Security and Privacy for Fat Intra-Body Communication: Mechanisms and Protocol Stack

Johan Engstrand*, Konrad-Felix Krentz*[1], Noor Badariah Asan†, Madhushanka Padmal*, Wenqing Yan*, Laya Joseph*, Pramod Rangaiah*, Bappaditya Mandal*, Christian Rohner*, Maria Mani*, Robin Augustine*, Thiemo Voigt*‡
*Uppsala University, Sweden. †Universiti Teknikal Malaysia Melaka, Malaysia. ‡RISE Computer Science, Sweden.

2024 IEEE 49th Conference on Local Computer Networks (LCN) | 979-8-3503-8800-8/24/$31.00 ©2024 IEEE | DOI: 10.1109/LCN60385.2024.10639677

***Abstract*—Innovative medical applications based on networked implants foster the development of in-body communication technologies. Among the in-body communication technologies that are being considered, fat intra-body communication (Fat-IBC) is a very recent approach. Its main advantage lies in its higher data rate compared to earlier approaches based on capacitive and galvanic coupling. However, Fat-IBC faces privacy-, security-, as well as safety-related attacks. In this paper, we discuss security and privacy concerns about Fat-IBC, as well as corresponding countermeasures. Furthermore, we present our secure protocol stack for Fat-IBC and suggest directions for future research.**

I. Introduction

Medical implants, such as pacemakers, implantable cardioverter-defibrillators, implantable drug pumps, or implantable glucose sensors, found their way into medical practice. The next step is to consider networks of implants, commonly referred to as in-body networks. In-body networks have several applications. One example is closed-loop insulin delivery, where implanted glucose sensors report their measurements to an implanted insulin pump, which automatically infuses insulin. Another example is electroceuticals, where implanted neurostimulators stimulate organs, taking into account physiological signals that are potentially sensed elsewhere in a patient's body by separate implants.

For the communication between implants, a recent approach is to use the fat tissue of the human body as a medium for transmitting radio frequency (RF) signals, as shown in Fig. 1 [1]. Generally, signals at microwave frequencies, such as in the 2.4-GHz band, are highly attenuated by skin and muscle tissues since the dielectric constant of these tissues is high. However, such signals are not attenuated by as much in the fat tissue due to its comparatively low dielectric constant. Furthermore, in most areas of the human body, fat is surrounded by muscle and skin, thereby forming a waveguide. This enhances the signal transmission through the fat tissue and ultimately allows implants to reduce their transmit power, as is crucial for meeting specific absorption rate (SAR) regulations.

Compared to prior approaches based on capacitive and galvanic coupling, Fat-IBC can achieve higher data rates. This opens up additional application areas for in-body networks, such as neuroprosthetics. In fact, the Horizon 2020 project "B-CRATOS" focuses on wirelessly connecting a brain-computer interface (BCI) to a prosthetic arm via Fat-IBC [2]. It is a cross-disciplinary project that leverages Fat-IBC for efficient and reliable transmission of neural data from brain to prosthetic in order to restore motor function and for getting sensory feedback from an artificial skin back to the brain.

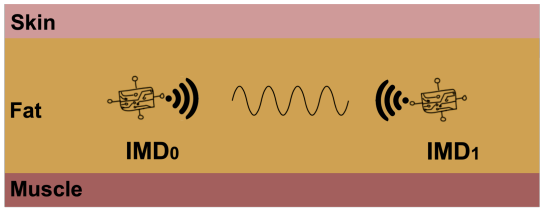


Fig. 1. In-body communication through the fat tissue [1].

Fat-IBC also plays a key role in the recently started BOS (Body Operating System) project [3]. BOS aims to create a cross-platform, modular, and energy-efficient software toolkit for developing body computing applications. Such applications employ sensors and actuators in and on the body, as well as computing platforms outside of the human body, comprising wearable technology, implants, and brain-machine interfaces, combined with computing resources at the edge and cloud.

However, two general concerns about in-body networks become more prevalent when using Fat-IBC. The first of them relates to privacy. Even just knowing about the presence of implants may be of concern for some patients, e.g., due to an associated social stigma or the high cost of certain implants. In the case of Fat-IBC, maintaining privacy is particularly challenging since RF signals may leak outside a patient's body, although they are highly attenuated by the skin [4]. The second general concern about Fat-IBC relates to security and safety. Altered measurements may, e.g., result in wrong treatment or cause implanted actuators to act malevolently. Such attack scenarios must be taken seriously when applying Fat-IBC, as RF signals may penetrate into a patient's body, too.

In this paper, we discuss security and privacy issues in Fat-IBC, as well as corresponding countermeasures. We start in Section II with a description of the most important physical properties of Fat-IBC including its sensing capabilities. We connect in-body networks to the external world using a gateway that we call aggregator. We describe different aggregator designs in Section III. Section IV is devoted to security and privacy while Section V describes the upper layers of our

[1] Konrad-Felix Krentz is now with Siemens

current Fat-IBC stack. Before concluding, we discuss future directions in Section VI.

II. Background: Fat Communication and Sensing

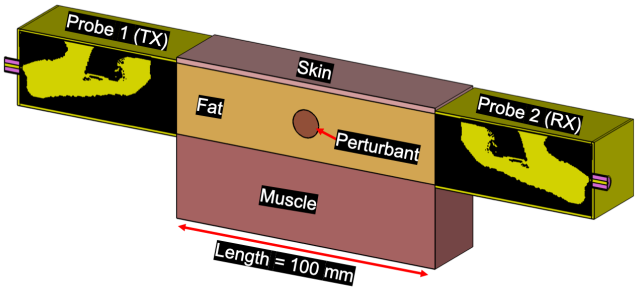
Human tissues have varying water concentrations. Adipose tissue contains 5–10% water and bone 8–16%, while other tissues such as muscle (73–78%) and skin (60–76%) have significantly higher water content [5]. Due to its low water content, adipose tissue has a low dielectric constant, which makes it a potential candidate as an in-body communication channel for microwave radio communication. As mentioned previously, human fat tissue, in particular the subcutaneous fat, i.e., the layer of fat beneath the skin, is sandwiched between the skin and the underlying muscles, creating a dielectric waveguide-like structure, which makes it a suitable communication medium for RF.

We have shown the feasibility of human fat as a communication medium through *i)* simulations with CST Studio Suite, *ii)* ex-vivo experiments that use porcine tissue, *iii)* phantoms, artifacts that emulate the dielectric properties of human tissue, and *iv)* in-vivo experiments with a live porcine model [6, 7].

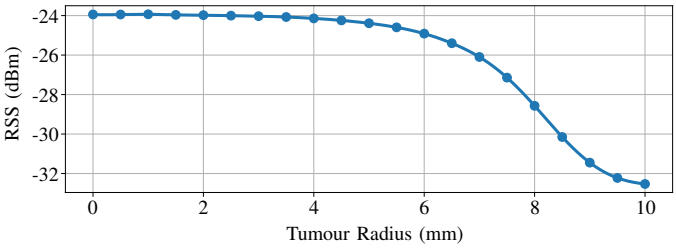
Our experiments have shown that the fat channel has an attenuation of 1–2 dB/cm [1]. Hence, it is possible to bridge larger distances through the fat tissue: We have communicated across 30–40 cm, and using phantoms we have shown that front-to-back communication is possible. While a thicker fat layer allows for more efficient communication, we have also communicated through thinner fat layers with diameters below 1 cm. Furthermore, we have demonstrated that efficient communication through fat tissue is possible even in the presence of perturbants such as embedded muscle layers and blood vessels [8]. We have further shown that there is not much impact when the antennas are not aligned [9].

We have experimented with different physical layer protocols. The 6LoWPAN protocol stack employs 2.4-GHz IEEE 802.15.4 offset quadrature phase-shift keying (O-QPSK) [10] as physical layer (PHY). This PHY was successfully tested for Fat-IBC [6, 11]. Using 10 dBm transmit power and the IEEE 802.11n protocol (Wi-Fi 4), the fat channel can support data rates as high as 92 Mbit/s for any combination of on-skin and in-fat antennas over distances up to 30 cm in a phantom [12]. Furthermore, we have also shown that Fat-IBC works well in the 5.8-GHz band [9]. The antennas can be made physically smaller at such higher frequencies, but there is also a loss in range inside the body. We have concentrated on the Industrial, Scientific and Medical (ISM) bands for Fat-IBC since they are often free from local regulations and thus do not impose travel restrictions on patients.

Fat-IBC can be used not only for communication, but also for monitoring changes in the properties of the communication channel. For example, using Fat-IBC we can detect a growing tumour by observing changes in the received signal strength (RSS) over a long period of time [13, 14]. Figure 2 shows the setup and result of a simulation that demonstrates the effect a growing tumour has on the RSS. When the tumour grows in size, the RSS decreases. We have demonstrated the same phenomenon with an anthropomorphic, semi-solid breast phantom [14]. By monitoring this change over time, we can detect the presence of a perturbant (such as a cancer relapse) in the channel. Such observations could be helpful for identifying a medical condition at an early stage in order to then initiate the appropriate treatment.



(a) Simulation setup. A perturbant (tumour) growing in adipose tissue between a layer of skin and another of muscle [13]. The layers are 2, 25 and 30 mm thick for the skin, fat and muscle respectively. The transmitter (TX) probe launches microwave signals (at 2.4 GHz) through the adipose layer to the receiver (RX) probe at 0 dBm output power.



(b) Simulation result [13]. As the tumour grows, the received signal strength (RSS) decreases. Monitoring this decrease over a period of time reveals the presence of the tumour/perturbant in the channel.

Fig. 2. Setup and result of a simulation demonstrating continuous in-body tumour monitoring.

III. Aggregator Designs

Coupling out signals from inside the human body is impossible from many locations at low transmit power. However, using a communication medium that is present almost everywhere in the human body, such as fat, will enable relaying in-body data to a location close to the skin from where it is easy to couple out signals. This enables remote patient monitoring and remote treatment.

An *aggregator* is the gateway between the in-body network and the external world. The aggregator's main task is to forward data from implants to the external world, for example, sensor data and implants' status information. In addition, the aggregator also relays data from the external world to the implants, for example, control commands and code updates.

There are multiple design options for an aggregator for Fat-IBC [15]: First, the aggregator can be partially implanted, i.e., there is an antenna that penetrates the skin. This antenna launches the signals into the subcutaneous fat tissue. Such a setup is similar to commercial glucose monitoring systems.

Second, the aggregator can be placed on the skin. Hence, the aggregator is completely outside and has to launch its signal through the skin into the fat tissue. Such an on-skin aggregator might be the most straightforward to realize. It must, however, overcome the large attenuation posed by the skin, which is around 27 dB [4].

A third design employs a repeater node implanted in the fat that is wirelessly powered by an on-skin aggregator, allowing for better performance at the cost of more engineering work (in particular related to wireless power transfer).

We have earlier discussed the pros and cons of each solution in more detail [15]. The three designs are summarized in Table I. The aggregator may also support other functions. Examples include security-related tasks, such as the reduction of the information leakage when performing in-body measurements [13].

IV. Security and Privacy: Attacks and Countermeasures

Typically, in wired communication, signals are confined to the wired medium. This prevents signal leakage to the outside environment. By contrast, the use of radio signals for wireless communication in Fat-IBC poses challenges in confining the signals within the body. The openness of the wireless medium also makes it prone to adversaries being able to tamper with the communication through injection and jamming attacks.

In this section, we catalogue attacks against Fat-IBC and outline the state of the art in defending against them, as summarized in Table II.

A. Types of Security Issues in Fat-IBC

The following are some of the security issues that can arise in Fat-IBC:

1) Eavesdropping attacks: Adversaries have access to several powerful tools and mechanisms to eavesdrop on implant-to-implant communication. The adversaries' resources stand in stark contrast to the low-power and resource-constrained environment in which the implants operate [16]. Adversaries can, e.g., use antenna arrays to take advantage of the spatial diversity of the signals to increase the receiver performance. Moreover, multiple adversaries can collaborate to perform signal pre-processing to extract the transmitted signals [17]. The communication therefore lacks security against eavesdropping attacks where external adversaries snoop on the channel to intercept packets or measure received signal strength indicators (RSSIs) [13].

2) Injection and replay attacks: In a similar manner, RF signals can penetrate the human body. This enables attackers with high transmit powers to inject radio messages into Fat-IBC. By means of such injection attacks, an attacker may, e.g., trick an implanted drug pump into acting in a malicious way.

Also, injection attacks can be combined with eavesdropping in order to replay previously captured radio messages. This may help an attacker pass security checks. One kind of replay attack is a reflection attack, where a radio message is resent to the original sender [18]. Another kind of replay attack is a delay attack, where the original message is delayed, thus causing its contents to be outdated on arrival [19]. Finally, eavesdropping, injection, and replay attacks may allow an attacker to mount a man-in-the-middle attack, where the attacker acts as a relay that alters, delays, drops, or inserts messages at will [18].

3) Denial of Service (DoS) attacks: Adversaries can hinder communication by jamming Fat-IBC. Depending on an attacker's goals, jamming may be carried out continuously or reactively. Continuous jamming generally hinders Fat-IBC. Reactive jamming, by contrast, only hinders Fat-IBC exactly when an implant transmits a radio message whose reception the attacker wishes to prevent. To extend the effective jamming range, an attacker can launch a drizzle attack, where the attacker emits properly modulated preambles in a back-to-back sequence [20]. Upon detecting such a preamble, receivers will interpret the trailing bytes as the PHY payload, just to conclude that the payload is malformed. Thus, drizzle attacks keep victim implants busy and thus unable to receive legitimate radio messages.

Instead of "only" hindering communication, attackers may aim at depleting the limited battery charge of implants [21]. Such attacks are often referred to as denial-of-sleep attacks because they deprive victim devices from entering energy-saving sleep modes. Denial-of-sleep attacks pose a severe threat to battery-powered implants as their batteries may be laborious to recharge, if they are rechargeable at all. A temporary outage of an energy-harvesting implant can be dangerous for a patient, too.

Important kinds of denial-of-sleep attacks are reception- and transmission-oriented ones [22]. In a reception-oriented denial-of-sleep attack, the victim device mainly loses charge due to spending more time in the energy-consuming receive mode. An often applicable reception-oriented denial-of-sleep attack is to inject unwanted radio messages. Even if a victim device eventually discards unwanted radio messages, it will normally consume some of its limited charge for receiving and processing them. Analogously, in a transmission-oriented denial-of-sleep attack, the victim device mainly loses charge due to spending more time in the energy-consuming transmit mode. An example of a transmission-oriented denial-of-sleep attack is a collision attack, where the attacker reactively jams unicast radio messages or corresponding acknowledgments [23]. This normally causes numerous energy-consuming retransmissions.

4) RF sensing: As signals propagate in the human body, organs bounce off these signals, and tissue dynamics also affect the propagation of RF signals. The resultant temporal variations in amplitude and phase can, e.g., be used for sensing human vital signs and for tracking tumours of cancer patients [13]. Such techniques are collectively referred to as "RF sensing".

Unfortunately, RF sensing can be perverted to attack a patient's privacy. Since the physical properties of RF signals are publicly visible, even when using encryption mechanisms, passive eavesdroppers can deduce medical patient information from these RF signals.

TABLE I
COMPARISON OF THE THREE AGGREGATOR TYPES

Aggregator type	Infection	Location	Power	Performance
Partially implanted	Highest risk	Less fat	Moderate	High
On-skin	Lower risk	More fat	More	Low
On-skin, with repeater	High risk	More fat	More (less for repeater)	Highest

TABLE II
ATTACKS AGAINST FAT-IBC AND STATE-OF-THE-ART DEFENSES

Attack	Defenses
eavesdropping and injection	friendly jamming, transmission power randomization, symmetric-key cryptography, PS-based symmetric key establishment
replay	time-based message authentication codes, RF fingerprinting
jamming	channel hopping, Black Networks
denial-of-sleep	one-time passwords, leaky bucket counters
RF sensing	specially designed antennas, wireless covert communication technology, friendly jamming, channel hopping

Moreover, active attackers may interfere with RF signals in a way that distorts the medical patient information obtained by implants through RF sensing. Thus, by contaminating the RF environment, active attackers may alter RF sensing measurements, potentially with safety-related repercussions.

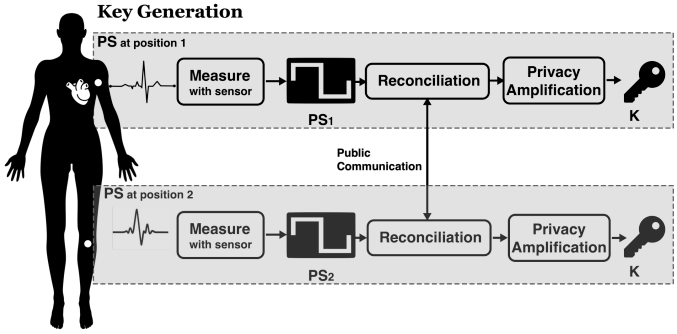
B. Countermeasures for Security Issues in Fat-IBC

In the following, we discuss possible methods to counter the above security issues.

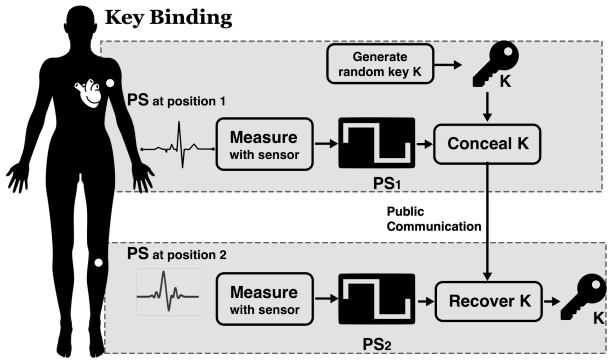
1) Eavesdropping attacks: Quantifying the amount of signal leakage is crucial to understand the security implications of the communication. This will allow us to design secure communication protocols that can protect the data transmitted by the implants. Through experimental and simulation results, the amount of signal leakage towards the external environment from the in-body fat (through the skin layer) has been quantified as 27 dB at 2.45 GHz [4]. The skin layer's high dielectric constant (compared to that of the fat layer) causes significant RF signal attenuation, which results in a lower signal strength outside the body compared to the in-body environment, rendering it difficult for adversaries to intercept the signals.

We can exploit this signal attenuation to counter eavesdropping attacks in multiple ways. One approach is to reduce the transmit signal power to such low levels that the leaked signal will be buried in the noise floor. Another approach is to use a friendly jammer to generate an interfering signal such that the adversaries get obstructed without being able to receive any information from the in-body signals. Combination of the above two methods is another approach to counter possible eavesdropping attacks where one can vary both the transmit power as well as the jamming signal power to further confuse the eavesdroppers.

2) Injection attacks: A basic defense against eavesdropping and injection attacks is to encrypt and authenticate radio messages. Symmetric-key cryptography is more suitable for implants than public-key cryptography. This is because symmetric-key cryptography consumes less of the scarce energy and computing resources of implants.



(a) Key Generation



(b) Key Binding

Fig. 3. Approaches to physiological signal-based symmetric key establishment.

However, symmetric-key cryptography depends on *symmetric keys*, which are challenging to establish due to the resource constraints on implants. This situation is similar in the Internet of things (IoT), where practitioners often resort to predistributing symmetric keys. While key predistribution is lightweight, it incurs management overhead: an implant must be preloaded with symmetric keys before it is implanted. In order to add more implants or to exclude certain implants from Fat-IBC, it is necessary to externally store the predistributed symmetric keys, as well as, potentially, to keep track of already implanted implants.

These issues give rise to a novel research direction in the context of in-body networks, namely physiological signal (PS)-based symmetric key establishment. Here, the basic approach is that a person's implants simultaneously collect measurements of a PS, such as interpulse intervals, and then derive a symmetric key from these correlated measurements.

More specifically, there are two approaches to PS-based symmetric key establishment, namely *key binding* and *key generation*, as shown in Fig. 3 [24]. In key binding, one communication partner generates a random symmetric key and uses its measurements to conceal that key. The resulting cipher text is sent to the other communication partner along with public helper data. Upon reception, the other communication partner uses its own measurements, which are correlated with those of the sender, and the public helper data to restore the random symmetric key. In key generation, the measurements themselves are turned into a symmetric key. This is done through a public discussion, where both communication partners reconcile the discrepancies in their measurements. Often, this reconciliation phase is followed by a privacy amplification phase, where the reconciled bit strings are distilled into shorter high-entropy bit strings, which can serve as symmetric keys.

Current research efforts revolve around three security concerns about PS-based symmetric key establishment. Firstly, PS-based symmetric key establishment becomes insecure if an attacker can measure a PS using other means than in-body or on-body sensors. For example, interpulse intervals were shown to be vulnerable to such an attack. Using a technique called remote photoplethysmography, one can accurately measure interpulse intervals via an on-site camera [25]. This result spurred the study of PSs that can only be measured through in-body or on-body sensors, such as local field potentials [18]. Secondly, several protocol-level vulnerabilities were found in prominent PS-based symmetric key establishment schemes, which might be eliminated through protocol verification [18]. Thirdly, to harden PS-based symmetric key establishment against various security incidents, such as compromised implants, hybrid solutions are being considered. We earlier proposed combining PS-based symmetric key establishment with PHY key generation in such a way that reciprocal channel characteristics add another layer of defense [26]. Later, we tailored this work to establish symmetric keys between 2-hop neighbors [27].

3) Replay attacks: A common technique for preventing replay attacks is counter-based replay protection. The general idea is that an implant A who wishes to send a message to another implant B adds an incrementing counter to the message. Upon reception of a message that presumably originates from A, B accepts the message only if its counter is greater than that of the last authentic message received from A.

Unfortunately, counter-based replay protection only provides sequential freshness. Sequential freshness ensures that no message is accepted more than once, but does not prevent delay attacks. Strong freshness, by contrast, additionally ensures that a message was sent during a limited prior to its reception so as to restrict delay attacks.

Techniques for achieving strong freshness are timestamps, nonces, and time-based message integrity codes (MICs). A drawback of timestamps, however, is that they depend on time synchronization, which is an energy-consuming continually ongoing process. A drawback of nonces is that they require the exchange of additional messages each time a message must be protected against replay attacks. Both of these drawbacks are widely avoided by entangling time information in MICs [22, 28].

RF fingerprinting attains strong freshness, as each communication is uniquely identifiable based on physical transmitter hardware characteristics such as its frequency response, modulation errors, and transient behavior [29, 30]. These features are difficult to replicate accurately unless the attacker has precise control over the hardware to imitate the RF fingerprint with high fidelity. Unlike timestamp and nonce-based methods, which rely on temporal data or random values to prevent replay attacks, RF fingerprinting does not depend on synchronization or additional data exchange, which makes it inherently more robust. The passive nature of these mechanisms completely eliminates the overhead on the transmitter side. We have recently demonstrated an implementation on resource-constrained embedded systems, making it suitable for implants [30].

4) Denial of Service (DoS) attacks: A mitigation to continuous jamming is to switch to less interfered channels, e.g., using multi-armed bandit (MAB)-based channel hopping [31]. Channel hopping has the added advantage of alleviating multipath fading and interference. It also complicates eavesdropping and RF sensing attacks. Reactive jamming may, on the other hand, be mitigated by padding radio messages to a common length — a concept sometimes called *black networks*. It makes it more difficult for attackers to reactively jam specific radio messages.

As for defending against denial-of-sleep attacks, two patterns emerged [22]; LBC, on the one hand, can limit the worst-case energy consumption of recurring tasks. This works through a rate limitation that may overshoot temporarily, as long as a virtual bucket does not overflow. The ability to overshoot temporarily preserves responsiveness under load. OTP, on the other hand, can serve to mitigate many reception-oriented denial-of-sleep attacks. The basic idea is to embed an one-time password (OTP) either in the Layer 1 or Layer 2 header of a radio message, and to validate this embedded OTP early during reception. If the OTP of a radio message turns out invalid, the reception of the radio message is cancelled, which avoids expending further energy. Meanwhile, the cancellation happens so fast that injection and replay attacks cause no increased energy consumption at all [22].

5) RF sensing: Encryption is insufficient for preventing passive eavesdroppers from figuring out medical data about a patient via RF sensing. This is because PHY features such as amplitude and phase can be obtained despite encryption. Countermeasures against this novel type of eavesdropping are still in an infant stage, yet three research directions are promising: The first one utilizes specially designed antennas that provide security benefits by limiting the effective radiation region. Antennas for in-body communication can be optimized to efficiently radiate into the fat tissue [1]. Limiting the radiation region reduces the likelihood of successful eavesdropping attacks. The second one relies on wireless covert communication technology, which hides the ongoing legiti-

CoAP
UDP
IPv6, RPL
6LoWPAN
TSCH
IEEE 802.15.4 PHY (2.4-GHz O-QPSK)

(a)

CoAP, OSCORE-NG
UDP
IPv6
6LoWPAN, SMOR
HPI-MAC
IEEE 802.15.4 PHY (2.4-GHz O-QPSK)

(b)

Fig. 4. (a) Standard 6LoWPAN protocol stack and (b) as adapted for Fat-IBC

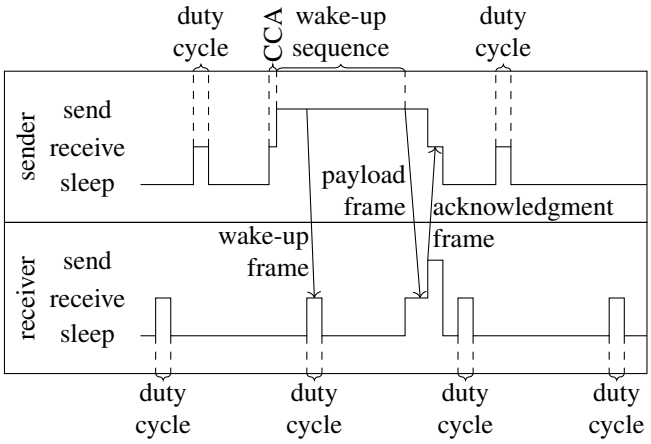


Fig. 5. CSL regularly wakes up to scan for a wake-up frame. Correspondingly, senders precede the transmission of an actual so-called *payload frame* with a sequence of *wake-up frames*, each of which contains the remaining time until the transmission of the payload frame begins. This allows a receiver to go back to sleep shortly after having received a wake-up frame. An acknowledgment frame confirms the reception of a unicast payload frame.

mate communication by randomly changing the transmission power [32]. The third and last one is using artificial noise-aided methods, which leverage friendly jammers that generate RF interference toward potential eavesdroppers [33].

V. Upper-Layer Protocols

As Fat-IBC networks are low-power radio networks, the upper-layer protocols for low-power radio networks are obvious candidates for Fat-IBC networks. In particular, the IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) protocol stack, which is shown in Fig. 4a, is a prime candidate since it is widely adopted in the IoT [34]. The 6LoWPAN protocol stack will therefore serve as a starting point for discussing upper-layer protocols for Fat-IBC in this section. Our discussion leads us to adapt the 6LoWPAN protocol stack shown in Fig. 4b.

A. Medium Access Control

The 6LoWPAN protocol stack uses time-slotted channel hopping (TSCH) as its medium access control (MAC) protocol [10]. In TSCH, transmissions happen within timeslots and a scheduler takes care of assigning the timeslots in a way that minimizes collisions. Furthermore, TSCH accounts for energy-constrained devices by letting receivers leave their radios off during timeslots where no incoming receptions are scheduled. Another feature of TSCH is channel hopping, which alleviates the effects of multipath fading and interference.

Yet, TSCH has security vulnerabilities, which hinder its adoption for Fat-IBC. Compromised nodes can launch various attacks against TSCH's mechanisms for time synchronization [35]. Moreover, unsynchronized TSCH nodes waste much energy under beacon jamming, where an attacker exploits the fact that unsynchronized TSCH nodes stay in the energy-consuming receive mode until they receive a beacon frame indefinitely [22, 36]. Some mitigation methods have been conceived, but each of them comes with its own issues [22, 37].

An alternative to TSCH is the coordinated sampled listening (CSL) MAC protocol [10]. CSL works without network-wide time synchronization and avoids the associated security vulnerabilities, as shown in Fig. 5. Nevertheless, like TSCH, CSL features a low base energy consumption and supports channel hopping. Beyond that, CSL attains better throughput via so-called "streaming" [38], and possesses an intrinsic resilience to denial-of-sleep attacks [22]. Yet, CSL does not resist all denial-of-sleep attacks, something that is being addressed by Hasso Plattner Institute MAC (HPI-MAC) [22].

HPI-MAC adds denial-of-sleep defenses, a neighbor discovery and pairwise session key establishment scheme, as well as time-based MICs to CSL [22]. Experimental results suggest that HPI-MAC performs well on top of Fat-IBC, attaining a frame delivery ratio of 99.2% with MAB-based channel hopping [11, 31].

B. 6LoWPAN

6LoWPAN enables seamless IPv6 connectivity with and between low-power IEEE 802.15.4 nodes through two mechanisms [38, 39]. First, 6LoWPAN compresses IPv6 and user datagram protocol (UDP) headers during their transfer over IEEE 802.15.4 links. Second, 6LoWPAN fragments IPv6 packets that do not fit within single IEEE 802.15.4 frames despite of compression. However, it should be noted that 6LoWPAN comes without defenses against fragmentation attacks. Countering such attacks requires complementary defenses, for which we refer practitioners to [40]–[42].

C. Routing

For routing IPv6 packets, the 6LoWPAN protocol stack adopts the Routing Protocol for Low-Power and Lossy Networks (RPL) [43]. RPL organizes an IEEE 802.15.4 network into a set of destination-oriented directed acyclic graphs (DODAGs), each of which is directed to a single root node. Root nodes typically provide a path to the Internet. In the context of Fat-IBC, aggregators could act as root nodes.

Nevertheless, there are four reasons why RPL is a mismatch for Fat-IBC: First, RPL assumes a relaxed threat model and is particularly susceptible to compromised nodes [44]. Second, RPL takes routing decisions at the network layer. At the MAC layer, this causes long delays as it may take long until a

specific forwarder wakes up. Third, tree-based routing may incur detours and may even prevent communication despite the presence of operational routing paths. Forth, RPL is designed for mesh networks with arbitrary network diameters and therefore incurs much functionality that is superfluous for Fat-IBC.

These limitations motivated a dedicated routing protocol for Fat-IBC, namely secure multipath opportunistic routing (SMOR) [45]. Inspired by "INSENS" and EchoRing [46, 47], SMOR duplicates packets on purpose and routes them along disjoint paths. This results in unprecedented packet delivery ratios of 99.999% in Fat-IBC networks and makes SMOR tolerant of compromises of single nodes, too. Another main concept of SMOR is to opportunistically select a currently available forwarder, rather than waiting for a particular forwarder to awake. This measure improves delays by between 33.51% and 39.84% compared to RPL in Fat-IBC scenarios. To remain compatible with 6LoWPAN's fragmentation, SMOR operates as a mesh-under routing protocol, i.e., takes routing decisions underneath 6LoWPAN. Normally, 6LoWPAN requires delivering all fragments to the same next hop, thus preventing opportunistic routing for all but the first fragment of a packet. As a mesh-under routing protocol, SMOR can route fragments freely and reassembly happens on the destination host or aggregator. A final important concept of SMOR is to restrict itself to 2-hop topologies. This suffices for Fat-IBC while sidestepping security issues and avoiding unnecessary overhead.

D. Application Layer

At the application layer, the 6LoWPAN protocol stack utilizes the constrained application protocol (CoAP) [48]. CoAP follows the representational state transfer (REST) paradigm and is lightweight in terms of RAM usage and communication overhead due to its ability to run on top of UDP.

For securing CoAP, four protocols come into question, namely IPsec [49], Datagram Transport Layer Security (DTLS) [50], Object Security for Constrained RESTful Environments (OSCORE) [51], and OSCORE next-generation (OSCORE-NG) [28]. Among them, OSCORE-NG is the most secure, being the only one that prevents both delay and denial-of-sleep attacks. To also protect against remote denial-of-sleep attacks, however, all four protocols should be combined with a middlebox that filters out unwanted messages from the Internet en-route [52]–[55]. Ideally, the filtering should happen in a trusted execution environment (TEE) so as to confine the middlebox's trusted computing base. Note that with the right hardware support, the aggregator could act as the middlebox. A challenge in this context is to prevent bypassing of the TEE. This can be solved by empowering the TEE to issue special OTPs [55].

VI. Future Directions

As discussed in Section IV, the wireless nature of Fat-IBC allows for attacks. We have earlier presented privacy-preserving mechanisms for the protection of tumour relapse measurements [13]. We have also argued that friendly RF jamming can support such mechanisms [56]. At the same time, friendly jamming may also help to establish a covert communication channel, i.e., hiding that there is any communication inside the body. This should be possible due to the high attenuation of the skin layer [4].

Protecting RF sensing from active interference, on the other hand, was not yet investigated to the best of our knowledge. We conjecture that existing jamming detection techniques could be tailored to this problem. More specifically, by monitoring the consistency of received signal strengths, packet delivery ratios, bit error rates, or carrier sensing times, active interference with RF sensing could possibly be detected.

Powering implants is challenging in that there are not many opportunities to harvest large amounts of power inside the body. There are opportunities to further reduce the energy consumption for Fat-IBC using, for example, backscatter communications [57]. We believe that the salient properties of the fat tissue also make it possible to use RF harvesting by exploiting the aggregator or implants that can easily be powered, for example, since they are close to the surface of the body to launch RF waves into the fat channel that other implants may harvest. In this direction the use of metamaterials that help direct the RF waves in a way that improves efficiency [58]. Note, however, that the RF harvesting process may also be susceptible to attacks [59].

Also, in the context of energy harvesting, securing MAC protocols is a widely open issue. Standard MAC protocols, such as CSL or TSCH, are not very suitable for energy-harvesting devices due to the difficulty of timekeeping on such devices [60]. Hence, specialized MAC protocols should be developed without compromising on security features, such as denial-of-sleep resilience.

VII. Conclusions

In this paper, we have argued that Fat-IBC is a viable communication paradigm to network implants inside the human body. The fat tissue is often situated between skin and muscle, which enables a waveguiding effect that leads to communication with lower losses and higher data rates than other in-body communication technologies, with a range long enough to enable back-to-front body communication. As pertubants such as tumors impact the communication properties, Fat-IBC can also be used for sensing, for example, to detect cancer relapse. When networking implants, security and privacy are of utmost importance. We have detailed the current status of security and privacy of this novel communication paradigm. In particular, we have detailed the adaptation of the standard 6LoWPAN protocol stack for Fat-IBC. Finally, we have discussed some future directions.

Acknowledgements

This work has been financially supported the Swedish Foundation for Strategic Research.

REFERENCES

[1] N. B. Asan, *Fat-IBC: A New Paradigm for Intra-body Communication*. PhD thesis, Uppsala University, 2019.

[2] "What is B-Cratos — B-Cratos." https://www.b-cratos.eu/what-is-b-cratos/, 2024. Accessed: [09-06-2024].

[3] "BOS: software priniples & techniques for a body-centric OS." https://www2.it.uu.se/research/group/uart/bos, 2024. Accessed: [07-06-2024].

[4] M. Padmal, J. Engstrand, R. Augustine, and T. Voigt, "Signal Leakage in Fat Tissue-Based In-Body Communication: Preserving Implant Data Privacy," in *Proceedings of the Int'l ACM Conference on Modeling Analysis and Simulation of Wireless and Mobile Systems*, MSWiM '23, pp. 225–232, Association for Computing Machinery, 2023.

[5] V. Komarov, S. Wang, and J. Tang, "Permittivity and measurements," in *Encyclopedia of RF and microwave engineering* (K. Chang, ed.), New York, USA: John Wiley and Sons, Inc., 2015.

[6] N. B. Asan, C. P. Penichet, S. Redzwan Mohd Shah, D. Noreland, E. Hassan, A. Rydberg, T. J. Blokhuis, T. Voigt, and R. Augustine, "Data packet transmission through fat tissue for wireless intra-body networks," *IEEE Journal of Electromagnetics, RF and Microwaves in Medicine and Biology*, vol. 1, no. 2, pp. 43–51, 2017.

[7] J. Engstrand, M. D. Perez, B. Mandal, J. Liden, C. Rohner, T. Voigt, and R. Augustine, "End-to-end transmission of physiological data from implanted devices to a cloud-enabled aggregator using fat intra-body communication in a live porcine model," in *2022 16th European Conference on Antennas and Propagation (EuCAP)*, pp. 1–5, IEEE, 2022.

[8] N. B. Asan, J. Velander, Y. Redzwan, R. Augustine, E. Hassan, D. Noreland, T. Voigt, and T. J. Blokhuis, "Reliability of the fat tissue channel for intra-body microwave communication," in *2017 IEEE Conference on Antenna Measurements & Applications (CAMA)*, IEEE, 2017.

[9] N. B. Asan, E. Hassan, M. D. Perez, L. Joseph, M. Berggren, T. Voigt, and R. Augustine, "Fat-intrabody communication at 5.8 GHz: Verification of dynamic body movement effects using computer simulation and experiments," *IEEE Access*, vol. 9, pp. 48429–48445, 2021.

[10] "IEEE Standard 802.15.4-2020," 2020.

[11] K.-F. Krentz, M. Padmal, B. Mandal, R. Augustine, and T. Voigt, "Dataset: Enabling offline tuning of fat channel communication," in *Proceeindgs of the Data: Acquisition To Analysis (DATA '21)*, p. 524–525, ACM, 2021.

[12] P. K. B. Rangaiah, J. Engstrand, T. Johansson, M. D. Perez, and R. Augustine, "92 Mb/s fat-intrabody communication (fat-IBC) with low-cost WLAN hardware," *IEEE Transactions on Biomedical Engineering*, vol. 71, no. 1, pp. 89–96, 2024.

[13] S. Hylamia, W. Yan, A. Teixeira, N. B. Asan, M. Perez, R. Augustine, and T. Voigt, "Privacy-preserving continuous tumour relapse monitoring using in-body radio signals," in *2020 IEEE Security and Privacy Workshops*, 2020.

[14] L. Joseph, N. B. Asan, J. Ebrahimizadeh, A. S. Chezhian, M. D. Perez, T. Voigt, and R. Augustine, "Non-invasive transmission based tumor detection using anthropomorphic breast phantom at 2.45 GHz," in *2020 14th European Conference on Antennas and Propagation (EuCAP)*, pp. 1–5, IEEE, 2020.

[15] J. Engstrand, M. Padmal, B. Mandal, P. Rangaiah, M. D. Perez, M. Mani, R. Augustine, and T. Voigt, "Design options for aggregators for in-body networks," in *International Conference on Body Area Networks*, 2024.

[16] A. Ben Amar, A. B. Kouki, and H. Cao, "Power approaches for implantable medical devices," *Sensors*, vol. 15, no. 11, 2015.

[17] A. Arghavani, A. Ahlén, A. Teixeira, and S. Dey, "A game-theoretic approach to covert communications in the presence of multiple colluding wardens," in *2021 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–7, 2021.

[18] E. Marin, *Security and Privacy of Implantable Medical Devices*. PhD thesis, KU Leuven, 2018.

[19] H. Song, S. Zhu, and G. Cao, "Attack-resilient time synchronization for wireless sensor networks," in *Proceedings of the 2005 IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS 2005)*, IEEE, 2005.

[20] Z. He and T. Voigt, "Droplet: A new denial-of-service attack on low power wireless sensor networks," in *Proc. of the 2013 IEEE 10th International Conference on Mobile Ad-Hoc and Sensor Systems (MASS 2013)*, pp. 542–550, IEEE, 2013.

[21] 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. of the 2008 IEEE Symposium on Security and Privacy (S&P 2008)*, pp. 129–142, IEEE, 2008.

[22] K.-F. Krentz, *A denial-of-sleep-resilient medium access control layer for IEEE 802.15.4 networks*. PhD thesis, Potsdam University, 2019.

[23] Q. Ren and Q. Liang, "Secure media access control (mac) in wireless sensor networks: intrusion detections and countermeasures," in *Proc. of the 2004 IEEE 15th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2004)*, pp. 3025–3029 Vol.4, IEEE, 2004.

[24] D. Karaoğlan and A. Levi, "A survey on the development of security mechanisms for body area networks," *The Computer Journal*, vol. 57, no. 10, pp. 1484–1512, 2014.

[25] R. M. Seepers, W. Wang, G. de Haan, I. Sourdis, and C. Strydis, "Attacks on heartbeat-based security using remote photoplethysmography," *IEEE Journal of Biomedical and Health Informatics*, vol. 22, no. 3, pp. 714–721, 2018.

[26] S. Hylamia, W. Yan, Ch. Rohner, and T. Voigt, "Tiek: Two-tier authentication and key distribution for wearable devices," in *Proceedings of the 2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pp. 1–6, IEEE, 2019.

[27] V. N. Sathi, C. Rohner, and T. Voigt, "A PUF-based indirect authentication and key establishment protocol for wearable devices," in *Proc. of the IEEE International Conference on Communications (ICC 2023)*, pp. 615–621, IEEE, 2023.

[28] K.-F. Krentz and T. Voigt, "More lightweight, yet stronger: Revisiting OSCORE's replay protection," in *Proc. of the NDSS Workshop on Security and Privacy in Standardized IoT (SDIoTSec)*, Internet Society, 2024.

[29] W. Yan, T. Voigt, and C. Rohner, "RRF: A robust radiometric fingerprint system that embraces wireless channel diversity," in *Proceedings of WiSec*, 2022.

[30] W. Yan, G. Mikolai, T. Voigt, and C. Rohner, "Concise paper: Towards on-board radiometric fingerprinting fully integrated on an embedded system," in *EWSN*, 2024.

[31] K.-F. Krentz, A. Kangas, and T. Voigt, "Multi-armed bandit-based channel hopping: Implementation on embedded devices," in *Proceedings of the 4th International Conference on Machine Learning for Networking (MLN'2021)*, pp. 29–47, Springer, 2021.

[32] A. Arghavani, A. Ahlén, A. Teixeira, and S. Dey, "A game-theoretic approach to covert communications in the presence of multiple colluding wardens," in *2021 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–7, IEEE, 2021.

[33] F. Xu, Z. Qin, C. C. Tan, B. Wang, and Q. Li, "IMDGuard: Securing implantable medical devices with the external wearable guardian," in *Proceedings of IEEE INFOCOM*, pp. 1862–1870, IEEE, 2011.

[34] M. R. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. A. Grieco, G. Boggia, and M. Dohler, "Standardized protocol stack for the Internet of (Important) Things," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 3, pp. 1389–1406, 2013.

[35] W. Yang, Q. Wang, Y. Qi, and S. Sun, "Time synchronization attacks in IEEE 802.15.4e networks," in *Proceedings of the International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI 2014)*, pp. 166–169, IEEE, 2014.

[36] N. López, C. Azurdia-Meza, C. Valencia, and S. Montejo-Sánchez, "On the performance of 6LoWPAN using TSCH/Orchestra mode against a jamming attack," in *Proceedings of the 2019 IEEE Chilean Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON)*, pp. 1–5, IEEE, 2019.

[37] K. Sun, P. Ning, and C. Wang, "TinySeRSync: secure and resilient time synchronization in wireless sensor networks," in *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06)*, pp. 264–277, ACM, 2006.

[38] J. W. Hui and D. E. Culler, "IP is dead, long live IP for wireless sensor networks," in *Proceedings of the 6th ACM Conference on Embedded Network Sensor Systems (SenSys '08)*, p. 15–28, ACM, 2008.

[39] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks." RFC 4944, 2007.

[40] R. Hummen, J. Hiller, H. Wirtz, M. Henze, H. Shafagh, and K. Wehrle, "6LoWPAN fragmentation attacks and mitigation mechanisms," in *Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '13)*, pp. 55–66, ACM, 2013.

[41] M. Hossain, Y. Karim, and R. Hasan, "SecuPAN: A security scheme to mitigate fragmentation-based network attacks in 6LoWPAN," in *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy (CODASPY '18)*, pp. 307–318, ACM, 2018.
[42] P. Ginzboorg, V. Niemi, and J. Ott, "Authentication of fragments with short tags," *Theoretical Computer Science*, p. 114643, 2024.
[43] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J.-P. Vasseur, and R. Alexander, "RPL: IPv6 routing protocol for low-power and lossy networks." RFC 6550, 2012.
[44] A. Mayzaud, R. Badonnel, and I. Chrisment, "A taxonomy of attacks in RPL-based Internet of things," *International Journal of Network Security*, vol. 18, no. 3, pp. 459–473, 2016.
[45] K.-F. Krentz and T. Voigt, "Secure opportunistic routing in 2-hop IEEE 802.15.4 networks with SMOR," *Computer Communications*, vol. 217, pp. 57–69, 2024.
[46] J. Deng, R. Han, and S. Mishra, "INSENS: Intrusion-tolerant routing for wireless sensor networks," *Computer Communications*, vol. 29, no. 2, pp. 216 – 230, 2006.
[47] C. Dombrowski and J. Gross, "Echoring: A low-latency, reliable token-passing mac protocol for wireless industrial networks," in *Proceedings of the 21st European Wireless Conference*, pp. 1–8, VDE, 2015.
[48] Z. Shelby, K. Hartke, and C. Bormann, "The Constrained Application Protocol (CoAP)." RFC 7252, 2014.
[49] K. Seo and S. Kent, "Security Architecture for the Internet Protocol." RFC 4301, 2005.
[50] E. Rescorla, H. Tschofenig, and N. Modadugu, "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3." RFC 9147, 2022.
[51] G. Selander, J. P. Mattsson, F. Palombini, and L. Seitz, "Object Security for Constrained RESTful Environments (OSCORE)." RFC 8613, 2019.
[52] K. Seitz, S. Serth, K.-F. Krentz, and Ch. Meinel, "Demo: Enabling en-route filtering for end-to-end encrypted CoAP messages," in *Proc. of SenSys '17*, ACM, 2017.
[53] F. Seidel, K.-F. Krentz, and Ch. Meinel, "Deep en-route filtering of constrained application protocol (CoAP) messages on 6LoWPAN border routers," in *Proc. of WF-IoT 2019*, pp. 201–206, IEEE, 2019.
[54] S. Hristozov, M. Huber, and G. Sigl, "Protecting RESTful IoT devices from battery exhaustion DoS attacks," in *Proc. of HOST 2020*, pp. 316–327, IEEE, 2020.
[55] K.-F. Krentz and T. Voigt, "Reducing trust assumptions with OSCORE, RISC-V, and Layer 2 one-time passwords," in *Proc. of the 15th International Symposium on Foundations and Practice of Security (FPS 2023)*, p. 389–405, Springer, 2023.
[56] T. Voigt, W. Yan, L. Joseph, S. Hylamia, N. B. Asan, M. Mani, B. Mandal, M. Perez, and R. Augustine, "Jamming to support privacy-preserving continuous tumour relapse monitoring using in-body radio signals," in *Proceedings of the 1st International Workshop on Physical-Layer Augmented Security for Sensor Systems*, PLAS '20, (New York, NY, USA), pp. 1–2, Association for Computing Machinery, Nov. 2020.
[57] T. Voigt, C. Rohner, W. Yan, L. Joseph, S. Hylamia, N. B. Asan, B. Mandal, M. Perez, and R. Augustine, "Towards secure backscatter-based in-body sensor networks," in *Proceedings of the 18th Conference on Embedded Networked Sensor Systems*, pp. 741–742, 2020.
[58] T. Shaw, B. Mandal, D. Mitra, P. K. Rangaiah, M. D. Perez, and R. Augustine, "Wireless power transfer system design using zero-index metamaterial for implantable medical devices," in *2023 17th European Conference on Antennas and Propagation (EuCAP)*, pp. 1–5, IEEE, 2023.
[59] L. Mottola, A. Hameed, and T. Voigt, "Energy attacks in the battery-less internet of things: Directions for the future," in *Proceedings of the 17th European Workshop on Systems Security*, pp. 29–36, 2024.
[60] J. de Winkel, C. Delle Donne, K. S. Yildirim, P. Pawełczak, and J. Hester, "Reliable timekeeping for intermittent computing," in *Proceedings of the Twenty-Fifth International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS '20)*, p. 53–67, ACM, 2020.