Poster Abstract: Towards Secure Backscatter-based In-Body Sensor Networks

Thiemo Voigt, Christian Rohner, Wenqing Yan, Laya Joseph, Sam Hylamia*
Uppsala University, Sweden
firstname.lastname@it.uu.se

Noor Badariah Asan
CeTRI, FKEKK
Universiti Teknikal Malaysia Melaka
Malaysa
noorbadariah@utem.edu.my

Bappaditya Mandal, Mauricio Perez, Robin Augustine
Uppsala University, Sweden
firstname.lastname@angstrom.uu.se

ABSTRACT

We expect that in the near future more and more people will have multiple implants to handle their diseases. The implants benefit from being connected using in-body sensor networks. We have previously shown that RF communication through human adipose (fat) tissue is feasible. In this poster, we argue why we believe that backscatter communication within this fat channel is possible. As security is of utmost importance for in-body communication, we also discuss how backscatter-based in-body networks can be secured.

1 INTRODUCTION

As more and more people get older and may get multiple diseases, we expect the number of patients with several implants to increase rapidly. Networking implants in the body is meaningful for several reasons: embedded medical implants collect vital information about patients' health status, they may perform targeted drug delivery (possibly by distributed control loops of sensing and delivery devices) and may also replace non-functioning organs with artificial ones. While transmitting data out of deeply implanted devices is difficult, an in-body communication channel allows to transfer data to implants that are located in parts of the body where it is easier to couple out the signals [3].

Towards this end, we have recently shown that human adipose (fat) tissue can act as a communication channel inside the body [2]. The salient communication properties of the fat channel may indeed enable us to use extremely energy-efficient backscatter communication inside the body, at least between the gateway (that we call aggregator) and the devices within its communication range. While energy harvesting inside human bodies is attracting attention [5], the energy availability in human bodies is still scarce. Hence, backscatter could help to drastically reduce the energy consumption for networked implants. We present evidence that backscatter-based in-body communication might be possible.

Security for backscatter communication is, however, in its infancy [9] and in-body networks require a high degree of security. Therefore, we also discuss how we can combine our previous results on key distribution for wearable devices and authentication for backscatter devices into a security architecture that can pave the way for secure in-body sensor networks using backscatter.

*This project is financially supported by the Swedish Foundation for Strategic Research and the Swedish Research Council (grants 2017-045989 and 2018-05480)

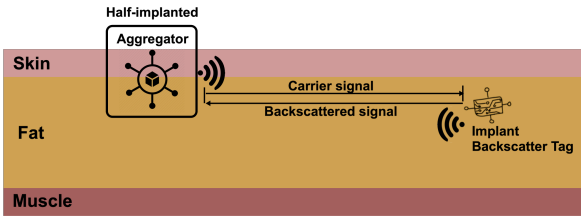

Figure 1: Backscatter in the Fat Channel where the aggregator acts as carrier generator and receiver.

2 FEASIBILITY OF IN-BODY BACKSCATTER COMMUNICATION

Using backscatter communications, sensor tags are relieved from the task of generating their own radio waves. Avoiding this energy-intensive task enables sensor tags to transmit their sensor readings at an energy consumption that is radically lower than that of conventional low-power radios. This makes backscatter attractive for in-body networks where the energy is scarce.

We have earlier shown that the human fat tissue can serve as a communication channel for microwave radio communication, e.g. , using RF in the 2.4 GHz band [2]. One particular characteristic of this communication channel is that fat is in many parts of the body situated between layers of skin and muscle, i.e., between tissues which are electrically different to it, creating natural waveguiding structures from these tissues inside the body. This implies that the signal attenuation per distance unit is constant for the fat channel (at least where the geometry is roughly constant). Our earlier works show that the signal loss in human tissue is below 2 dB/cm [2].

Figure 1 presents a scenario where a half-implanted aggregator, i.e., the gateway between the in-body network and the external world, acts as both a carrier generator and receiver for a backscatter-based implant. Note that such a setup would not necessarily require two radios that are implanted. We could place one of the radios outside the body, i.e., on the non-implanted part of the body aggregator with the antenna connected to the skin. Our experiments with phantoms (artifacts that are designed to mimic the characteristics of human tissues, for example, their dielectrical properties) have shown that an antenna that is outside the body but in touch with the skin and optimized for the purpose of communicating through the fat channel has a loss around 8 dB. For our case, an in-body antenna specifically designed for communication into the fat channel can be considered as lossless [1]. Hence, we can estimate the signal loss for this communication as consisting of three parts: the loss for communication to and from the implant and the loss at the backscatter-based implant. The latter can be estimated to be less than 5 dB [7].

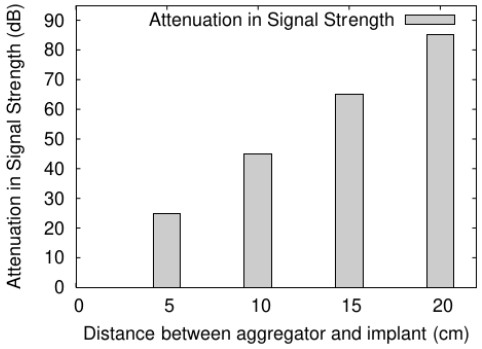

Figure 2: Signal Attenuation over Different Distances for Backscatter in the Fat Channel.

Based on these inputs, we estimate the signal attenuation as shown in Figure 2. The figure shows that even for a distance of 20 cm, the signal attenuation is around 85 dB assuming two implanted radios. A typical low-power radio such as the CC2420 has a sensitivity threshold of around -95 dBm and an output power of 0 dBm, i.e., a difference of around 95 dB and could hence be used as carrier transmitter and receiver. For bridging larger distances, we could use other backscatter technologies that achieve longer ranges such as LoRea that can leverage more sensitive receivers [10].

3 TOWARDS SECURE IN-BODY BACKSCATTER

In-body sensor networks must be secured to avoid life-threatening scenarios where attackers control implanted devices such as pacemakers or insulin pumps, or install malware or ransomware inside a human's body.

3.1 Key Generation and Distribution

The basic of most security schemes are keys for encryption and authentication. In earlier work, we have presented Tiek [6], a novel authentication and key distribution protocol. Tiek is a physical measurement-based authentication and key distribution scheme that in contrast to other approaches does not assume that body-worn or implanted devices are benign and uncompromised. On a high level, Tiek utilizes a common source of randomness such as the interpulse-interval or gait and a pairwise source such as RSSI to distribute a unique key to every device in the network. In our current architecture, Tiek uses the aggregator to generate keys and the sources of randomness to distribute them securely among the implants. Tiek is currently devised for one-hop networks, i.e., networks where all implants can be reached from the aggregator. Future work aims at extending it to multi-hop networks.

3.2 Authentication

While security for backscatter communication is in its infancy [9], we have recently presented a first stab at authentication for backscatter devices [11]. In this work, we propose to add authentication information in the chip sequences of the Direct-Sequence Spread Spectrum (DSSS)-based physical layer for IEEE 802.15.4-based backscatter tags for which both backscatter transmitters and backscatter-based receivers exist [8]. The authentication information is added in form of chip flips in the chip sequence where these chip flips become the message authentication code. The choice of chip flip is derived from a key that is shared between sender and receiver where we use Tiek to distribute the keys. Note that manipulating the chip sequences in 802.15.4 may decrease reliability since additional chip flips may cause the decoding process at the receiver to fail. While our earlier experiments have shown that the fat channel has a high reliability [4], future work needs to investigate this trade-off between security and reliability in the fat channel in more detail. Furthermore, this approach requires a receiver that exposes low-level information such as the chip sequence. Such a radio could be outside the body as discussed in the previous section.

Using 802.15.4-based backscatter, we are able to manipulate the chip sequence. Other approaches for backscatter such as LoRea do not employ DSSS. Here, one could implement a similar approach in the application layer. The disadvantage of this approach would be the increase of the packet size but on the other hand, there is no need for receivers with access to the physical layer chip sequence.

4 CONCLUSIONS

Using a simple model, we have shown that backscatter communications seems to be feasible in the fat channel in human bodies. Leveraging our previous work on security both for in-body networks and for backscatter, we have outlined paths towards secure in-body sensor networks.

REFERENCES

[1] Noor Badariah Asan, Emadeldeen Hassan, Jacob Velander, Syaiful Mohd Shah, Daniel Noreland, Taco Blokhuis, Eddie Wadbro, Martin Berggren, Thiemo Voigt, and Robin Augustine. 2018. Characterization of the Fat Channel for Intra-Body Communication at R-Band Frequencies. *Sensors* 18, 9 (2018).

[2] Noor Badariah Asan, Daniel Noreland, Emadeldeen Hassan, Syaiful Redzwan, Mohd Shah, Anders Rydberg, Taco J. Blokhuis, Per-Ola Carlsson, Thiemo Voigt, and Robin Augustine. 2017. Intra-body microwave communication through adipose tissue. *IET Healthcare Technology Letters* (2017).

[3] Noor Badariah Asan, Carlos Pérez Penichet, Syaiful Redzwan Mohd Shah, Daniel Noreland, Emadeldeen Hassan, Anders Rydberg, Taco J Blokhuis, Thiemo Voigt, and Robin Augustine. 2017. Data packet transmission through fat tissue for wireless intraBody networks. *IEEE Journal of Electromagnetics, RF and Microwaves in Medicine and Biology* 1, 2 (2017).

[4] Noor Badariah Asan, Jacob Velander, Yaiful Redzwan, Robin Augustine, Emadeldeen Hassan, Daniel Noreland, Thiemo Voigt, and Taco J Blokhuis. 2017. Reliability of the fat tissue channel for intra-body microwave communication. In *2017 IEEE Conference on Antenna Measurements & Applications*.

[5] Canan Dagdeviren, Zhou Li, and Zhong Lin Wang. 2017. Energy harvesting from the animal/human body for self-powered electronics. *Annual review of biomedical engineering* 19 (2017), 85–108.

[6] Sam Hylamia, Wenqing Yan, Christian Rohner, and Thiemo Voigt. 2019. Tiek: Two-tier Authentication and Key Distribution for Wearable Devices. In *WiMob*. IEEE, 1–6.

[7] Bryce Kellogg, Vamsi Talla, Shyamnath Gollakota, and Joshua R Smith. 2016. Passive wi-fi: Bringing low power to wi-fi transmissions. In *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI)*.

[8] Carlos Pérez-Penichet, Dilushi Piumwardane, Christian Rohner, and Thiemo Voigt. 2020. TagAlong: Efficient Integration of Battery-free Sensor Tags in Standard Wireless Networks. In *ACM/IEEE IPSN*. IEEE.

[9] Nguyen Van Huynh, Dinh Thai Hoang, Xiao Lu, Dusit Niyato, Ping Wang, and Dong In Kim. 2018. Ambient backscatter communications: A contemporary survey. *IEEE Communications Surveys & Tutorials* 20, 4 (2018), 2889–2922.

[10] Ambuj Varshney, Oliver Harms, Carlos Pérez-Penichet, Christian Rohner, Frederik Hermans, and Thiemo Voigt. 2017. LoRea: A backscatter architecture that achieves a long communication range. In *ACM SenSys*.

[11] Thiemo Voigt, Carlos Perez-Penichet, and Christian Rohner. 2020. Extended Abstract: Towards Physical-LayerAuthentication for Backscatter Devices. In *3rd International Workshop on Attacks and Defenses for Internet-of-Things (ADIoT)*.