# On the Negatively Correlated Eavesdropper in Indoor Wireless Body Area Networks

Ruslan Dautov* and Gill Tsouri†
Communications Laboratory
Department of Electrical and Microelectronic Engineering, Rochester Institute of Technology
Rochester, NY, USA
Email: *rid6541@rit.edu, †grteee@rit.edu

***Abstract*—Wireless Physical Layer Security (WPLS) provides attractive lightweight data security methods suitable for resource constrained Wireless Body Area Networks (WBANs). As WPLS methods entirely rely on wireless transmission, they are prone to eavesdropping. Most previous work assume that the eavesdropper's channel is independent if it is more than half a wavelength away from the legitimate participants. In this paper, we demonstrate that due to unique properties of WBANs, this assumption does not hold. In particular, the body shadowing phenomenon gives rise to negative correlation that can be easily exploited by the eavesdropper without being anywhere near the legitimate parties.**

***Index Terms*—Wireless Body Area Networks, Physical Layer Security, Body Shadowing**

## I. Introduction

In many cases, Wireless Body Area Networsk (WBANs) perform critical tasks by monitoring health conditions and facilitating medical diagnosis. In this context, data security must be an integral part of data transmission. Traditional encryption methods such as Advanced Encryption Standard (AES) [1] or Rivest Shamir Adleman (RSA) [2] were designed for systems with abundant computational power and may be of burden for resource constrained WBAN applications.

Wireless Physical Layer Security (WPLS) [3], [4] is an alternative to the aforementioned algorithms. WPLS is more computationally efficient and is capable of providing theoretical secrecy. However, as WPLS solely relies on the wireless channel, it is vulnerable to passive eavesdropping [5]. A commonly made assumption in past work is that the eavesdropper's channel Z is independent of the channel established by the legitimate participants A and B if the eavesdropper is at least half a wavelength away from them. In mathematical terms it can be expressed using Mutual Information (MI):

$$I(A, B|Z) = I(A, B) \tag{1}$$

where left hand side is a conditional mutual information. This assumption has been questioned previously in [5], [6]. Multiple experimental studies in [5] revealed that under typical propagation conditions of residential, confined office or open outdoor environment, there are many occasions when the aforementioned assumption does not hold. The work in [6] proposed a correlation attack that exploits channel correlation. It showed through analysis and experimental validation that it is possible for the eavesdropper to extract a close replica of the legitimate channel.

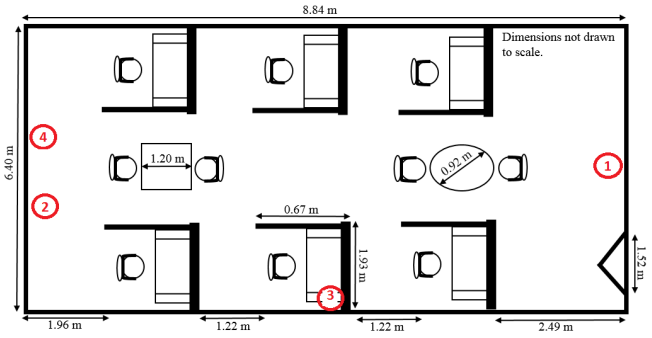


Fig. 1. Indoor experimental environment with sensors placement

Contrary to past work, in this paper we challenge the assumption given by (1) from WBAN perspective. We demonstrate that unique propagation conditions caused by the presence of a human body can be exploited by the eavesdropper to gain information about the legitimate channel. To the best of our knowledge, this is the first effort to investigate the implications of negative correlation on security in WBANs.

## II. Experimental Setup

We use experiment to provide a validation of a negatively correlated eavesdropper in WBANs. To show how much information the attacker can gain, MI is evaluated using the Kraskov Stoegbauer Grassberger (KSG) estimator with local nonuniformity correction as described in [7].

Our experimental study is carried out in a typical office environment with walls, chairs, desks, computers and laboratory equipment providing rich scatters. The layout of the room is presented in Fig. 1. We employ TeloSB platform that is based on a TI MSP430 micro controller and a IEEE compliant Chipcon CC2420 RF tranceiver utilizing 2.4 GHz ISM band. The network in consideration consists of five sensors one of which serves as an Access Point (AP) using TDMA polling mechanism at a rate of 10-12 packets/sec. All devices are equipped with a trace printed circuit board antenna and configured for 1 mW output power. The platform provides digital Received Signal Strength Indicator (RSSI)

978-1-5386-5553-5/19/$31.00 ©2019 IEEE

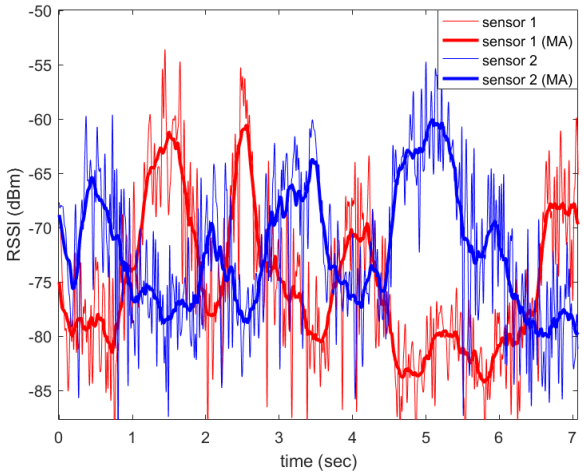


Fig. 2. Experimental data with 200 msec moving average applied

also available in most commercial RF systems currently on the market. Direct Sequence Spread Spectrum (DSSS) baseband modem allows for data rates up to 250 kb/sec.

In the experiment, the AP is located on the subject's chest. The subject is a 90 kg weight and 177 cm tall male. Four sensors are placed at different locations around the room depicted in Fig. 1 by circles. All devices are approximately 1.5 meters above the floor. In this scenario, we treat the AP and sensor 2 as legitimate participants, while the rest act as passive eavesdroppers. During data collection, the subject casually walks around the room in a random fashion. On average 10,000 RSSI samples are collected for every sensor in this experiment. After gathering, data is taken off line for processing and analysis.

## III. Results and Discussion

Table I reports correlation coefficient and MI between all 4 sensors in our experiment. MI is given in parenthesis. Diagonal entries in the table represent channel entropy - upper bound on MI. In real settings, the upper bound is unachievable due to non simultaneous channel estimation. However, for simplicity, we will assume that the channel between the AP and sensor 2 is perfect and maximum MI is obtained. As all devices operate in similar conditions, their entropies are approximately the same and equal $\approx$35 bits. From the table it is clear that sensors 2 and 4 are highly correlated with positive correlation coefficient $\rho = 0.51$, whereas sensors 2 and 1 have noticeable negative correlation of $\rho = -0.28$. At the same time, sensor 3 is almost completely uncorrelated with sensor 2 with $\rho = 0.05$. Although the fact of having strong positive correlation is interesting, the cause of it is due to proximity and has been discussed before in [5], [6].

In this paper we focus on negative correlation as it occurs naturally in WBANs. The reason behind it is another phenomenon named body shadowing - full or partial obstruction of the Line of Sight (LoS) between transmitter and receiver. Thus, when the subject (with AP on his chest) is facing sensor 1, the RSSI is stronger due to presence of LoS. At the same time, sensor 2 is shadowed by the body resulting in weak reception. Consequently, when one of the sensors experiences favorable channel conditions, another is likely to experience channel degradation. This fact is supported by experimental results reported in Fig. 2. This figure presents RSSI values gathered from sensor 1 and 2 for the duration of approximately 7 seconds. As a commonly used preprocessing step, low pass filter in the form of 200 msec Moving Average (MA) is also applied to both RSSI streams. It can be clearly seen that two sensors are inversely related. When RSSI of one sensor is on the rise, another sensor's RSSI is falling and vice versa.

TABLE I
Correlation and Mutual Information of Experimental Data

| | **sensor 1** | **sensor 2** | **sensor 3** | **sensor 4** |
|---|---|---|---|---|
| **sensor 1** | 1 (34.55) | -0.28 (0.18) | -0.07 (0.05) | -0.24 (0.14) |
| **sensor 2** | -0.28 (0.18) | 1 (35.72) | 0.05 (0.08) | 0.51 (0.29) |
| **sensor 3** | -0.07 (0.05) | 0.05 (0.08) | 1 (35.56) | -0.01 (0.06) |
| **sensor 4** | -0.24 (0.14) | 0.51 (0.29) | -0.01 (0.06) | 1 (35.77) |

## IV. Conclusion

In this paper, we explored the implications of negative correlation on physical layer security in indoor WBANs. Through experimental validation we showed that under certain circumstances negative correlation occurs naturally due to body shadowing phenomenon and with carefully chosen location can be exploited by a passive eavesdropper. More importantly, we demonstrated that in presence of negative correlation, commonly accepted assumption that Eve's channel is independent, given sufficient distance from the legitimate participants, does not hold. In fact, negatively correlated attacker can be located on the opposite wall to the legitimate party and still gain some knowledge of the channel.

As experimental work is inherently limited, our future efforts will extend to simulations in order to provide more thorough consideration of the problem, and analyze the implications of negative correlation on the practical key extraction algorithms.

## References

[1] J. Daemen and V. Rijmen, *The design of Rijndael: AES-the advanced encryption standard*. Springer Science & Business Media, 2013.

[2] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[3] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. i. secret sharing," *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1121–1132, 1993.

[4] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE transactions on information theory*, vol. 39, no. 3, pp. 733–742, 1993.

[5] M. Edman, A. Kiayias, and B. Yener, "On passive inference attacks against physical-layer key extraction?" in *Proceedings of the Fourth European Workshop on System Security*. ACM, 2011, p. 8.

[6] X. He, H. Dai, W. Shen, and P. Ning, "Is link signature dependable for wireless security?" in *2013 Proceedings IEEE INFOCOM*, April 2013, pp. 200–204.

[7] S. Gao, G. Ver Steeg, and A. Galstyan, "Efficient estimation of mutual information for strongly dependent variables," in *Artificial Intelligence and Statistics*, 2015, pp. 277–286.