Secure In-body Communication and Sensing

SAM HYLAMIA
Secure In-body Communication and Sensing

Sam Hylamia
sam.hylamia@it.uu.se

September, 2022

Division of Computer Systems
Department of Information Technology
Uppsala University
Box 337
SE-751 05 Uppsala
Sweden

http://www.it.uu.se/

Dissertation for the degree of Licentiate of Philosophy in Computer Science

© Sam Hylamia 2022
ISSN 1404-5117
Printed by the Department of Information Technology, Uppsala University, Sweden
Abstract

Implantable medical devices (IMDs) such as cardiac implants and insulin pumps provide patients with lifesaving functions and improve their lives. These properties make them an integral part of medical professionals’ toolbox. Today, IMDs which can be controlled or adjusted wirelessly are widely adopted and are becoming increasingly connected to each other and to the internet. While the modern communication properties of IMDs provide substantial benefits, they pose a major cybersecurity risk when devices are not secured adequately.

In this thesis, we explore security issues related to the communication and sensing capabilities of modern on-body devices such as IMDs. In particular, we investigate authentication and key agreement in a network of body-worn devices, and address the privacy of in-body continuous sensing and monitoring.

The main contributions of this thesis are twofold: (1) We propose and evaluate Tiek, an authentication and key distribution protocol for networked body-worn devices. Tiek authenticates the presence of participating devices on the body and distributes cryptographic keys to them using environment based sources of randomness. The protocol utilizes a two-tier authorization scheme to restrict the access of mal-behaving body-worn participants to the network. (2) We also study the information leakage associated with the deployment of a novel in-body continuous monitoring technique. We target the information leakage from the sensing process, and propose and evaluate privacy enhancing measures that prevent a passive eavesdropper from violating the privacy of the patient. We believe this thesis contributes to the development of secure in- and on-body networks of medial devices.
Acknowledgments

I would like to acknowledge the effort, engagement and patience of my main advisor Thiemo Voigt and co-advisor Christian Rohner who both supported and guided me in my academic process since my Bachelor’s thesis work all the way to the completion of this thesis.

I would also like to thank all present and former members of the UNO, CoRe, and MMG groups at Uppsala University, the NES group at RISE, and the LifeSec project members for their support and valuable feedback. And especially to my colleague Wenqing Yan for her contributions to my published work.

Many thanks to The Swedish Foundation for Strategic Research (SSF) for funding the LifeSec project.

Finally, I would like to express my gratitude for my friends and family who supported and encouraged me through this process.
Included papers

This thesis is based on the following papers:


Reprints were made with permission from the publishers.
List of work not included in this thesis


II Papers

Paper I - Tiek: Two-tier Authentication and Key Distribution for Wearable Devices

Paper II - Privacy-preserving Continuous Tumour Relapse Monitoring Using In-body Radio Signals
Part I

Thesis
Chapter 1

Introduction

1.1 Implantable Medical Devices

IMDs are devices permanently or semi-permanently implanted within the body to perform a medical function, such as treatment and monitoring of medical conditions [1]. Examples of these devices are neurostimulators, pacemakers, heart defibrillators, insulin pumps, glucose monitors, and drug delivery systems. Today, millions of people rely on these devices to perform critical life-support functions. This number is expected to grow rapidly as the human population continues to age and new medical applications of IMDs continue to emerge.

An increasing number of IMDs are being developed with advanced communication and computation capabilities. This enables medical professionals to more easily monitor the condition of the patient and reconfigure the device. Moreover, these new capabilities could allow multiple devices implanted in the same body to communicate, share measurements and coordinate actions. This further enables medical professionals to develop new diagnostic and monitoring techniques that utilize a network of IMDs [2].

1.2 Body Coupled Communication

Traditional communication techniques that use over-the-air microwave signals face challenges when communicating between IMDs since the skin and muscle tissue absorb these signals. A novel approach, called body coupled communication (BCC) tackles this challenge by using the human body as propagation medium. There are different ways to achieve BCC. Examples are galvanic coupling [3], capacitive coupling [4], and ultrasonic waves [5]. However, these techniques are only able to provide communication at a low data-rate [6].
A novel BCC technique pioneered at Uppsala University uses the body fat tissue as a propagation medium for in-body microwave signals [7, 8]. Body fat tissue has low water concentration (5-10%) compared to muscle (73-78%) and skin (60-76%) tissue. The low water content of fat tissue gives it a low dielectric constant and makes it a good medium for in-body microwave communication. A significant advantage of using this technique over other BCC technique is its ability to support high data-rates [6] which are useful for data intensive applications such as brain-machine interfaces [9, 10]. Moreover, this novel communication technique could also be utilized to monitor changes in the properties of the communication channel. Such changes could help with early detection of diseases such as lymphedema or tumour relapse [11].

1.3 Security of Implantable Medical Devices

IMDs perform critical life-support functionality and store and communicate private patient information. This makes security and privacy a primary concern for many people when using IMDs. While the increase in complexity and functionality of these devices enables more sophisticated use-cases, it poses a major security risk, especially with the addition of wireless communication technology [2]. Consequently, several attacks on IMDs have been demonstrated in lab environments [12, 13, 14, 15] where the researchers were able to uncover vulnerabilities that enable attackers to take full control of the attacked IMD. Attackers utilizing such vulnerabilities in the real-world could cause numerous adverse events that range from discomfort to heart failure depending on the attacked device and attacked functionality.

IMDs share many of their security challenges with Wireless Sensor Network (WSN) devices [16]. However, they add stricter space, energy and access constraints. Moreover, they introduce some unique security challenges such as emergency access for medical personnel [17]. The environment of IMDs also provides them with unique opportunities that help address some of the new challenges, such as confined communication channels [18] and access to sources of entropy localized to the body [19, 20, 21]. In this thesis, we utilize these new opportunities to address challenges related to cryptographic key agreement and the privacy of in-body sensing.
Chapter 2

Research Questions and Contributions

In this chapter, we provide background on our main contributions, motivate and state our research questions, and discuss how we answer these questions. We divide this chapter into two sections: In the first section, we focus on Tiek; our contribution to environment-based authentication and key agreement. In the second section, we discuss our contribution to privacy preserving in-body sensing.

2.1 Environment-based Security

We define environment-based security as the utilization of external sources of randomness present in the environment of a device to generate random numbers. These random numbers are the fundamental building block of environment-based key generation, key distribution, and authentication. Schemes based on randomness obtained from the environment are developed for small devices with limited computation, power consumption, and connectivity constraints. They provide an alternative to traditional methods that rely on computational hardness and the availability of infrastructure, such as Public Key Infrastructure (PKI).

Environment-based schemes typically rely on a physical time-varying random process available to legitimate participating devices. An eligible random process produces correlated results when measured independently by different devices at the same time. Participating devices simultaneously measure a random process to obtain correlated random values. Then, they use these values to authenticate each other [19], derive keys [22], or exchange them [21]. Examples of such processes are wireless channel fading [23], body movement patterns [21], and the heart inter-pulse interval (IPI) [19].
Chapter 2. Research Questions and Contributions

2.1.1 Research Question

Existing environment-based authentication and key agreement/distribution techniques for wearable devices and IMDs assume that all devices participating in the scheme are benign and untampered with [21, 22]. However, numerous studies have uncovered security vulnerabilities in this class of devices [24, 25]. Such vulnerabilities could compromise a legitimate participating device enabling an adversary to gain substantial knowledge of the secrets of the compromised device; hence, jeopardizing the security of such systems. Therefore, we ask the question: Can we design an environment-based authentication and key distribution scheme that mitigates the threat a mal-behaving body-worn device or IMD poses to the secrecy of the distributed keys?

2.1.2 Tiek

To address the above research question, we design and evaluate Tiek, a two-tier authentication and key distribution technique. Tiek assumes a star-topology network where a relatively more powerful device, a hub, exists at the centre of the network. The hub facilitates communication between peripheral devices and orchestrates the authentication and key distribution technique. The scheme utilizes two sources of environment-based randomness to authenticate body-worn devices and distribute a unique symmetric cryptography key to each authenticated device.

We refer to the first source of randomness as a common source. A common source of randomness provides the same random values to body-worn devices when measured simultaneously, such as heart IPI, and body movement patterns. We use this source to authenticate the presence of devices on the body; therefore, a suitable common source of randomness is one that can only be measured by legitimate body-worn devices. We utilize this common source of randomness to distribute a group key portion to all participating body-worn devices and refer to this group portion as \( g \). We refer to the other source of randomness as a pairwise source. A pairwise source of randomness is available to a pair of collaborating devices. When measured independently and simultaneously by Alice, Bob and Eve, a pairwise source provides different values to Alice and Bob than Alice and Eve or Bob and Eve. An example of this source is wireless channel fading. We utilize this source to distribute a unique key portion between the hub and each participating device. We refer to these unique portions as \( \{u_i\} \) where \( i \in [1, N] \) and \( N \) is the number of participating peripheral devices.

Tiek distributes the cryptographic key portions \( g \) and \( \{u_i\} \) using a cryptographic construct known as a multi-secret fuzzy vault [26, 27]. As opposed
to point to point key reconciliation techniques [28], the multi-secret fuzzy vault enables us to distribute the cryptographic key portions to all devices simultaneously without leaking any information. We encode $g$ in the vault using the random values obtained from the common source of randomness and encode each $u_i$ using the random values obtained from the pairwise source between the hub and each participating device. The vault is then published to all participating devices.

Upon receiving the vault, each device decodes $g$ using the random values it obtained from the common source. $g$ is only available to participating devices that can measure the common source accurately enough; therefore, devices that can decode $g$ correctly are considered authenticated (proving their presence on the body). Then, each device decodes its unique key portion $u_i$ using the random values obtained from the pairwise source. Finally, each device combines $g$ with its $u_i$ resulting in the master key $K_i$. Figure 2.1 illustrates this key distribution technique.

The master keys $\{K_i\}$ Tiek generates are composed of both the group key portion $g$ and unique key portion $\{u_i\}$; thus provides two levels of authorization in the network. The first level is granted by the group portion $g$ and constitutes the ability to participate in the network. Therefore, any body-worn device, including mal-behaving ones, can communicate with the hub and appear as an authentic device. The second level is where Tiek mitigates the risk mal-behaving body-worn devices pose to the network. Since every key $K_i$ is constructed with a unique portion $u_i$, only devices that share this portion are authorized to communicate with each other. Hence, a mal-behaving body-worn device would not be able to impersonate the hub and communicate directly with another body-worn peripheral device. In
conclusion, Tiek utilizes the security of the full master keys \( \{K_i\} \) against off-body adversaries. Simultaneously, it utilizes the significant but potentially reduced security of \( \{u_i\} \) against body-worn devices courtesy of their knowledge of the group portion. Additionally, since Tiek employs two independent sources of randomness it can alleviate the potential damage in situations where one of the sources is compromised.

### 2.2 In-body Sensing

As we describe in Section 1.2, the body fat tissue can be used as a propagation medium for in-body communication [7]. A side-effect of this communication technique is the ability to detect changes in the properties of the communication channel. Such changes can be monitored and utilized for early detection of disease such as tumour relapse [11]. This monitoring technique operates by placing small probes around the monitoring area where they launch microwave signals between each other and observing changes in received signal strength (RSS) over a long period. In Figure 2.2, we simulate this monitoring technique by placing probes on the sides of a 100 mm wide model of three tissue layers. The layers are 2, 25, and 30 mm of skin, fat and muscle respectively. In the figure, we observe the changes in RSS as a perturbant grows in the middle of the fat layer from 0 to 10 mm in radius. The RSS drops as the perturbant grows. This change in propagation properties can be used to trigger a medical checkup which could result in early detection of a tumour relapse.

![Figure 2.2: A perturbant grows in a model of skin, fat, and muscle. We measure the RSS drop across the propagation channel as the perturbant grows. The RSS decreases over the growth period of the perturbant which reveals its presence in the channel.](image)
2.2. In-body Sensing

2.2.1 Research Question

Radio transmissions used in fat BCC radiate outside the body as skin does not absorb or reflect the signals completely [8]. Hence, there is a risk that an eavesdropper could exploit these leaked signals to infer the growth of a perturbant in the channel and, thereby, violate patient privacy and reveal information about their health status. This introduces a novel challenge where not only the sensing result must be kept private but also the sensing process itself. Therefore, we ask the question: Can we devise a strategy that would allow the use of such sensing technique without leaking sensitive patient information to potential eavesdroppers?

2.2.2 Privacy Preserving In-body Sensing

To address the research question we study the information leakage of this monitoring technique from the perspective of a powerful eavesdropper and propose and evaluate a set of privacy-enhancing techniques.

We model our evaluation setup similarly to the model we describe in Section 2.2. We model the adversary in that model as two passive eavesdroppers on opposite sides of the perturbant. These eavesdroppers can measure the RSS of the messages between the two sensing probes but cannot read or alter the content of the messages exchanges between them. Moreover, they cannot exchange messages or introduce signals of their own. Additionally, the two eavesdroppers cannot cooperate. We choose this rather powerful adversary model to analyse the privacy of the system from the perspective of a worst-case scenario and to simplify our simulations.

We experiment with various ways of enhancing the privacy of the measurements collected by our model. We start with simply varying the output power of the transmitter randomly. This technique quickly proves ineffective as the mean of the RSS measurements collected by the eavesdropper drop as the perturbant grows. We augment this technique by adaptively increasing the minimum output power of the transmitter as the perturbant grows to counteract the drop in mean RSS. This fails since the adversary on the side of the transmitter now sees this increase in minimum output power. Given this observation, we augment our privacy-enhancing technique further by having both our probes alternate randomly between sending and receiving signals. This addition utilizes sender anonymity as given these conditions, each eavesdropper cannot individually distinguish the source of the signals with high accuracy. Our new combination succeeds in removing the correlation between the perturbant radius and the mean RSS. However, we observe that the distribution of RSS measurements at the eavesdroppers change overtime as we increase the minimum output power. This change
can reveal the growth of the perturbant to the eavesdroppers. Finally, we introduce channel hopping to our privacy-enhancing technique where the transmitter changes transmission channel with every sent message. Given that the eavesdroppers cannot monitor all possible transmission channels at the same time, this enables us to limit number of overall measurements that the eavesdroppers can perceive. Thus, we limit the ability of the eavesdroppers to collect sufficient measurement to perform any meaningful statistics.

In conclusion, adaptive and random variation of output power, in addition to sender anonymity and channel hopping enables the monitoring system to prevent a worst-case scenario passive eavesdropper from detecting the growth of perturbant in the monitoring area. Hence, this technique enables similar sensing applications to perform their functions while preserving the privacy of patients.
Chapter 3

Related Work

The proliferation of IMDs have motivated researchers to study the security of these devices and propose novel ways to protect them against attackers. Some demonstrated vulnerabilities in commercially available devices such as glucose monitors and insulin pumps [13, 29], and pace makers and implantable cardiac defibrillators [12]. In all these instances, attackers were able to take full control of the IMD. They were able to reveal sensitive medical information and actuate the device in a manner that would harm a patient wearing such a device. Others proposed novel ways to secure these device. Examples include defensive jamming against anomalous [30] or unauthenticated [31, 32] device access. In these examples, an external device (worn or carried by the patient) protects the IMD from attackers. Other examples include authentication techniques that rely on signals only available to on-body or body adjacent devices [19, 33, 34]. We divide the rest of this chapter into two sections; each section discusses the research work related to one of our main contributions.

3.1 Environment-based Security

Several studies have utilized randomness harvested from the environment of communicating devices to establish secure communication with nearby devices. Some utilize randomness from the human body, such as IPI [19, 35], hand resonance [20] and gait [21]. While others utilize randomness from their physical communication layer, such as channel fading [22] and channel anonymity [36]. Two contributions similar to our work in this area are:

1. Revadigar et al. [21] generate and distribute cryptographic keys to body-worn devices using gait as a source of randomness. In their scheme, the hub device measures the gait using an on-board accelerometer and generates a random bit-string (group key). Then, all participating devices, including
the hub, measure the gait together using their on-board accelerometers. Finally, the hub distributes the bit-string, generated in the first step, using the obtained measurements in a fuzzy vault scheme.

2. Shi et al. [22] authenticate body-worn devices and generate unique cryptography keys between each participating device and a hub device using received signal strength (RSS) measurements. Their scheme leverages the significant difference in RSS fluctuations between two body-worn devices and between a body-worn device and an off-body device. They use this difference to prove the presence of a device on the body. Then, devices, whose presence on the body has been authenticated, collaborate to establish a unique key between each one of them and the hub.

Both of the aforementioned studies assume that body-worn devices are behaving in accordance with the scheme and pose no threat to it. We differentiate our work in this area by removing this assumption and designing an authentication and key distribution scheme that mitigates the potential of a malicious body-worn device.

### 3.2 In-body Sensing Privacy

There are plenty of studies on the security and privacy of medical data. Examples of these studies include, lightweight security schemes for the preservation of sensed data [37], as well as data aggregation [38], integration [39] and big data analytics [40] of medical data. Additionally, many studies cover rules and policies to protect and handle sensitive patient data [41], in particular, the security of medical health records [42, 43].

The aforementioned schemes and studies address the privacy and security of medical data post its acquisition from sensors. Our work in this area takes a different focus; we aim to avoid information leakage from the sensing process in applications that utilize wireless communication technologies for sensing [44]. Unlike the aforementioned work, which addresses the complementary issue of handling the sensed data in a privacy-preserving manner.

Aside from the medical field, researchers have devised techniques to enhance the privacy of sensing applications, such as, location-based services that do not leak the user’s exact location [45, 46] and smart-home applications that do not leak the user’s behavior patterns [47]. These techniques, together with our work on in-body sensing privacy, aim to enable applications and services while preserving the user’s privacy.
Chapter 4

Summary of Papers

4.1 Paper I: Tiek: Two-tier Authentication and Key Distribution for Wearable Devices

Summary: Tiek is an environment-based authentication and key distribution technique for Intra-Body Area Network (IBAN) devices. It utilizes two different environment-based randomness sources to authenticate devices into a star-topology network, and distribute unique cryptographic keys to each of them. The scheme uses two sources of randomness: one common source; shared between all devices on the body, such as gait, and another pairwise source; unique to the hub and each other participating device, such as radio channel fading. Tiek uses the common source to establish the presence of the participating device on the body (authentication) and the pairwise source to provide uniqueness to each distributed cryptographic key. Tiek differentiates from previous work on environment-based authentication and key distribution techniques by protecting IBAN devices from each other.

Contribution: Tiek is the first environment-based authentication and key distribution for IBAN devices designed to mitigate the threat of a mal-behaving IBAN device. It is also the first protocol that uses two sources of randomness to authenticate and distribute cryptographic keys to IBAN devices.

My Contribution: I have designed and evaluated the Tiek protocol. I am the main author of the paper and wrote all parts of the paper in collaboration with my co-authors. I presented the paper at the 2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob).
4.2 Paper II: Privacy-preserving Continuous Tumour Relapse Monitoring Using In-body Radio Signals

Summary: Earlier work has concluded that fat in-body communication (IBC) can be used as a sensing technique to detect changes to the fat channel. Such sensing technique could be utilized as an early warning system against disease, such as tumour relapse. The hypothesized system works by inserting two fat IBC devices at opposite sides relative to the monitoring area: One device sends periodic radio signals through the fat channel and the other measures the change in RSS over time. A decrease in average received RSS over time indicates a decrease in channel quality and, thus, a warning against a potential tumour relapse in the targeted area. This sensing technique creates a challenge from a privacy perspective since these sensing signals leak outside the body; an eavesdropper could capture these signals and learn about the health condition of the person wearing this system. In this work, we investigate this leakage and propose and evaluate different privacy-enhancing techniques. Finally, we devise a combination of these techniques that preserves the privacy of the patient.

Contribution: We hypothesize a powerful eavesdropper and use it to study the information leaked from this sensing system. We evaluate through simulation a set of privacy-enhancing techniques and conclude that trivial solutions are ineffective at reducing information leakage from our hypothesized eavesdropper. Finally, we present a combination of the evaluated techniques that preserves the privacy of the patient.

My Contribution: I have developed the adversary and simulation models, proposed the use of the privacy-enhancing techniques and the evaluation methodology, conducted the simulations and recorded the results. I am the main author of the paper and wrote most parts of the paper in collaboration with my co-authors. I presented the paper at the 2020 IEEE Workshop on the Internet of Safe Things (SafeThings@S&P).
Chapter 5

Conclusions and Future Work

In this thesis, we explore challenges related to the security and privacy of in-body communication and sensing techniques.

In our first paper, Tiek, we present an environment-based authentication and key distribution scheme that mitigates the harm of a mal-behaving body-worn device. Our technique leverages two separate types of environment-based sources of randomness to authenticate the presence of devices on the body and distribute a unique cryptographic key to each device. Our proposed scheme assumes a star topology where all peripheral devices can reach the hub device. A future extension of our work could extend this approach to cover multi-hop networks where devices can only reach the hub through an intermediate relay. This would enable BCC applications where the distance between or the location of in-body devices prohibits the formation of star topology networks. Additionally, future work could implement Tiek on resource constrained devices, and evaluate its system requirements. This evaluation could also be extended to evaluate the requirements and constraints imposed by combining different sources of randomness in the key extraction phase of the protocol.

In our second paper, we address information leakage from a novel in-body microwave radio based sensing technique. We propose a set of privacy-enhancing techniques and evaluate them in simulation. We show that these techniques cannot provide adequate protection individually. However, when combined together they can protect against a worst case scenario passive adversary. We evaluated our work in simulation against a worst case scenario passive adversary. A future extension of this work could reevaluate the current setup experimentally using phantom models or real tissue. This would help affirm or update our findings. Moreover, future work could
study the information leakage problem from the prospective of a more realistic adversary, then update the mitigation strategies and evaluate them experimentally. Additionally, future work could explore the use of friendly jamming to reduce information leakage from the sensing channel.

Extending to the field in general, future work could specify an upper level communication protocol (e.g. ZigBee, 6LoWPAN, etc) with built-in security features designed to fit the needs of body-worn devices. Moreover, future work could devise an intrusion detection system that is able to detect internal attackers to mitigate the risk of malbehaving devices within the network.
Bibliography


[22] Lu Shi, Jiawei Yuan, Shucheng Yu, and Ming Li. Mask-ban: Movement-aided authenticated secret key extraction utilizing channel characteristics in body area networks. *IEEE Internet of Things Journal*, 2(1), 2015.


[35] Qi Lin, Weitao Xu, Jun Liu, Abdelwahed Khamis, Wen Hu, Mahbub Hassan, and Aruna Seneviratne. H2b: heartbeat-based secret key gen-


Part II

Papers
Paper I
Paper I
Tiek: Two-tier Authentication and Key Distribution for Wearable Devices
Tiek: Two-tier Authentication and Key Distribution for Wearable Devices

Sam Hylamia\textsuperscript{1}, Wenqing Yan\textsuperscript{1}, Christian Roher\textsuperscript{1}, Thiemo Voigt\textsuperscript{1,2}
\textsuperscript{1}Uppsala University, Uppsala, Sweden
\textsuperscript{2}RISE, Stockholm, Sweden

Abstract

Wearable devices, such as implantable medical devices and smart wearables, are becoming increasingly popular with applications that vary from casual activity monitoring to critical medical uses. Unsurprisingly, numerous security vulnerabilities have been found in this class of devices. Yet, research on physical measurement-based authentication and key distribution assumes that body-worn devices are benign and uncompromised. Tiek is a novel authentication and key distribution protocol which addresses this issue. We utilize two sources of randomness to perform device authentication and key distribution simultaneously but through separate means. This creates a two-tier authorization scheme that enables devices to join the network while protecting them from each other. We describe Tiek and analyze its security.

1 Introduction

Wearable devices span various application areas from health care to information delivery and fitness tracking. Smart wearables often measure, communicate and store sensitive and personal information, such as user identification, physiological signals, location data, etc. Some even provide life-saving and critical functions, like cardiac defibrillators and insulin pumps. Hence, securing these devices is imperative [1].

Authentication and key distribution/agreement are fundamental challenges in communication security. The unique environment available to wearable devices enables a novel technique that addresses these challenges, namely physical and physiological measurement-based authentication and key agreement [2–6]. Systems employing this technique provide an alternative to traditional methods that rely on computational hardness and available infrastructure, such as Public Key Infrastructure (PKI). This paper leverages this technique and presents a novel authentication and key distribution protocol.
Figure 1: A smartphone and four other smart devices use Tiek to establish secure communication. Each device obtains the group portion $g$ and its unique portion $u_i$ and fuses them to create the final key $K_i$.

named Tiek. We enhance state-of-the-art systems by fortifying distributed keys against mal-behaving body-worn devices.

Physical and physiological measurement-based authentication and key agreement techniques utilize their environment to generate cryptographic keys and authenticate devices without any prior knowledge. These techniques typically rely on a physical time-varying random process available to legitimate participating devices. An eligible random process produces correlated results when measured independently by different devices at the same time. Examples of such processes are the inter-pulse interval (IPI) of a heart [2], body movement patterns [5] and wireless channel fading [6]. Participating devices obtain correlated random strings by simultaneously measuring one of these processes. They, then, use these strings to authenticate each other [2] or derive keys [5]. We refer to these random processes as sources of randomness and divide them into two categories:

1. Common sources, such as IPI and body movement patterns, are physiological features that can be measured accurately enough anywhere on the body. When measured independently and at the same time, these sources provide correlated values to all devices sharing the body.
2. **Pairwise sources**, such as wireless channel fading, are only available to a pair of collaborating devices. When measured independently and simultaneously by Alice, Bob and Eve, a pairwise source provides different values to Alice and Bob than Alice and Eve or Bob and Eve.

To the extent of our knowledge, all systems that employ the aforementioned technique assume that participating body-worn devices are benign and untampered with [5, 6]. However, studies have uncovered numerous security vulnerabilities in wearable devices [7, 8]. Such vulnerabilities could compromise a body-worn device enabling an adversary to gain substantial knowledge of the secrets of the compromised device; therefore, jeopardizing the security of such systems. We challenge this commonly accepted assumption and consider the situations where a body-worn device exhibits malicious behaviour enabled, for example, by an exploited vulnerability.

**The Tiek protocol.** On a high level, Tiek is a multilevel authentication and key distribution protocol for wearable devices. In essence, our protocol utilizes a common source of randomness and a pairwise source to distribute a unique key to every device in the network. We generate all keys at a relatively powerful hub device and use the sources of randomness to distribute them securely.

Each key consists of two parts that we fuse together into the final key. The first part of the key is distributed through the common source and is known to all devices sharing the body. For example, all devices in Figure 1 measure the body’s motion pattern (gait) and, through that, decode the same bit-string $g$. We call $g$ the *group portion* and use it to grant (authorize) devices access to the network. In other words, devices authenticate their presence on the body by demonstrating their knowledge of the group portion to the hub. The second part is called the *unique portion* and is distributed through the pairwise source. This portion is shared between every individual device and the hub. In our previous example, all devices in Figure 1 measure the channel fading between themselves and the smartphone and use their measurements to decode the unique portion $u_i$. We use the unique portion to tie the final key to a specific device. For the *final key*, we fuse the group portion and the unique one to obtain a cryptographic key unique to every device in the network. All final keys are known to the hub where they are used to establish an authenticated and encrypted channel with every device. The final key is denoted $K_i$ in Figure 1 where $f$ is the fuse portions function.

Our method leverages this two-part key to establish two levels of authorization in the network. The first level is granted by the group portion and constitutes the ability to participate in the network. Therefore, any body-worn device, including mal-behaving ones, can communicate with the hub and appear as authentic devices. For example, all devices in Figure 1 know the group portion $g$ and are, therefore, allowed to communicate with
the smartphone. However, this, unfortunately, implies that if an off-body adversary learns $g$ through a vulnerability in one of the devices, it will be able to communicate with the smartphone. The second level is where Tiek mitigates the risk mal-behaving body-worn devices pose to the network. Since every key is constructed with a unique portion, only devices that share this portion are authorized to communicate with each other. Hence, in our previous example, only the smartphone is allowed to communicate with the implantable medical device since only those two know $u_2$.

As a result of this scheme, Tiek utilizes the security of the full final key against off-body adversaries. Simultaneously, it utilizes the significant but potentially reduced security of the unique portion against body-worn devices courtesy of their knowledge of the group portion. Additionally, since Tiek employs two independent sources of randomness it can alleviate the potential damage in situations where one of the sources is compromised.

**Contributions.**

- We leverage the variety of randomness sources available to wearable devices to design the first protocol to utilize different sources of randomness for authentication and key distribution for wearable devices.

- Our protocol is also the first design to mitigate the threats a mal-behaving body-worn device poses to the secrecy of the distributed keys.

**Organization.** The rest of this paper is organized as follows: §2 provides a summary of the related work and how it compares to ours. In §3, we state our goals, assumptions and adversary model. Then, we describe Tiek in §4 and analyze its security in §5. Finally, we conclude this work in §6.

## 2 Related Work

Various studies have adopted physical and physiological measurements-based authentication and key agreement as an alternative to those based on computational hardness. In this section, we categorize existing studies based on their utilized source of randomness and compare Tiek with the state-of-art.

**Common source based schemes.** Several studies have proposed to use biometric and physiological signals to authenticate devices and agree on keys, such as IPI [2, 3], hand resonance [4] and gait [5]. Rezadigar et al. [5] utilize human motion to generate and distribute a group key between multiple wirelessly connected wearable devices. The proposed scheme uses an accelerometer to generate a random bit-string (group key) at a hub device. Then, all devices extract gait and use it to distribute the group key through a fuzzy vault scheme. This method of key distribution assumes that all body-worn devices are benign since a malicious wearable could bypass the
protection offered by this scheme. In contrast, Tiek mitigates the potential of a malicious wearable device by complementing the group key with another one unique to every device. We obtain the unique key portions from a pairwise source which enables us to protect devices from each other.

**Pairwise source based schemes.** Existing schemes using pairwise sources are concentrated around wireless channel characteristics, such as channel fading [6] and channel anonymity [9]. Shi et al. [6] use received signal strength (RSS) to authenticate wearable devices and generate a unique key between each wearable and a hub. The proposed scheme leverages the significant difference in RSS fluctuations between two body-worn devices and between a body-worn device and an off-body device. This difference is used to prove a device’s presence on the body. Then, devices whose presence on the body has been authenticated collaborate to establish a unique key between each one of them and the hub. Similar to Revadigar et al., Shi et al. do not consider malicious body-worn devices. Moreover, their method requires additional wearable devices to facilitate their authentication scheme. We differentiate from their approach by separating the means of device authentication from those of key distribution. This enables us to establish clear boundaries between body-worn devices and protect them from each other. Moreover, our method does not require additional devices to facilitate its operations.

3 System Model

3.1 Design Goals and Requirements

Our main design objective is to create an authentication and key distribution protocol that alleviates the risk of a system-wide security failure against mal-behaving body-worn devices. The protocol must be realizable using existing hardware and standardized protocols. It must also fit energy, memory and time constraints of wearable devices by minimizing the communication and computation overhead. Moreover, the system must not compromise usability by minimizing user interaction.

3.2 Assumptions

We consider a network of wirelessly connected wearable devices, such as the one shown in Figure 1. We assume that all devices can measure a common source and a pairwise source of randomness. For example, all devices can measure gait using an on-board accelerometer, and RSS using their radio. A dedicated device in the network, e.g. the smart phone, acts as a communication hub between body-worn devices and between body-worn devices and the outside world. In other words, all devices form a star topology.
network around the hub. We refer to the hub as the central control unit (CU).

3.3 Adversary Model

In this work, we identify two types of adversaries:

1. **Off-body adversaries** are the typical type of adversaries discussed in previous systems [5, 6]. We define off-body adversaries as passive and active attackers that cannot measure the utilized sources of randomness accurately. In passive attack scenarios, off-body adversaries can eavesdrop on all exchanged messages between legitimate devices. Eavesdroppers analyze these messages to learn about the distributed keys. In active attack scenarios, off-body adversaries attempt to impersonate a body-worn device. Here, adversaries can employ advanced sensing techniques to learn about the distributed keys, such as measuring IPI using cameras [10] or imitating a person’s gait [5]. The goal of an off-body adversary is to gain access to the network to eavesdrop on confidential communication or launch subsequent attacks on other devices.

2. **Body-worn adversaries** are body-worn devices that exhibit malicious behaviour caused by a vulnerability. Such an adversary can measure the common source of randomness accurately. This effectively grants the body-worn adversary access to the network. In other words, this adversary can establish an authenticated and confidential channel with the CU. The goal of a body-worn adversary is to eavesdrop on the confidential communication between the CU and other body-worn devices or attack a benign body-worn device. As mentioned in the introduction, previous systems have disregarded body-worn adversaries. Therefore, considering them in our adversary model and limiting their potential in our design are among our contributions.

We assume that the CU is benign and untampered with. This is an exception to our previous assumptions because of the central role of this device in our protocol and the network as a whole. Similar to previous work [5,6], we do not consider jamming and denial-of-service (DoS) attacks. We assume that the CU can detect jamming and DoS attacks, interrupt the key agreement procedure and alert the user.

4 The Tiek Protocol

As introduced earlier, Tiek utilizes a common source of randomness and a pairwise source to authenticate devices and distribute keys. Tiek, in essence, is a **key distribution** scheme where we generate keys independently from the utilized sources of randomness but distribute them through these sources.
The proposed method is orchestrated by the CU and follows an intentionally simple, yet effective, procedure.

As shown in Figure 1, we assume a network of a CU and $N$ wearable devices, denoted $\{n_i\}$ for $i \in [1, N]$. We refer to all devices other than the CU as nodes. In this network, Tiek generates and distributes keys following a three-step process: First, the CU generates all key portions needed to construct the final keys. Next, all devices utilize the sources of randomness to distribute each generated key portion to its target node. Finally, each node combines its key portions and obtains its final key. We detail these steps below.

4.1 Secret Key Material (SKM) Generation

Leveraging the superior resources available to the CU compared to other devices, the CU generates $N + 1$ true random and unique strings. These strings are the group portion $g$ and the $N$ unique portions $\{u_i\}$. The SKM can be obtained from a true physical random number generator on-board the CU or communicated securely from a trusted third party.

4.2 Key Distribution

Following SKM generation, the CU needs to distribute these strings to all participating nodes securely without any prior shared keys or infrastructure. Hence, Tiek utilizes a cryptographic construct known as a multi-secret fuzzy vault [11]. This scheme enables us to distribute all key portions (SKM) to all
devices simultaneously without leaking any information. We first introduce
the fuzzy vault scheme and then extend to its multi-secret variant. Fuzzy
vault is an information-theoretically secure construct proposed by Juels and
Sudan [12]. It enables us to distribute a secret though a “vault” using two
operations, namely, vault locking and unlocking. To lock a vault, we encode
the secret using a set of random values (vault key) and add a set of noise
(chaff) to obfuscate the encoded secret. Then, we publish the vault which
contains our encoded secret and the noise. Devices receiving the vault can
unlock it and retrieve the secret by demonstrating substantial knowledge
of the vault key. To unlock the vault, a device must use its version of the
vault key to pick out a substantial number of correct values from the vault
and decode the secret. Multi-secret fuzzy vault [11] is an extension to the
fuzzy vault scheme. It allows us to encode and decode multiple secrets using
multiple keys in the same vault. In Tiek, the vault keys are obtained from
the sources of randomness and encode the generated SKM.

The key distribution protocol as illustrated in Figure 2 is detailed as
follows:

1. **Vault Key Extraction:** At this step, we extract the sets of values (vault
keys) we use to encode the SKM and construct the vault. These sets are
sampled from the common and pairwise sources of randomness as follows:
(a) The CU initiates the vault key extraction procedure and provides the
necessary parameters devices need to collect the right set of random values.
(b) Upon receiving the initiation signal, all devices, including the CU, sample
the common source and retrieve an unordered set of random values (common
set). This set is the vault key that encodes/decodes the group portion
$g$.
(c) During the common source sampling procedure, the CU collaborates
with the nodes individually to sample the pairwise source and retrieve an
unordered set of values (pairwise set) for every node. These sets are the vault
keys that encode/decode the unique portions $\{u_i\}$. For details on how these
values are sampled and processed we refer to earlier work [2,4–6].

The result of this procedure at each node is a set of values correlated
between all devices and another set correlated between the CU and the node
itself. At the CU, these vault keys are denoted $A_0$ for the common set and
$\{A_i\}$ for the pairwise sets. The counterpart of these sets at the nodes are
denoted $\{B_j\}$ for $j \in [0,N]$ respectively.

2. **Vault Locking:** The goal of this step is to construct and publish a
multi-secret vault that enables nodes to retrieve their SKM. Using the vault
keys extracted in the previous step, the CU constructs a vault containing
all SKM and publishes it to participating devices. The vault construction
process proceeds as follows: (a) The CU creates a polynomial $p_j$ for every
SKM by breaking the SKM into small consecutive blocks of length $s$ and
using them as the polynomial coefficients. These polynomials are \( p_0 \) for SKM \( g \) and \( \{p_i\} \) for SKM \( \{u_i\} \). The order of polynomial \( p_j \) is denoted \( k_j \) and equals the length of the SKM it encodes divided by the block size \( s \) minus one. (b) Following polynomial construction, the CU projects each vault key \( A_j \) on its respective polynomial \( p_j \) and obtains the sets of points \( \{ P_j = (A_{jl}, p_j (A_{jl})) \mid l \in [0, \text{len}(A_j)] \} \). (c) Additionally, we create a set of random chaff points \( C \). Elements in \( C \) are not members of any set \( \{A_j\} \) and do not intersect with any polynomial \( \{p_j\} \). Chaff points are generated randomly and must not be distinguishable from points in \( \{P_j\} \) [12]. (d) All generated points are combined to create the set \( V = P_0 \cup \ldots \cup P_N \cup C \). Set \( V \) is our vault which contains all the points required to retrieve all SKM, in addition to chaff points designed to throw an attacker off any useful information. Figure 2 illustrates a multi-secret fuzzy vault containing four secrets. Any node \( n_i \) that receives the vault will be able to retrieve only SKM \( g \) and \( u_i \) through demonstrating their substantial knowledge of the vault keys \( A_0 \) and \( A_1 \). To this node, the rest of the points in \( V \) will appear as part of the chaff. (e) Finally, the CU broadcasts the vault to all participating devices.

3. **Vault Unlocking**: At this step, all nodes have the vault and the keys required to unlock their key portions. The goal here is for every node \( n_i \) to extract the group portion \( g \) and its unique portion \( u_i \) from the vault. This step proceeds as follows: (a) Node \( n_i \) extracts two sets of points from the vault \( V \), namely set \( R_0 \) and \( R_i \). Set \( R_0 \) is selected such that its elements are in set \( B_0 \). Similarly, set \( R_i \) elements are in set \( B_i \). (b) By applying Lagrange interpolation to the sets \( R_0 \) and \( R_i \), each node \( n_i \) reconstructs the polynomials \( p_0 \) and \( p_i \). (c) Node \( n_i \) then retrieves the SKM \( g \) and \( u_i \) from the coefficients of the reconstructed polynomials; hence receiving the group and the unique portions of its key.

4.3 **Key Combination**

At this point, every node has the group portion and unique portion of its key. These portions can be fused into the final key in various configurations influenced by the required security and the available resources. We use a key derivation function (KDF) to securely combine the two portions into the final key.

HKDF [13] is a KDF that relies on HMAC in a two-phase operation known as extract-then-extend. In the extract phase, a randomness extractor (XTR) samples the input SKM and produces a close-to-random output. The output of the XTR is then fed to a variable-length pseudorandom function (PRF*) to extend it to the required length or to generate multiple keys. In
HKDF both XTR and PRF* are implemented using HMAC with an optional salt as a key in the extract phase. We use HKDF because of its general applicability and simplicity.

We slightly alter the extract phase of HKDF to fit our purpose. Instead of using the extract phase to extract randomness from an SKM, we utilize it to fuse the two key portions securely. We run HMAC on the unique portion \( u_i \) and replace the salt with the group portion \( g \); \( K_i = \text{HMAC}(g, u_i) \). In the extend phase, we derive an \( x \) number of session keys from \( K_i \) which we use to enforce confidentiality and authenticity of exchanged messages between the node and the CU. Each session key is used for some hours then replaced by the next session key. When all \( x \) session keys have expired, the Tiek protocol restarts and replaces the master key.

In some situations, the cost of vault key extraction is prohibitive of distributing sufficiently long SKM. This can be rectified by using a key stretching primitive, such as Argon2 [14], as the XTR of HKDF. Note that this only increases the resources needed to brute-force the key, however, does not introduce any additional entropy. We maximize the length of the SKM before applying any key stretching technique.

The master keys \( \{K_i\} \) Tiek generates are composed of both the group and unique portions; thus enforcing the knowledge of both. An adversary must access the common source to participate in the network and must brute-force the unique key portion of every node it intends to attack individually. This makes Tiek resilient to off-body and body-worn adversaries.

5 Security Analysis

In this section, we analyze how Tiek fairs against the adversaries we consider in the adversary model. First, we analyze the security of key distribution through the multi-secret fuzzy vault scheme. Then, we elaborate on the properties of the distributed keys. Finally, we discuss different attack scenarios.

Throughout our analysis, we consider an example of four wearable devices \( (N = 4) \) and a CU, such as that in Figure 1. The network uses Tiek to agree on an individual key between each device and the CU.

5.1 Security of the Vault

The security offered by the fuzzy vault depends on the order of the encoded polynomial and the number of chaff points added. The minimum size of a vault key set that encodes/decodes a polynomial of order \( k \) is \( k + 1 \). In other words, for node \( n_i \) to reconstruct the polynomial \( p_j \) of order \( k_j \), \( R_j \) must contain \( k_j + 1 \) correct points; \( \text{len}(R_j \cap P_j) \geq k_j + 1 \). Recall that \( P_j \) is the
Figure 3: Security of the vault in relation to the polynomial order and the chaff size for four devices. The security of the vault increases with higher polynomial orders and a larger chaff. A body-worn adversary only slightly reduces the security of the vault. Note that C400 and C200 refers to a chaff size of 400 and 200 points respectively.

projection of the vault key $A_j$ on $p_j$, and $R_j$ is the set of vault points whose elements are in $B_j$.

During the key distribution phase of Tiek in our analysis example, the CU publishes a vault $V$ containing five polynomials which represent the group portion $g$ and four unique portions $\{u_i\}$. The vault also contains 200 chaff points ($\text{len}(C) = 200$). To simplify, we assume that all polynomials are of the same order $k = 19$. Hence, the size of our vault $\text{len}(V) = 300$ points. We use this example to discuss two scenarios where a passive adversary (eavesdropper) attempts to leak information about one or more keys from the vault.

In the first scenario, we consider a passive off-body adversary attempting to eavesdrop on the communication between the CU and a body-worn device. The adversary receives the vault and attempts to brute-force the key portions encoded in the vault. To violate the secure communication between the CU and a node $n_i$, this adversary needs to brute-force the group portion $g$ and the node’s unique portion $u_i$. Suppose the adversary tries every combination of 20 out of the 300 points. This sums up to over $7.5e30$ possible combinations which equals the requirements of brute-forcing a 102.56-bit key; $\log_2(\binom{300}{20}) \approx 102.56$.

For the second scenario, we assume a body-worn adversary as defined
in our adversary model. This adversary is already part of the network and knows the group portion as well as its unique portion. This leaves our vault with three encoded polynomials unknown to this adversary. In other words, if we assume that node \( n_1 \) is the body-worn adversary, then \( g \) and \( u_1 \) are revealed while \( u_2, u_3 \) and \( u_4 \) are still secret. Hence, the vault size is reduced to 260 points. Following our previous calculations, a body-worn adversary tries \( 3.87e29 \) different combinations which equals a 98.28-bit key.

In both scenarios, we find that Tiek achieves more than the recommended minimum of 85-bit security [12] even with a small 300-point vault. Figure 3 shows the security of the vault in relation to the polynomial order and the vault size in both scenarios. The security of the vault in our example can be improved by choosing a higher polynomial order or adding more chaff points.

There is an indirect relationship between the polynomial order and the cost of key distribution. Generally, higher polynomial orders require longer vault keys and, by conjunction, more measurements of the randomness sources. Previous work has shown that group sources of randomness can provide more bits per second compared to pairwise sources [5, 6, 15]. In Tiek this speed disparity gives system designers a trade-off between security and cost: On one hand, it is cheaper to increase security against off-body adversaries by using a polynomial of higher order to encode the group portion rather than the unique one. On the other hand, encoding the unique portion with a polynomial of higher order increases security against body-worn adversaries, as well as off-body ones, but comes at a higher cost. Moreover, different unique portions can use different polynomial orders which enables designers to further adjust Tiek to each device’s security needs and available resources.

5.2 Properties of the Distributed Keys

As introduced, the master keys \( \{K_i\} \) are composed of two portions. We elaborate on their properties and use:

Group portion \( g \) is Tiek’s way of authenticating a device’s presence on the body. In other words, if a device can retrieve \( g \) from the vault, it is considered an authentic device which authorizes it to participate in the network. Another possible use of \( g \) is to broadcast confidential messages to all body-worn devices. Broadcast messages can be encrypted using a key derived from the group portion alone. The authentication and broadcast security are only as strong as \( g \).

Unique portions \( \{u_i\} \) are the way Tiek enforces the second level of authorization and enables the CU to establish secure communication with individual devices. In other words, only node \( n_i \) can retrieve \( u_i \) from the vault which makes it the only node capable of constructing \( K_i \). Therefore, \( K_i \) is as strong as the combination of \( g \) and \( u_i \) against off-body adversaries,
but only as strong as \( u_i \) against body-worn ones.

The length of a key portion is a function of the polynomial order and the block size. Thus, by increasing the block size we can increase the length of a key portion at no additional cost. However, in reality, this may not contribute anything to the security of the system, because it is only as secure as the weakest point. For example, if we distribute 256-bit key portions using our vault from earlier, we gain no additional security over that provided by the vault. Simply because the adversary will resort to breaking the vault instead of the harder key portions. Therefore, we choose the key portion to match the security of the vault.

5.3 Attack Scenarios

We assume the presence of two adversaries in our analysis example: An off-body adversary within eavesdropping distance and one of our four wearables as a body-worn adversary. In the following, we identify multiple active attack scenarios and discuss them in light of our adversary model.

**Adversary joining the network:** The goal of the adversary is to impersonate a body-worn device and join the network. To join the network, an adversary would need to possess the group portion and its unique portion. While obtaining a unique portion from the CU is as easy as asking for it, the group portion bounds the presence of the device to the body. In other words, body-worn devices, including mal-behaving ones, can join the network, whereas off-body adversaries cannot obtain all the necessary key parts to participate. However, this property is violated on occasions when an off-body adversary obtains substantial information on the group portion through a side channel, such as advanced remote sensors or a vulnerable body-worn device. For instance, if a body-worn device has a vulnerability that reveals the group portion, an off-body adversary could exploit it to join the network. Note that an adversary that joins the network cannot eavesdrop on the communication between the CU and any other node without breaking the unique portion of that node. We can set a device count limit to mitigate DoS attacks where an adversary exploits this vulnerability to add many devices to the network.

**Adversary impersonating the CU:** This attack scenario is similar to the previous one, except, here, the adversary attempts to join the network as the CU. This is especially dangerous because if an adversary succeeds, it could control the entire network. To carry out this attack, an adversary must be able to measure both sources of randomness to encode its own key portions such that legitimate nodes are able to retrieve them. In other words, a body-worn adversary can easily impersonate the CU and publish its own vault. Hence, we propose an additional step in the protocol to allow nodes to verify the identity of the CU: Following the key combination step in our
protocol, the CU commits to a random value $v_i$ for each node $n_i$ and binds it to $K_i$. The next time Tiek distributes keys, the CU decommits $v_i$, commits to a new one and binds it to the newly distributed key. Assuming that a legitimate CU distributes keys using Tiek the first time, this commitment scheme ensures that only the same CU can run Tiek successfully the next times.

Side-channel attacks on the sources of randomness: These attacks are tied to the specific sources we utilize. In general, all the security requirements of the sources must hold for Tiek to function at its highest level of security. However, as discussed earlier, we design Tiek to tolerate situations where an adversary obtains unauthorized access to (compromises) a source of randomness through a side channel. Tiek only fails at the severest scenarios where both sources of randomness are compromised. However, successful side-channel attacks on the sources of randomness (even those that reveal insubstantial information) can reduce the overall provided security.

6 Conclusions

We provide a detailed description and security analysis of a novel authentication and key distribution protocol for wearable devices. We improve state-of-the-art by considering body-worn adversaries and mitigating the risk they pose. To this end, we utilize a common source of randomness to authenticate the presence of the devices on the body and leverage a pairwise source to tie each final key to a specific device. Finally, we show that our protocol is immune against eavesdropping and impersonation attacks under our adversarial model.

References


Paper II
Paper II
Privacy-preserving Continuous Tumour Relapse Monitoring Using In-body Radio Signals
Privacy-preserving Continuous Tumour Relapse Monitoring Using In-body Radio Signals

Sam Hylamia\textsuperscript{1}, Wenqing Yan\textsuperscript{1}, André Teixeira\textsuperscript{1}, Noor Badariah Asan\textsuperscript{1}, Mauricio Perez\textsuperscript{1}, Robin Augustine\textsuperscript{1}, Thiemo Voigt\textsuperscript{1,2}
\textsuperscript{1}Uppsala University, Uppsala, Sweden
\textsuperscript{2}RISE, Stockholm, Sweden

Abstract

Early detection and treatment of cancerous tumours significantly improve the lives of cancer patients, as well as increase their chance of surviving and reduce treatment cost. A novel study has utilised the human adipose (fat) tissue as a propagation channel for radio frequency communication within the human body. A notable application of this technology is the continuous monitoring of the growth of perturbants, such as tumours, in the channel. This paper addresses the privacy issues associated with the deployment of this monitoring technology. Our work departs from previous studies in that we consider the privacy of the sensing process itself, rather than the privacy of sensed data. We study the information leakage associated with the deployment of this technology and propose and evaluate a set of privacy-enhancing techniques that reduces information leakage. Finally, we propose and evaluate an approach that combines these techniques and, thereby, protects patient’s privacy.

1 Introduction

As the second leading cause of death, cancer claims the lives of millions of people every year \cite{1}. Early detection and treatment of cancerous tumours significantly improve the lives of cancer patients, as well as increase their chance of surviving and reduce treatment cost \cite{1}. However, as cancer treatments are not always efficient, cancer recurrence can occur with higher or lower rates depending on the type of disease in question \cite{2}. A recent review on challenges in early detection of breast cancer recurrence \cite{3} suggests that early detection of asymptomatic local recurrence via appropriate surveillance techniques could improve long-term survival when compared to late symp-
Automatic detection. This review also highlights the need of sensitive, and cost-effective surveillance strategies to detect early local recurrence.

A recent discovery may address this issue: Asan et al. have shown that the human adipose (fat) tissue can serve as a propagation channel for microwave radio communication [4]. A side-effect of this novel communication technique is its ability to monitor changes in the properties of the communication channel. Such changes could help with early detection of diseases, such as lymphedema or tumour relapse [5]. This paper addresses the privacy concerns associated with the deployment of this monitoring technology and proposes techniques to reduce information leakage.

This technique monitors tumours by observing changes in received signal strength (RSS) over a long period. Figure 1 shows the setup and result of a simulation demonstrating the effect of a growing tumour on the RSS. As the tumour grows in size, the RSS decreases. Monitoring this change over time reveals the presence of a perturbant in the channel. This observation could prompt an early medical examination and initiate the appropriate treatment.

From a privacy perspective, this is a challenging scenario since radio transmission, like those in Figure 1, radiate outside the body as skin does not absorb or reflect the signals completely [6]. Hence, there is a risk that an eavesdropper could infer the growth of a perturbant in the channel by exploiting such signal leakage and, thereby, violate patient privacy and reveal information about their health status.

Medical data, including information in electronic health records, is inherently private [7]. Once such private data leaks, it “may be reproduced infinitely, transmitted instantaneously, [or] used in ways formerly unimaginable” [8]. Parties interested in such private data include insurance companies, potential employers and the general public in the case of celebrities, for example. The suggested monitor technology introduces a novel challenge where not only the sensing result must be kept private but also the sensing process itself. This work is concerned with the privacy of the sensing process; contrary to previous work on data privacy and security as we discuss further in §7.

Contributions. In this work, we consider an eavesdropping attack scenario and

- study information leakage from the perspective of a powerful passive eavesdropper,
- demonstrate that trivial solutions are ineffective under our adversary model,
- propose and evaluate a set of practices to reduce information leakage, and
- present an adequate privacy-enhancing technique that preserves the privacy of the patient.
(a) Simulation setup. A perturbant (tumour) growing in adipose tissue between a layer of skin and another of muscle. The thickness of these layers are 2, 25 and 30 mm for the skin, fat and muscle respectively. The Tx probe launches microwave signals (2.4 GHz) through the adipose layer to the Rx probe at 0 dBm output power.

(b) Simulation Result. As the tumour grows, the RSS decreases. Monitoring this decrease over a period of time reveals the presence of the tumour/perturbant in the channel.

Figure 1: Setup and result of a simulation demonstrating continuous in-body tumour monitoring.

Outline. We organize the rest of this paper as follows: §2 provides a background on the communication and sensing technology we address. §3 describes the monitoring system model and the adversary model. In §4 we list and describe the privacy-enhancing techniques we propose. §5 provides an overview of our simulation setup, communication channel model and how we simulate the monitoring system. In §6 we expand on, analyse and evaluate our privacy-enhancing techniques. §7 presents the related work and,
finally, in §8, we summarize our findings.

2 In-body Communication and Sensing

Human body tissues have different concentrations of water; some tissues have a low water content, such as adipose (5-10%) and bone (8-16%) tissues, while others have a higher water content, such as muscle (73-78%) and skin (60-76%) tissues [9]. The low water content of adipose tissue gives it a low dielectric constant and makes it a potential candidate as an in-body communication channel for microwave radio communication as Asan et al. demonstrate and characterise [4, 6]. This communication channel works well as the human adipose tissue is often situated between muscle and skin tissues which improves the confinement of radio waves in the fat channel similar to a dielectric waveguide.

An in-body communication channel is useful for several reasons: First, as life-expectancy increases, more patients contract multiple diseases. Hence, the number of embedded medical devices in their bodies increases to collect vital information about their health status, perform targeted drug delivery and replace non-functioning organs with artificial ones. Second, we envision distributed control loops enabled by implanted devices, for example, sensing devices at one part in the body that control drug delivery devices in other parts. Third, transmitting data out of deeply implanted devices is difficult; hence, an in-body communication channel makes it possible to transfer data to devices located in parts of the body where it is easier to couple out the signals [10].

A significant advantage of this approach is its ability to support high data rates [10]. This allows for supporting multiple sensors and, in the long run, more data-intensive applications, such as brain-to-machine interfaces. As we discussed in §1, this communication channel can also be used for sensing the growth of tumours. However, this puts the privacy of the patients at risk if not addressed properly.

3 System Model and Adversary Model

We consider an application scenario, such as that in Figure 1a, where two devices are implanted on opposite sides of a high probability tumour relapse area. The two devices send and receive messages through the adipose layer that connects them. Both devices can send and receive messages, as well as coordinate their actions. All exchanged messages are encrypted and tamper-proofed. The goal of the system is to monitor the area between the two devices for changes that could indicate a tumour relapse. To this end, they
exchange messages periodically and measure the RSS. Long-term decrease in measured RSS is considered to be indicative of tumour relapse, in which case a medical exam is required.

We recognize a passive eavesdropper capable of picking up transmissions originating from our monitoring system. It can measure the RSS of the messages it detects, but it cannot decrypt these messages, tamper with their content nor inject additional messages. The eavesdropper can be as close as the surface of the skin above the monitoring area for as long as the monitoring system is operational. Additionally, we assume that the eavesdropper knows where each of the monitoring devices is implanted and the role of each device. We choose this rather powerful adversary model to analyse the privacy of the system from the perspective of a worst-case scenario. The goal of the eavesdropper is to violate the patient’s privacy and disclose information about their health status to an unauthorised party. The monitoring system we describe is aware of the possible presence of eavesdroppers and their ability to violate the patient’s privacy.

4 Privacy Preservation

The monitoring system employs privacy-enhancing techniques to reduce the amount of information the adversary can deduce from its observations; hence, preserving the patient’s privacy. In this work, we propose and evaluate a set of privacy-enhancing techniques the system could employ. Additionally, we advise a combination of these techniques that minimizes information leakage. The privacy-enhancing techniques we consider are:

1. Random variation of output power. The transmitter varies its output power according to a predetermined secret sequence. The receiver knows this sequence and accounts for it during analysis. This technique aims to hide the changes in RSS the tumour causes by introducing noise at the eavesdropper.

2. Adaptive variation of output power. The transmitter and receiver cooperate in response to low-frequency variations of the RSS. The transmitter varies the output power to compensate for variations that could indicate a tumour relapse. The receiver is aware of these variations and accounts for them during analysis. The goal here is to compensate for the changes in RSS at the eavesdropper to obfuscate signs of tumour growth.

3. Channel hopping. The transmitter varies the channel at which it sends each message according to a predetermined secret sequence. This makes it impossible for the adversary to record the RSS of all messages. The receiver knows this sequence and is able to receive the messages. The transmission frequency of each message is considered during analysis since different fre-
quencies experience different path loss [4].

4. **Sender anonymity.** Both devices are transceivers. They remove any public identification information from their messages, vary their output power randomly and transmit at random intervals. This makes it impossible for the adversary to identify the source of messages perfectly. RSS readings from both devices are collected and analysed with respect to the output power and source of message.

While the first two techniques add (controlled) noise to the sensing signal, the latter two reduce the number of effective samples for a statistical analysis by the adversary. In §6, we expand on, analyse and evaluate each of these techniques. Moreover, we analyse and evaluate approaches that leverage the combined benefits of these techniques.

## 5 Simulation Setup

We use simulations to illustrate and evaluate the privacy-enhancing techniques we propose in §4. In this section, we describe the setup and assumptions we use for this simulation. We describe the simulation setup, followed by the channel model and the system operation model.

**Simulation setup.** We utilize the channel model in Figure 1a where a perturbant grows in an adipose layer between a skin and a muscle layer. Each of these layers is 2, 25 and 30 mm for skin, fat and muscle respectively [5]. Two monitoring devices sense any changes in RSS indicative of perturbant growth in the channel. We place each device on either side of where the perturbant grows; 50 mm away from its center. This symbolizes an application scenario where these devices are implanted to monitor local tumour relapse after removing a cancerous tumour. The perturbant grows to 10 mm in radius when it would typically be detected and removed.

Eavesdropping on this channel are two passive non-cooperating adversaries. Each adversary is 25 mm on either side of the perturbant. Our monitoring system is aware of the possible presence of eavesdroppers but their location. To simplify path-loss calculations, we assume that the eavesdroppers are in the adipose layer rather than on the surface of the skin. Note that to place the adversary on the skin we only need to factor in the skin path-loss.

**Channel model.** Our signals (2.4 GHz) propagate through two mediums, namely adipose tissue and perturbant tissue. We model path-loss through adipose tissue \( L_a \) as a function of the distance between the transmitter and receiver \( d \).

\[
L_a = 0.24d \tag{1}
\]

We extract the constant (0.24) from the simulation shown in Figure 1; before
the tumour starts growing and at a distance of 100 mm the path-loss is 24 dB. Further, we model path-loss through perturbant tissue \( (L_p) \) as a function of the radius of the perturbant \( (R) \).

\[
L_p = -\frac{9.52}{1 + e^{-1.2(R-8.04)}}
\]  

(2)

The loss function (2) is obtained through a non-linear least-squares curve fit over the points shown in Figure 1b. Finally, we model the RSS \( (P_{Rx}) \) as a function of the output power \( (P_{Tx}) \) and the path-loss of adipose tissue \( (L_a) \) and perturbant tissue \( (L_p) \).

\[
P_{Rx} = P_{Tx} - L_a - L_p
\]  

(3)

Note that Equation 3 applies to signals that does not propagate through the perturbant by settings the radius of the perturbant \( (R) \) to 0. For simplicity, we consider that, aside from the perturbant, the channel does not change in dielectric nor physical properties during simulations.

**System operation model.** For the purpose of this simulation we use a simple discrete event simulator written in python simpy. We set the radius of the perturbant to grow from 0 to 10 mm in 0.1 mm increments every \( t_p \) time units (ticks). The monitoring system operates by sending messages from the transmitter to the receiver periodically every \( t_m \) time units. The simulation runs while the perturbant is growing, in addition to \( t_o \) offset time units before the perturbant starts growing and after it stops.

## 6 Evaluation

In this section, we evaluate and discuss the privacy-enhancing techniques we proposed in §4. Note that our analysis is primarily concerned with the effectiveness of the privacy-enhancing techniques. We leave the analysis of the trade-off between privacy, processing complexity and detection accuracy for future work. We setup a simulation as described in §5 with the following parameters: The perturbant grows by 0.1 mm every tick \( (t_p = 1) \). The transmitter sends a message every \( t_m = 1 \) tick. The time offset before and after perturbant growth \( t_o = 25 \) ticks. The transmitter can use an output power between \(-40\) and \(0\) dBm. We run each simulation 500 times. Figure 2 shows the results of these simulations. Alice and Bob represent our monitoring devices, while Eve and Trudy represent the eavesdroppers between Bob and the perturbant and between Alice and the perturbant respectively. Figure 2a shows their relative locations. Next, we describe, analyse and evaluate each proposed technique.
(a) Relative location of simulated devices and tumour.

(b) **Random variation of output power.** Eve can detect the perturbant by monitoring the decrease in its average RSS.
(c) **Adaptive variation of output power.** Trudy can detect the perturbant by monitoring the increase in its average RSS.

(d) **Channel hopping.** Eve and Trudy receive fewer messages. However, Eve can often detect the perturbant by monitoring its average RSS.
(e) **Sender anonymity.** Eve and Trudy are unable to distinguish the source of all messages. However, they can detect the perturbant by monitoring their average or minimum RSS.

(f) **Sender anonymity with adaptive variation of output power.** Neither adversary can detect the perturbant from their observations.
(g) **Sender anonymity with adaptive variation of output power and channel hopping.** Further reduces the data eavesdroppers can observe.

Figure 2: Figure 2a illustrates the location of the Alice, Bob, Eve and Trudy in relation to the perturbant. Each of the figure pairs in the following pages shows the simulation result of one of the privacy-enhancing techniques. The top figure of each pair shows the output power of each sent message of a simulation run for illustration. Additionally, it shows the moving average of the output power of each run averaged over five hundred simulation runs. The first four figure pairs show the privacy-enhancing techniques individually, while the last two show a combination of two or more of these techniques.
6.1 Output Power Manipulation Techniques

A naive approach to enhance the privacy of the system is to randomly vary the output power of the transmitter. This technique hides the changes in RSS at the eavesdropper by introducing noise to its measurements. As a result, the adversary can no longer observe the decrease in RSS by comparing consecutive samples. However, it can simply detect the perturbant by calculating the moving average of the measurements. Thus, this naive approach alone is ineffective at reducing information leakage. In Figure 2b, Alice varies its output power between $-40$ and $0$ dBm randomly. Eve can simply detect the perturbant by observing the decrease in the moving average of the signal. On the other hand, Trudy cannot detect the tumour since it measures the RSS of messages before they propagate through the perturbant.

An adaptation of the previous technique is to increase the average output power as the perturbant grows. In other words, we vary the output power randomly while adaptively increasing its average as we detect the growth of a perturbant. This technique requires coordination between the monitoring devices. We use measurements from the receiver as feedback to adapt the output power accordingly. This approach is simple and effective at eliminating information leakage at an eavesdropper located between the perturbant and our receiver. However, an adversary located between the transmitter and the perturbant can easily detect these changes and infer the presence of the perturbant. Figure 2c makes this clear as Trudy can detect the presence of the perturbant by observing the increase in the moving average of its measurements. Eve, on the other hand, cannot detect the perturbant as Alice increases its output power to compensate for its effect.

6.2 Information Reduction Techniques

Neither of the above techniques proved effective at reducing information leakage. In either approach, one of the two eavesdroppers could detect the perturbant depending on their location relative to it. Hence, we explore two additional techniques, namely channel hopping and sender anonymity. In the following two paragraphs, we discuss and evaluate each of these two techniques.

In channel hopping, additional to randomly varying the output power, the transmitter chooses the channel at which to send each message according to a predetermined random sequence known to both monitoring devices. Oblivious to this sequence, eavesdroppers can only measure a subset of the exchanged messages. The number of channels our system can utilize ($N_c$) versus the number of channels the eavesdropper can measure ($N_e$) determines the effectiveness of the technique. In other words, an eavesdropper has
a probability $P_r = \frac{N_e}{N_c}$ of measuring the RSS of any exchanged message. This technique reduces the number of messages an eavesdropper can detect; hence, increasing the deviation between its measurements. Figure 2d is an application of this technique with $P_r = 0.2$. In this figure, we observe that despite the significant increase in standard deviation, Eve can still detect the perturbant on average. As we observe, increasing the number of channels – hence reducing $P_r$ – yields a substantial decrease in information leakage at a higher cost.

Sender anonymity requires both monitoring devices to act as transceivers. They send and receive messages and measure their RSS. We omit all identification information from exchanged messages and have devices take turns sending messages according to a predetermined secret sequence. Oblivious to this sequence, the eavesdroppers cannot successfully identify the source of a message with a high success rate. As Figure 2e shows, the average decrease in RSS an eavesdropper measures is less than that in previous techniques. This is because half of the messages an eavesdropper observes do not experience signal attenuation from propagating through the perturbant. However, this still insufficiently reduces the ability of an eavesdropper to detect the perturbant, especially when it can identify the source of messages furthest from the average. Moreover, the observable decrease in the lower envelope of the eavesdropper’s measurements can indicate perturbant growth.

Figure 3: **Sender anonymity with adaptive variation of output power.** Histogram KDE of measurements before and after perturbant growth over 500 simulation. The figure to the left shows the KDE Eve and Trudy measure before the perturbant starts growing. The figure to the right shows the KDE after the perturbant stops. The difference in KDE reveals the presence of a perturbant to the eavesdroppers.
6.3 Compound Techniques

Despite its shortcomings, sender anonymity provides the advantage of virtually eliminating the differences between the two sides of the perturbant. In other words, Eve and Trudy in Figure 2e measure a similar moving average. This forms the basis of the two techniques we propose next. These techniques are a combination of two or more of the previous ones, namely, sender anonymity with adaptive variation of output power and sender anonymity with adaptive variation of output power and channel hopping.

Combining sender anonymity with adaptive variation of output power addresses the shortcomings of both techniques. In other words, the former eliminates the differences between observations before and after the perturbant; meanwhile, the latter hides the decrease in RSS the perturbant causes. For this to work, however, we cannot increase the average output power as we did previously. In doing so, we increase the moving average power both eavesdroppers receive revealing the perturbant. Instead, we increase the minimum power as the perturbant grows and keep the maximum power constant. This addresses the issue where the lower envelope of the RSS measurements decreases as observed in 2e. Figure 2f shows that as Eve and Trudy observe no changes in the moving average nor the envelope of their measurements. A complementary advantage of this approach is that both monitoring devices can detect the growth of the perturbant; hence, require no feedback to vary their output power adaptively.

We arrive at a decent solution when we utilize sender anonymity and vary the output power adaptively. However, a close examination of this technique reveals a change in the distribution of RSS measurements the eavesdroppers collect. Figure 3 shows an observable difference in the KDE of Eve’s and Trudy’s measurements before and after perturbant growth; hence, revealing the presence of the perturbant. We address this issue with our final proposal: We combine the former technique with channel hopping. This reduces the number of measurements eavesdroppers can collect; hence, minimizing their ability to make any meaningful inferences from their observations. In Figure 2g, Eve and Trudy observe no changes in the moving average nor the envelope of their measurements. Additionally, they are unable to collect enough points for a meaningful statistical analysis of their measurements. This technique is simple to implement and provides adequate privacy for the user.

Overall, we conclude that, independently, the techniques we propose are insufficient at preserving the privacy of the sensing signal. However, combining sender anonymity, channel hopping and adaptive variation of output power provides a solution that adequately preserves the user’s privacy.
7 Related Work

We are unaware of any research on the privacy of the sensing process itself. A notable exception is an extensive body of privacy-preserving localisation techniques [11, 12]. While there is plenty of work (including a large body of survey papers on security and privacy) in the field of wireless sensor networks for healthcare applications, Ameen et al. state that “privacy issue[s] or other social implications are not discussed extensively regarding this field” [13]. Existing research to a large extent covers rules and policies to protect and handle sensitive patient data [14], in particular, the security of medical health records [15, 16]. Related to our work are also schemes that securely handle data; thus, preserving the privacy of sensed data, especially in medical applications. These schemes include lightweight security schemes for preservation of sensed data [17], as well as data aggregation [18], integration [19] and big data analytics [20] of medical data. As mentioned above, our work differs from these approaches; we aim to avoid information leakage from the sensing process itself rather than the complementary issue of handling the sensed data in a privacy-preserving manner.

8 Conclusions

In-body communication and sensing using adipose tissue is a novel technology that enables an innovative technique of continuous tumour relapse monitoring. However, since the transmissions this technology uses are not confined to the body, it poses a risk to the patient’s privacy. In this work, we consider the privacy of the sensing process, rather than the privacy of the sensed data. We analyse the information leaked to a powerful passive eavesdropper and present four privacy-enhancing techniques. We describe, analyse and evaluate each of these techniques individually and in combination of each other. We observe that, while each of these four techniques enhances the privacy of the measurement process, they are, individually, ineffective at preserving the patient’s privacy. Finally, we propose and evaluate an approach that protects the patient’s privacy adequately by leveraging the combined benefits of three of these techniques.

References


<table>
<thead>
<tr>
<th>Year</th>
<th>编号</th>
<th>作者</th>
<th>标题</th>
</tr>
</thead>
<tbody>
<tr>
<td>2021-002</td>
<td>Karl Bengtsson Bernander</td>
<td>Improving Training of Deep Learning for Biomedical Image Analysis and Computational Physics</td>
<td></td>
</tr>
<tr>
<td>2021-001</td>
<td>Niklas Gunnarsson</td>
<td>On the Registration and Modeling of Sequential Medical Images</td>
<td></td>
</tr>
<tr>
<td>2020-006</td>
<td>David Widmann</td>
<td>Calibration of Probabilistic Predictive Models</td>
<td></td>
</tr>
<tr>
<td>2020-005</td>
<td>Anna Wigren</td>
<td>Exploiting Conjugacy in State-Space Models with Sequential Monte Carlo</td>
<td></td>
</tr>
<tr>
<td>2020-004</td>
<td>Muhammad Osama</td>
<td>Machine Learning for Spatially Varying Data</td>
<td></td>
</tr>
<tr>
<td>2020-003</td>
<td>Christos Sakalis</td>
<td>Securing the Memory Hierarchy from Speculative Side-Channel Attacks</td>
<td></td>
</tr>
<tr>
<td>2020-002</td>
<td>Ulrika Sundin</td>
<td>Global Radial Basis Function Collocation Methods for PDEs</td>
<td></td>
</tr>
<tr>
<td>2019-006</td>
<td>Kristiina Ausmees</td>
<td>Efficient Computational Methods for Applications in Genomics</td>
<td></td>
</tr>
<tr>
<td>2019-005</td>
<td>Carl Jidling</td>
<td>Tailoring Gaussian Processes for Tomographic Reconstruction</td>
<td></td>
</tr>
<tr>
<td>2019-004</td>
<td>Amin Kaveh</td>
<td>Local Measures for Probabilistic Networks</td>
<td></td>
</tr>
<tr>
<td>2019-003</td>
<td>Viktor Bro</td>
<td>Volterra Modeling of the Human Smooth Pursuit System in Health and Disease</td>
<td></td>
</tr>
</tbody>
</table>