclusions

Over the last few years, energy harvesting has been presented as the most effective solution for protecting IMDs against battery-depletion attacks. In this paper, we have provided an extensive review of IMD-specific ZPD works from literature. We analyzed these works based on our formulated design considerations, and highlighted their shortcomings. This paper is the first to substantiate these considerations and to provide practical recommendations towards practical ZPD implementations. These include, among others, the concept of adaptive ZPD with the purpose of facilitating bedside-base-station operation, and the standalone ZPD module with the aim of improving the IMD-certification effort and the time to market.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

- Abbott (2016). Prodigy MRI™ IPG - Clinician's Manual.
- Basaeri, H., Christensen, D.B., Roundy, S. (2016). A review of acoustic power transfer for bio-medical implants. *Smart Materials and Structures*, 25(12), 123001.
- Chang, S.Y., Kumar, S.L.S., Tran, B.A.N., Viswanathan, S., Park, Y., Hu, Y.C. (2017). Power-positive networking using wireless charging: protecting energy against battery exhaustion attacks. In *Proceedings of the 10th ACM conference on security and privacy in wireless and mobile networks* (pp. 52–57). ACM.
- Corporation, C.S. (2017). AN 210772 - energy calculation for energy harvesting with S6AE101A, S6AE102A and S6AE103A.
- Costanzo, A., Dionigi, M., Masotti, D., Mongiardo, M., Monti, G., Tarricone, L., Sorrentino, R. (2014). Electromagnetic energy harvesting and wireless power transmission: a unified approach. *Proceedings of the IEEE*, 102(11), 1692–1711.
- Denning, T., Fu, K., Kohno, T. (2008). Absence makes the heart grow fonder: new directions for implantable medical device security. In *HotSec*.
- Deterre, M. (2013). Toward an energy harvester for leadless pacemakers. Theses, Université Paris Sud - Paris XI. <https://tel.archives-ouvertes.fr/tel-00868838>.
- Ellouze, N., Allouche, M., Ben Ahmed, H., Rekhis, S., Boudriga, N. (2013). Securing implantable cardiac medical devices: use of radio frequency energy harvesting. In *Proceedings of the 3rd international workshop on trustworthy embedded devices* (pp. 35–42). ACM.
- Ellouze, N., Rekhis, S., Boudriga, N., Allouche, M. (2018). Powerless security for cardiac implantable medical devices: Use of wireless identification and sensing platform. *Journal of Network and Computer Applications*, 107, 1–21.
- Evanczuk, S. (2014). Capacitor characteristics impact energy harvesting efficiency digikey.
- FCC (2018). Medical device radio communications service. Title 47 Chapter I, Subchapter D, Part 95, Subpart I.
- FDA (2008). Guidance for Industry and FDA Staff - Information for Manufacturers Seeking Marketing Clearance of Diagnostic Ultrasound Systems and Transducers. Guidance Document.
- Gelenbe, E., & Kadioglu, Y.M. (2018). Battery attacks on sensors. In *International symposium on computer and information sciences, security workshop*. Berlin: Springer International Publishing.
- Gollakota, S., Hassanieh, H., Ransford, B., Katabi, D., Fu, K. (2011). They can hear your heartbeats: non-invasive security for implantable medical devices. In *Proceedings of the ACM SIGCOMM 2011 conference* (pp. 2–13).
- Halevi, T., & Saxena, N. (2010). On pairing constrained wireless devices based on secrecy of auxiliary channels: the case of acoustic eavesdropping. In *Proceedings of the 17th ACM conference on computer and communications security* (pp. 97–108). ACM.
- Halperin, D., Heydt-Benjamin, T.S., Ransford, B., Clark, S.S., Defend, B., Morgan, W., Fu, K., Kohno, T., Maisel, W.H. (2008). Pacemakers and implantable cardiac defibrillators: software radio attacks and zero-power defenses. In *IEEE symposium on security and privacy*, 2008. SP 2008 (pp. 129–142). IEEE.
- Hei, X., Du, X., Wu, J., Hu, F. (2010). Defending resource depletion attacks on implantable medical devices. In *2010 IEEE global telecommunications conference GLOBECOM 2010* (pp. 1–5). IEEE.
- Ho, J.S., Yeh, A.J., Neofytou, E., Kim, S., Tanabe, Y., Patlolla, B., Beygui, R.E., Poon, A.S. (2014). Wireless power transfer to deep-tissue microimplants. *Proceedings of the National Academy of Sciences*, 111(22), 7974–7979.
- Hu, C., Cheng, X., Zhang, F., Wu, D., Liao, X., Chen, D. (2013). Opfka: secure and efficient ordered-physiological-feature-based key agreement for wireless body area networks. In *2013 Proceedings IEEE INFOCOM* (pp. 2274–2282). IEEE.
- IEC (2008). Functional safety of electrical/electronic/programmable electronic safety-related systems. IEC 61508.
- IEEE (2006). IEEE standard for safety levels with respect to human exposure to radio frequency electromagnetic fields, 3 kHz to 300 GHz. IEEE Std C95.1-2005 (Revision of IEEE Std C95.1-1991) pp. 1–238, <https://doi.org/10.1109/IEEESTD.2006.99501>.
- Kadirvel, K., Carpenter, J., Lum-Shue-Chan, B. (2012). Power-management functions for energy harvesting. EE Times.
- Laboratories, S. (2013). Using EFM32 in Energy Harvesting Applications AN0061 - Application Note.
- Laboratories, S. (2018). EFM32™ Tiny Gecko 11 32-bit Microcontroller.
- Lafrance, A. (2014). Who killed the rechargeable pacemaker? The Atlantic.

26. Li, P., & Bashirullah, R. (2007). A wireless power interface for rechargeable battery operated medical implants. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 54(10), 912–916.
27. Lindqvist, P. et al. (2005). Compression and storage of medical data in pacemakers. Master's Thesis, Royal Institute of Technology, Stockholm, Sweden.
28. Liu, J.W., Al Ameen, M., Kwak, K.S. (2010). Secure wake-up scheme for WBANs. *IEICE Transactions on Communications*, 93(4), 854–857.
29. Mansano, A.L., Li, Y., Bagga, S., Serdijn, W.A. (2016). An autonomous wireless sensor node with asynchronous ECG monitoring in 0.18 μm CMOS. *IEEE Transactions on Biomedical Circuits and Systems*, 10(3), 602–611.
30. Guerra, M. (2016). Can supercapacitors surpass batteries for energy storage? Electronic Design.
31. Mariani, R. (2011). Deliverable D2.1: application analysis guide. DeSyRe: on-demand system reliability. <http://www.desyre.eu/?q=%3Cdeliverables%3E>.
32. Marin, E., Singelée, D., Garcia, F.D., Chothia, T., Willems, R., Preneel, B. (2016). On the (in) security of the latest generation implantable cardiac defibrillators and how to secure them. In *Proceedings of the 32nd annual conference on computer security applications* (pp. 226–236). ACM.
33. Martins, G.C., Urso, A., Mansano, A., Liu, Y., Serdijn, W.A. (2017). Energy-efficient low-power circuits for wireless energy and data transfer in iot sensor nodes. arXiv:1704.08910.
34. Medical, S.J. (2015). FAQs - Merlin.net™ Patient Care Network (PCN) 8.0 Q&A.
35. Medtronic (2008). Activa PC - Implant manual.
36. Medtronic (2017). Intellis™ Rechargeable neurostimulators - Implant Manual.
37. Mehta, N. (2018). When to consider getting a rechargeable SCS. Veritas Health.
38. Microsemi (2015). ZL70103 Medical Implantable RF Transceiver.
39. Mishra, D., De, S., Chowdhury, K.R. (2015). Charging time characterization for wireless rf energy transfer. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 62(4), 362–366.
40. Patrick, C., & Schaumont, P. (2016). The role of energy in the lightweight cryptographic profile. In *NIST lightweight cryptography workshop*.
41. Prutchi, D. (2012). St. Jude's (ANS) Rechargeable Spinal Cord Stimulators Eon and Eon Mini. <http://www.implantable-device.com/>.
42. Rostami, M., Burleson, W., Koushanfar, F., Juels, A. (2013). Balancing security and utility in medical devices? In *Proceedings of the 50th annual design automation conference* (p. 13). ACM.
43. Rostami, M., Juels, A., Koushanfar, F. (2013). Heart-to-heart (H2H): authentication for implanted medical devices. In *Proceedings of the 2013 ACM SIGSAC conference on computer & communications security* (pp. 1099–1112). ACM.
44. Rushanan, M., Rubin, A.D., Kune, D.F., Swanson, C.M. (2014). Sok: security and privacy in implantable medical devices and body area networks. In *2014 IEEE symposium on security and privacy* (pp. 524–539). IEEE.
45. Sample, A.P., Yeager, D.J., Powledge, P.S., Smith, J.R. (2007). Design of a passively-powered, programmable sensing platform for uhf rfid systems. In *2007 IEEE international Conference on RFID* (pp. 149–156). IEEE.
46. Schaumont, P., Yuce, B., Pabbuleti, K., Mane, D. (2016). Secure authentication with energy-harvesting: a multi-dimensional balancing act. *Sustainable Computing: Informatics and Systems*, 12, 83–95.
47. Siddiqi, M.A., Seepers, R.M., Hamad, M., Prevelakis, V., Strydis, C. (2018). Attack-tree-based threat modeling of medical implants. In *PROOFS 2018. 7th international workshop on security proofs for embedded systems*, Kalpa publications in computing vol. 7 (pp. 32–49). Easy Chair.
48. Siddiqi, M.A., & Strydis, C. (2019). IMD security vs. energy: are we tilting at windmills? POSTER. In *Proceedings of the 16th ACM international conference on computing frontiers* (pp. 283–285). ACM.
49. Siddiqi, M.A., & Strydis, C. (2019). Towards realistic battery-DoS protection of implantable medical devices. In *Proceedings of the 16th ACM international conference on computing frontiers* (pp. 42–49). ACM.
50. Strydis, C., Seepers, R.M., Peris-Lopez, P., Siskos, D., Sourdis, I. (2013). A system architecture, processor, and communication protocol for secure implants. *ACM Transactions on Architecture and Code Optimization (TACO)*, 10(4), 57.
51. Technologies, E. (2020). Empowering life - batteries for medical devices. <https://www.eaglepicher.com/markets/medical-power/>.
52. Tippenhauer, N.O., Malisa, L., Ranganathan, A., Capkun, S. (2013). On limitations of friendly jamming for confidentiality. In *2013 IEEE symposium on security and privacy* (pp. 160–173). IEEE.
53. Yang, Q., Mai, S., Zhao, Y., Wang, Z., Zhang, C., Wang, Z. (2014). An on-chip security guard based on zero-power authentication for implantable medical devices. In *2014 IEEE 57th international midwest symposium on circuits and systems (MWSCAS)* (pp. 531–534). IEEE.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Muhammad Ali Siddiqi received the B.E. degree in electrical (telecommunication) engineering from National University of Sciences and Technology, Islamabad, Pakistan, in 2009 and the (joint) M.Sc. degree in embedded computing systems from Norwegian University of Science and Technology, Trondheim, Norway, and University of Southampton, UK, in 2012. He is currently pursuing the Ph.D. degree at the Neuroscience department

of the Erasmus Medical Center, the Netherlands.

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



Wouter A. Serdijn was born in Zoetermeer ('Sweet Lake City'), the Netherlands, in 1966. He received the M.Sc. (cum laude) and Ph.D. degrees from Delft University of Technology, Delft, The Netherlands, in 1989 and 1994, respectively. Currently, he is a full professor in bioelectronics at Delft University of Technology, where he heads the Section Bioelectronics, and a visiting honorary professor at University College London, in

the Analog and Biomedical Electronics group.

His research interests include integrated biomedical circuits and systems for biosignal conditioning and detection, neuroprosthetics, transcutaneous wireless communication, power management and energy harvesting as applied in, e.g., cardiac pacemakers, cochlear implants, neurostimulators, bioelectronic medicine and electroceuticals.



Christos Strydis is an assistant professor with the Neuroscience department of the Erasmus Medical Center, the Netherlands, and is also a chief engineer with Neurasmus BV, the Netherlands. His current research interests span the fields of brain simulations, high-performance computing, low-power embedded (in particular, implantable) systems and functional ultrasound imaging. Dr. Strydis holds a M.Sc. (Cum Laude)

and a Ph.D. in computer engineering from the Delft University of Technology. He is a senior member of the IEEE.