Enabling Physically Secure Human Body Communication in Body Resonance Region with Faraday Fabric

Qi Huang*, Samyadip Sarkar*, Shreyas Sen*
*School of Electrical and Computer Engineering, Purdue University, USA

***Abstract*—Human Body Communication (HBC) is an energy-efficient alternative to conventional radio frequency (RF) communication. The HBC in the Electro-Quasistatic (EQS) region is physically secure as the signal is mostly confined within 5∼10 cm around the human body. However, HBC in the body resonance (BR) region suffers greatly from radiation, which makes the signal easily eavesdropped even at a large distance, and there have not been any efficient shielding methods. This paper, for the first time, introduces a method to shield the BR HBC signal and greatly minimize leakage. Firstly, the transmitter-body interface leakage of the BR HBC signal is measured from 10 cm to 30 cm. Then with the Faraday fabric shielding the transmitter, the interface leakage is measured again for comparison. Moreover, the on-body measurements are implemented with and without the Faraday fabric shield. The measurement results show that the Faraday fabric shield can reduce the leakage by 23.1∼48.6 dB at 10 cm, and at 20 cm and 30 cm the leakage from the shielded transmitter is lower than -70 dB. The shield can reduce the channel gain of the on-body receiver by up to 20.41∼40.88 dB and makes the leakage channel gain decrease by 10.1 ∼ 22 dB more than the on-body scenario. The security benefit achieves the largest around the BR peak frequencies. Beyond the BR peak frequencies, the on-body receiver detects similar or even lower power than the off-body ones. Therefore, the human body plays a major role in the BR peak frequencies while beyond that the transmitter radiation is dominant in transmitting information in the BR HBC system.**

***Index Terms*—Human Body Communication (HBC); Channel gain measurement; Physical security; Body resonance region**

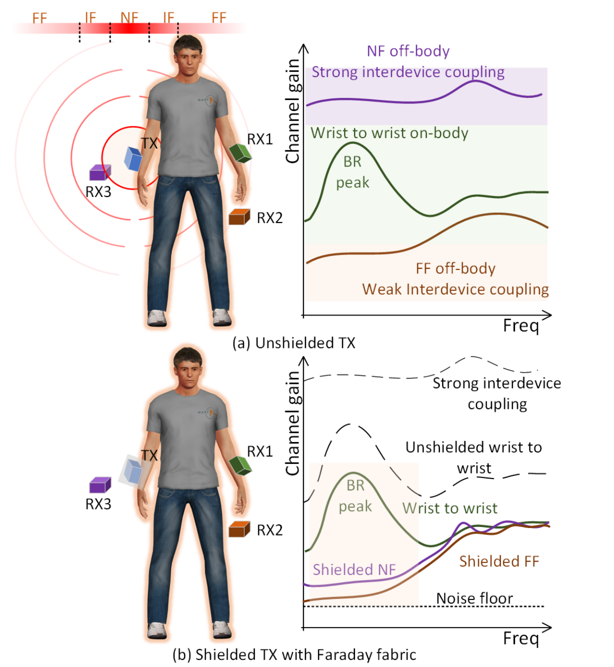

Fig. 1: Comparison of channel gain patterns in BR region. (a) Channel gain pattern of an unshielded transmitter; (b) Channel gain pattern of a shielded transmitter. NF: near field; IF: intermediate field; FF: far field.

I. Introduction

Over the past decades, HBC, with the human body as the low-loss communication channel, has been an energy-efficient alternative to RF in the wireless body area network (WBAN), providing up to 100X improved energy efficiency [1]. Moreover, there have been HBC systems for biosignal transmission developed based on commercial off-the-shelf components or platforms [2]–[5]. However, the electromagnetic (EM) signal radiates in all directions from the transmitter and cannot be completely confined within the human body, depending on different frequencies, surroundings, and many other factors. These allow hackers and eavesdroppers to detect or even attack critical biosignals easily, causing much danger to the patients. Additional encryption techniques, such as AES256, spread spectrum, frequency hopping, etc., apply to WBAN systems to improve physical security but with extra power consumption. There have been some studies on the physical security performance of the EQS HBC, but the physical security of BR HBC has never been explored, and an effective method to shield the HBC signal has not been found.

D. Yang [6] measured the EQS HBC signal leakage in 3 scenarios: direct line-of-sight (LoS) leakage, body obstructed leakage, and standalone coupler. The results showed that the presence of the human body as a coupler to receive the signal significantly increases the leakage, and the body-obstructed scenario has a lower leakage than the LoS one. D. Das et al. [7] comprehensively explored the EQS HBC physical security performance and compared the privacy space between the traditional RF WBAN and EQS-HBC based on correlation and bit error rate (BER) analysis. The measurement results show that the leakage from the on-body EM wireless communication in WBAN systems is detectable up to 5 m. In comparison, the leakage from the EQS-HBC transmitter-body interface is detectable only up to 0.15 m, and the leakage from the human body has a detection range of ∼0.01 m. M. Nath [8] explored the effect of the human body as a capacitive coupler for inter-body attack and interference and identified three different regions based on the frequencies: EQS region, body EM coupling region, and device EM coupling region. Moreover, the signal level of the transmitter can be tuned to maintain a limit for the signal-to-noise ratio (SNR) at the receiver side to remedy the vulnerability of the EQS HBC and keep the safe distance within 10 cm. In the BR region, the HBC transmitter can be approximated as an infinitesimal dipole, which radiates the signal to the environment and resonates the human body. In the near-field region of the dipole, the leakage signal received by the off-body receivers can be even stronger than the detected signals by the on-body receivers due to the very strong inter-device coupling, as shown in Fig. 1 (a). When the distance is larger, the leakage signal is still detectable and decodable, which largely compromises the physical security performance of BR HBC. However, shielding the transmitter with Faraday fabric greatly weakens the leakage signal while keeping the on-body received power well above the leakage around the BR peak frequencies, as shown in Fig. 1 (b). This paper for the first time explores the physical security problem of the BR HBC and proposes an effective shielding method to enable a physically secure BR HBC system.

II. Measurement Setup and Procedure

A. Measurement Setup

The transmitter is the RF Explorer signal generator (RFE6GRN) with a frequency range of 24 MHz $\sim$ 6 GHz with a step of 1 kHz. Around -1 dBm output power with $\sim$0.8 V peak-to-peak voltage is used, which satisfies the safety limits from the International Commission on Non-ionizing Radiation Protection (ICNIRP). The receiver is the handheld RF Explorer spectrum analyzer (WSUB1G+) covering from 50 kHz to 960 MHz. Before the receiver, a BUF602 buffer is used to which provides a high and capacitive receiver termination. The electrodes are connected to the device through short SMA cables to prevent excessive radiation from the cable. The contact between the subject hand and the grounded metallic cases of the devices is also prevented. Both devices are calibrated with the benchtop Keysight signal generator and spectrum analyzer. The shield is made of the Titan Faraday fabric, which can block the signal from low MHz to 40 GHz. The transmitter and the electrode are both shielded with four layers of Faraday fabric in the experiments with the shielded transmitter, as shown in Fig. 2 (b and d). In the on-body experiments, both transmitter and receiver are worn on the wrist of the subject while in the experiment with the off-body receiver, the transmitter is worn on the wrist of the subject while the receiver is placed on the stools to keep the same height with the transmitter, as shown in Fig. 2 (e).

B. Measurement Procedure

1) On-body experiments: During the experiments with both on-body transmitter and receiver, the TX to RX distances d_1 of 10 cm is used. At each distance, the frequencies are swept from 30 MHz to 300 MHz with a step of 10 MHz. Both the unshielded transmitter (Fig. 2 (a)) and the shielded transmitter (in Fig. 2 (b)) are used in the experiments. Each measurement is repeated thrice, and the average value is used to plot the curve, and the maximum and minimum values at each measurement point are used to plot the error bars.

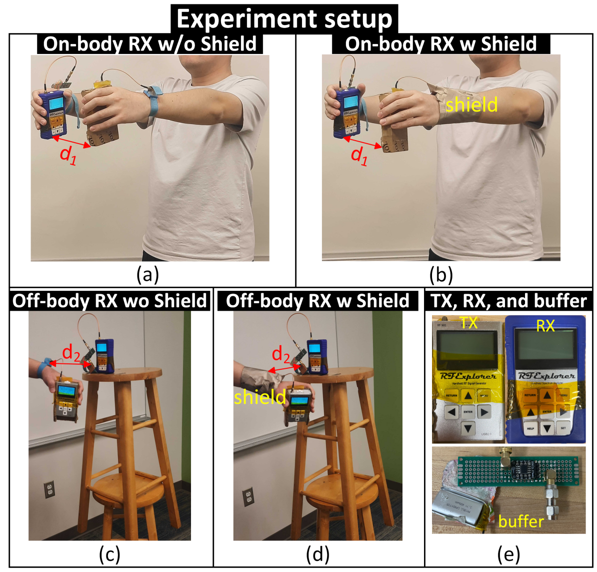

Fig. 2: Experiment setup. (a) On-body receiver with the unshielded TX. (b) On-body receiver with the shielded TX. (c) Off-body receiver with unshielded TX. (d) Off-body receiver with shielded TX. (e) Off-body receiver placed on stools

2) On-body to off-body experiments: During the experiment with the unshielded on-body transmitter and off-body receiver, the TX to RX distances d_2 of 10 cm to 30 cm with a step of 10 cm are used. For the experiments with the shielded on-body transmitter, the same distances are used. Same as on-body experiments, each measurement is repeated three times for average values and error bars.

III. Measurement Results

A. BR HBC Leakage

Fig. 3 shows detected leakage power at the transmitter-body interface with and without the shield at the distances of 10$\sim$30 cm. At 10 cm, due to very strong near-field inter-device coupling, the detected leakage power is very strong, and the channel gain can reach as high as -31.56 dB at 140 MHz while at most frequencies, the channel gain is above -50 dB. Similarly at 20 cm and 30 cm, the channel gains are generally above -60 dB when the frequency is larger than 100 MHz. These make the leakage signal well above the noise floor and easily hacked or eavesdropped, which greatly compromises the physical security of the BR HBC system. Compared with the transmitter shielded with the Faraday fabric, at 10 cm, the leakage power with the unshielded transmitter is reduced by 23.1$\sim$48.6 dB, which provides great benefit for the physical security performance. With the distance increasing, the received powers go below the noise floor (indicated by the red dashed line shown in Fig. 3) at more frequencies.

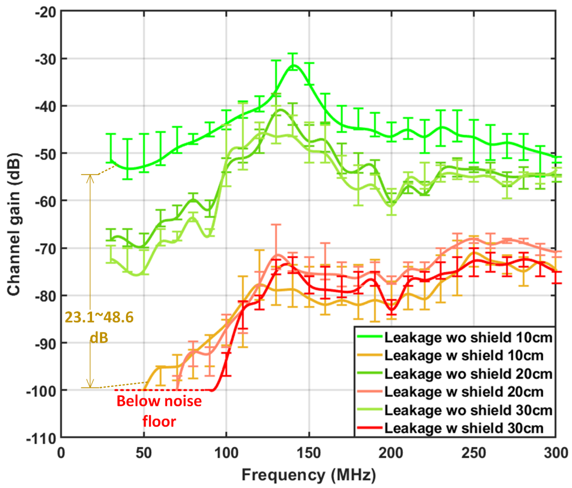

Fig. 3: Measurement results of the transmitter-body interface leakage with and without the shield. The top three green curves are leakage channel gain with unshielded TX while the bottom three curves in red are that with shielded TX.

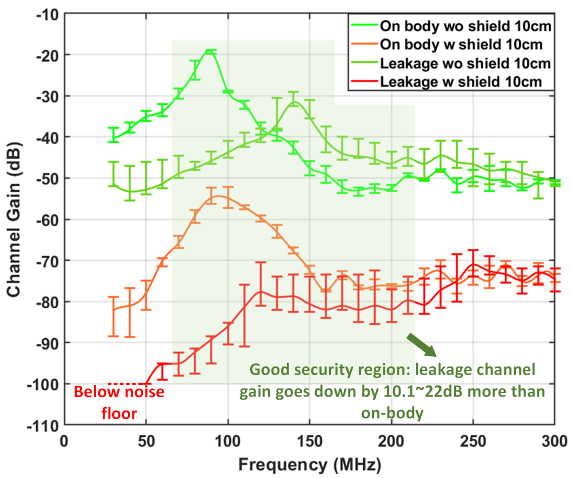

Fig. 4: Measurement results with on-body TX and RX with and without the shield (top two curves) compared with that with and without the shield (bottom two curves).

B. Measurement with on-body TX and RX

Fig. 4 shows the influence of the Faraday fabric shield on the channel gain of the BR HBC system with the on-body transmitter and receiver, as well as the comparison of the received signal powers by the on-body receiver and off-body receiver (leakage) at the same distance of 10 cm. Firstly, comparing the on-body measurement with the unshielded transmitter and the leakage with the shielded transmitter at 10 cm, the power of the received signal by the on-body receiver is much larger than the leakage (up to 70 dB at 90 MHz). Then with the shielded transmitter, the channel gain of the on-body receiver scenario is reduced by up to 20.41∼40.88 dB depending on different frequencies. With the frequency going up, the difference of channel gain reduces. This is the power contributed by the radiation of the transmitter and inter-device coupling. Comparing the on-body measurement and leakage with the shielded transmitter, around the BR peak frequencies, the received power by the on-body receiver is up to 18.07∼34.4 dB larger than the 10 cm leakage. However, beyond the BR peak frequencies, the received power of the on-body receiver is getting close to or even up to -2.7 dB (at 150 MHz) lower than the off-body receiver. The leakage channel gain goes down more than the on-body signal over all frequencies. Within the frequency range of 70∼220 MHz, the leakage channel gain goes down by 10.1∼22 dB more than the on-body channel gain, which means the Faraday fabric shield can provide a large security benefit. This region is marked as good security region, as shown in Fig. 4. Around the body resonance peak frequencies (50∼100 MHz), this security benefit (the difference between the reduction of leakage channel gain and that of on-body channel gain) is the largest. This proves around the BR peak frequencies, the human body is resonated by the transmitter so the human body plays a major role in transmitting signals, while beyond that till 300 MHz, the transmitter radiation plays a larger role. Therefore, the BR peak frequencies should be the most physically secure.

IV. Conclusion

This paper for the first time explores the physical security performance of BR HBC and proposes a method with Faraday fabric to effectively shield the BR HBC signal. The results show that the Faraday fabric can significantly reduce leakage, which greatly improves the physical security performance of BR HBC systems. Around the BR peak frequencies with the shielded transmitter, the channel gain of on-body measurements is well above that of off-body measurements.

Acknowledgement

This work was supported by Quasistatics, Inc. under the Grant 40003567.

References

[1] S. Maity *et al.*, "Bodywire: A 6.3-pj/b 30-mb/s 30-db sir-tolerant broadband interference-robust human body communication transceiver using time domain interference rejection," *IEEE Journal of Solid-State Circuits*, vol. 54, no. 10, pp. 2892–2906, 2019.

[2] Q. Huang *et al.*, "Wearable vital signal monitoring prototype based on capacitive body channel communication," in *2022 IEEE-EMBS International Conference on Wearable and Implantable Body Sensor Networks (BSN)*, 2022, pp. 1–5.

[3] N. Fahier *et al.*, "Wearable cardiovascular monitoring system design using human body communication," in *2021 IEEE International Symposium on Circuits and Systems (ISCAS)*, 2021, pp. 1–5.

[4] J. Wang *et al.*, "Wearable ecg based on impulse-radio-type human body communication," *IEEE Transactions on Biomedical Engineering*, vol. 63, no. 9, pp. 1887–1894, 2016.

[5] J. Sakuma *et al.*, "Performance of human body communication-based wearable ecg with capacitive coupling electrodes," *Healthcare Technology Letters*, vol. 3, no. 3, pp. 222–225, 2016. [Online]. Available: https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/htl.2016.0023

[6] D. Yang *et al.*, "Physically secure wearable–wearable through-body interhuman body communication," *Frontiers in Electronics*, vol. 2, p. 807051, 2022.

[7] D. Das *et al.*, "Enabling covert body area network using electro-quasistatic human body communication," *Scientific reports*, vol. 9, no. 1, p. 4160, 2019.

[8] M. Nath *et al.*, "Inter-body coupling in electro-quasistatic human body communication: Theory and analysis of security and interference properties," *Scientific Reports*, vol. 11, no. 1, p. 4378, 2021.