RSS-based Secret Key Generation for Indoor and Outdoor WBANs using On-Body Sensor Nodes

Thijs Castel, Patrick Van Torre, Hendrik Rogier
INTEC Department
iMinds/Ghent University
Ghent, Belgium
thijs.castel@intec.ugent.be

***Abstract*—Given that the market of wearables is in so-called hypergrowth mode, more and more of these on-body devices will interact with each other. These body-to-body, device-to-device links should not only provide reliable but also secure communication of personal user data. Therefore, we have analyzed the potential of using the unique reciprocal body-to-body channel between two legitimate parties, to create a high-level security key that is unknown to an eavesdropper. Both randomly moving legitimate parties, typically called Alice and Bob, were equipped with low-power wireless on-body sensor nodes, which collect the Received Signal Strength values. Additionally, the eavesdropper Eve, who is continuously sniffing the body-to-body channel using a third sensor node, collects her own sequence of RSS values, which are expected to be highly decorrelated from the RSS values from both Alice and Bob. Based on a statistical analysis, applied to Received Signal Strength values to verify the correlation, entropy and mutual information, the body-to-body link seems very suitable for RSS-based secret key generation in indoor and outdoor Wireless Body Area Networks. Moreover, this practical and lightweight alternative for secret key generation ensures low on-chip complexity and, hence, low computational power consumption.**

I. Introduction

In the near future, people will be connected to the internet through multiple wearables which could autonomously communicate personal data towards desired recipients, creating the Internet of People (IoP) [1], [2]. These new Wireless Body Area Networks (WBANs) will go hand in hand with the Internet of Things (IoT) concerning healthcare, fitness monitoring and lifestyle computing [3]. Of course, for users' safety and privacy, data protection is necessary to prevent that intruders could access personal, and hence, sensitive data when wireless data transfer is in progress. Moreover, since power consumption is crucial for on-body devices, the proposed secret key generation algorithm should require low computational complexity with limited memory size and bandwidth [4]. Therefore, the unique characteristics of the underlying reciprocal body-to-body channel between two mobile legitimate parties are exploited to generate joint randomness between both.

We have performed several mobile body-to-body (Alice-to-Bob and vice versa) measurements at indoor and outdoor locations, with a passive stationary eavesdropper (Eve) in the vicinity of both Alice and Bob. The legitimate parties, Alice and Bob, are equipped with low-power wireless nodes, placed upon the human body, to set up autonomous communication towards each other. Moreover, we assume that the passive eavesdropper, represented by a third wireless node, is only capable of calculating the Received Signal Strength (RSS) from intercepted packets sent by Alice or Bob. If Alice transmits a packet towards Bob and Bob retransmits a packet towards Alice within the coherence time of a fast fluctuating wireless body-to-body channel, the RSS at Alice and Bob is expected to be approximately equal owing to reciprocity. In contrast, the RSS at the eavesdropper is expected to be significantly different or decorrelated from the quasi-equal RSS values received by Alice and/or Bob. These unique streams of RSS values at both legitimate parties could further be used to generate a secret key, which is unknown for an intruder. The collected RSS sequences are suitable for secret key generation if the entropy and the Mutual Information (MI) between both legitimate parties are high, whereas the mutual information between a legitimate user and an eavesdropper should be low. For an intruder, this complicates deciphering the secret key and, hence, maximizes data security. Therefore, we have analyzed the correlation, entropy and mutual information of all collected RSS sequences, for three indoor and four outdoor measurement scenarios, indicating the potential to use unique RSS sequences for secret key generation.

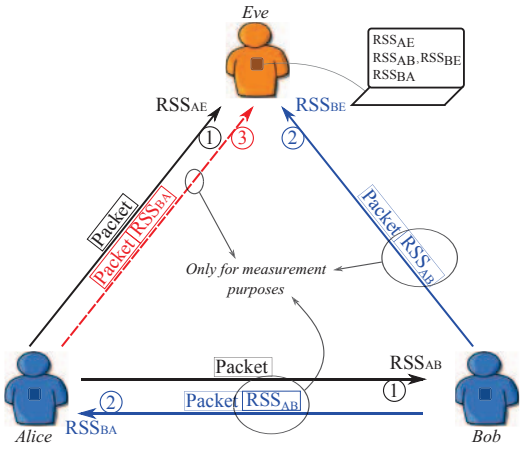

Fig. 1. Measurement principle. The value RSS_{AB} and the transmission from Alice to Eve that includes RSS_{BA} are only included for measurement purposes and not for the actual applications.

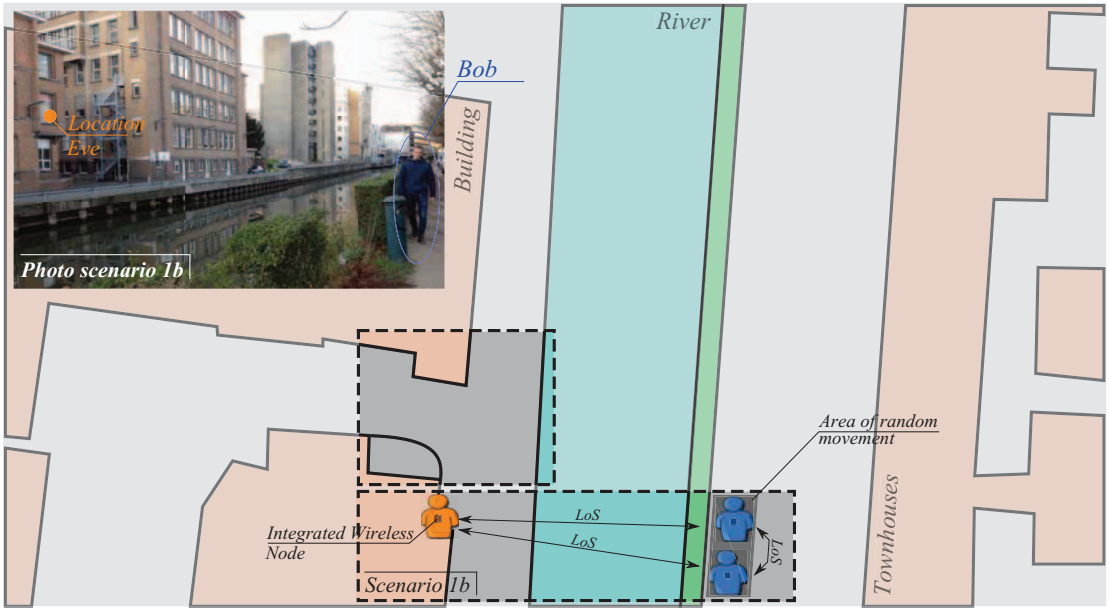

Fig. 2. Outdoor measurement location and measurement scenario 1b. The top left photo, included to provide more insight into the outdoor measurent location, was taken by Alice during measurement scenario 1b. Note that the on-body sensor node is covered by Bob's jacket

To the authors' best knowledge, this is the first work where fully-autonomous low-power nodes were placed upon the human body for RSS-based secret key generation, between two moving legitimate parties in the presence of a stationary eavesdropper, and where the quality of the key was validated based on indoor and outdoor measurements. Despite the fact that this is a relative new research domain, J. Jenssen et al. have already presented interesting work concerning secret key generation based on RSS values, albeit not in a body-centric context. Linked to our work, [5] explores the effectiveness of using highly reconfigurable antennas to generate varying channels which are used to establish secret encryption keys. Additionally, [6] shows that sufficient (and random) movement is necessary to generate high entropy keys between two mobile devices.

The paper is further organized as follows. Section 2 describes the measurement setup, scenario and location, Section 3 presents the statistical results and Section 4 summarizes the main conclusions. Finally, in Section 5, we outline potential future work since this work is only the (fundamental) beginning of RSS-based secret key generation for indoor and outdoor WBANs using on-body sensor nodes.

II. Measurement Setup

Wireless on-body sensor nodes, composed of a dual-polarized textile patch antenna that serves as a platform for the flexible electronic circuits, were deployed on the bodies of test persons [7]. The on-body sensor nodes placed upon Alice and Bob operated fully-autonomous while Eve's on-body sensor nodes was connected to a laptop, which was used as the central storage for all RSS values of one measurement: RSS from Alice to Bob (RSS_{AB}), RSS from Bob to Alice (RSS_{BA}), RSS from Alice to Eve (RSS_{AE}) and RSS from Bob to Eve (RSS_{BE}). As visualized in Fig. 1, the dedicated embedded software was programmed as follows:

1) Alice transmit a packet towards Bob who calculates RSS_{AB}. Moreover, the packet is also received by Eve who calculates (and saves) RSS_{AE}.
2) Bob retransmits a packet towards Alice, who calculates RSS_{BA}, and he includes, only for measurement purposes and not in the actual application, RSS_{AB}. Additionally, the retransmitted packet is received by Eve, who calculates RSS_{BE} and saves both RSS_{BE} and the included RSS_{BA} on the laptop.
3) For measurement purposes only and not in the actual application, Alice retransmit a packet which includes RSS_{BA} towards Eve, who stores this value on the laptop.

Of course, in real-life scenarios, Alice and Bob do not (re)transmit packets which include RSS_{AB} or RSS_{BA} because the secret key generation is based on these unique values. However, since only Eve could save the RSS values on the laptop, this was necessary for measurement purposes.

Three measurement scenarios, with legitimate parties Alice and Bob simultaneously moving around in the presence of a stationary eavesdropper Eve, were performed at an indoor and outdoor location. At the indoor office location, a lot of potential reflectors and scatterers were present in the close vicinity of Alice, Bob and Eve. In contrast, at the urban outdoor location, all three parties were surrounded by high buildings, on the one side, and high townhouses, at the opposite side of the river, as shown in Fig. 2. In the first and second scenario, Alice and Bob, randomly moving around, remained in Line-of-Sight (LoS) of each other, as shown in Fig. 3. However, in the first scenario, Eve is visible to both

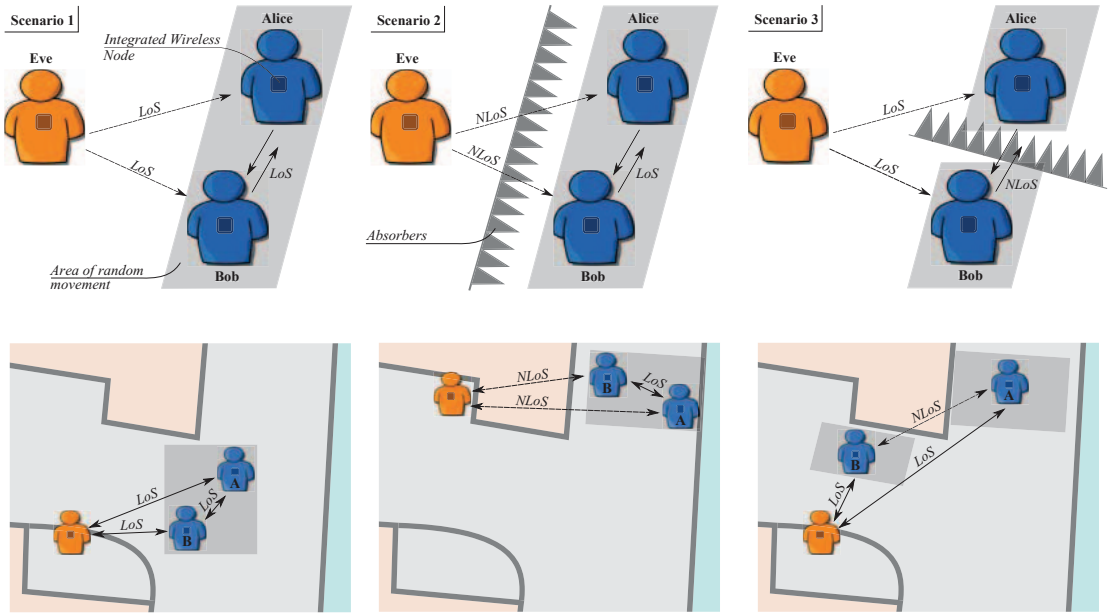

Fig. 3. Measurement scenarios 1, 2 and 3, for both the indoor and outdoor measurement locations. Note that outdoor scenario 1b is depicted in Fig. 2.

Alice and Bob whereas, in the second scenario, Eve is at a Non-Line-of-Sight (NLoS) position from Alice and Bob. In the third scenario, Eve is visible to both Alice and Bob, who do not see each other. Furthermore, one additional outdoor measurement, corresponding to scenario 1b as shown in Fig. 2, was performed with Alice and Bob, being in each other's LoS, randomly moving around at the opposite side of the river with a Line-of-Sight link towards Eve.

For one measurement scenario, we gathered one set of four RSS values every 100 milliseconds for a total of 15.000 sets of RSS values. If the received RSS value, further digitized in an 8 bit value, was below the detection limit of the on-body sensor, the value was dropped and a new packet was sent by Alice to gather 15.000 reliable sets of RSS values. Note that the delay between transmission from Alice and retransmission from Bob was only 5 milliseconds, and hence within the coherence time of the channel, which is equal to 10 milliseconds.

III. Results

A. Envelope Correlation

To create a highly-reliable security key from the RSS values, the envelope correlation ρ between RSS_{AB} and RSS_{BA} should be high whereas the signal strengths, received by Eve, should be sufficiently decorrelated from RSS_{AB} and RSS_{BA}.

With $\mathbf{X}$ and $\mathbf{Y}$, being vectors containing 15.000 RSS samples (in dBm), the envelope correlation is calculated as

$$\rho_{\mathbf{X},\mathbf{Y}} = \frac{E(\mathbf{X}\cdot\mathbf{Y}) - E(\mathbf{X})E(\mathbf{Y})}{\sqrt{\left[E(\mathbf{X}^2) - (E(\mathbf{X}))^2\right]\left[E(\mathbf{Y}^2) - (E(\mathbf{Y}))^2\right]}}. \quad (1)$$

As seen in Table I, which presents the envelope correlation ρ for all measurement scenarios at both the indoor and outdoor measurement locations, the correlation between AB-BA is significantly higher than the correlation with RSS values received by Eve. This indicates that the received signal strength values may be used to generate a high-level security key.

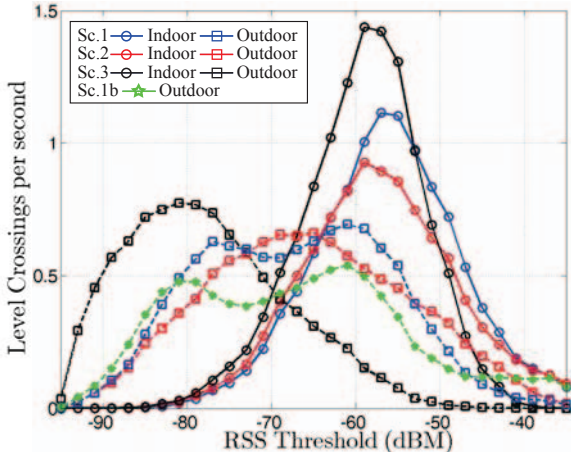

Fig. 4. Level Crossing Rate (LCR) for the Alice-to-Bob link

At the indoor measurement location, a large number of potential reflectors are in the close proximity of Alice and Bob. In contrast, at the outdoor locations, the potential scatterers contributing to the received signal at Alice or Bob are further away from both legitimate parties. This implies that, when both Alice and Bob are simultaneously and randomly moving around, the indoor body-to-body channel could vary faster, compared to the outdoor body-to-body channel. For the Alice-Bob link, this is verified by means of the Level Crossing Rate (LCR), as visualized in Figure 4. Additionally, the faster varying indoor body-to-body links decrease the coherence time

and, hence, increase the probability that RSS_{AB} and RSS_{BA} exhibit, to a small extent, more decorrelation within the round-trip time between Alice and Bob. Moreover, when focusing on the indoor measurements, the correlation between RSS_{AB} and RSS_{BA} is the smallest for scenario 3, because of the faster varying channel, compared to scenarios 1 and 2, as shown in Fig. 4. Given the NLoS link between Alice and Bob in scenario 3, the correlation with Eve is somewhat higher at both the indoor and outdoor locations, because communication between Alice and Bob only happens via reflectors, which may be in the close vicinity of Eve. Additionally, for outdoor scenarios 1 and 3, the correlation between AB-AE (and BA-AE) is unexpectedly higher than the correlation between AB-BE (and BA-BE). This could be caused by the fact that, during the (non-perfect) random walks, Bob was regularly standing closer to Eve, compared to Alice. This increases correlation between the Alice-Eve link and the Bob-Alice (and vice versa) link. However, the correlation is still significantly lower than the correlation between Alice and Bob. In contrast, this phenomenon is not noticeable for scenario 1b where the distances Eve-Alice and Eve-Bob were approximately equal during the complete measurement.

TABLE I
ENVELOPE CORRELATION

Link	Indoor			Outdoor			
	1	2	3	1	1b	2	3
AB-BA	0.878	0.912	0.704	0.970	0.975	0.968	0.984
BA-AE	0.032	-0.039	0.144	0.269	0.059	-0.042	0.390
BA-BE	0.044	0.034	0.141	0.077	0.099	-0.073	0.152
AB-AE	0.031	-0.037	0.138	0.270	0.062	-0.040	0.391
AB-BE	0.051	0.020	0.124	0.078	0.063	-0.073	0.149
AE-BE	-0.050	-0.024	0.004	-0.063	-0.024	0.039	-0.064

B. Entropy

The entropy indicates how many bits of the 8 bit RSS value could be used to generate a safe key towards intruders. It is calculated as

$$\mathrm{H}(\mathbf{X}) = \sum_{i=1}^{N} P(\mathbf{X}_i) \cdot \log_2\Big(P(\mathbf{X}_i)\Big). \tag{2}$$

In an ideal situation, all RSS values, within the detection range of the receiver, have equal probability for every consecutive measurement. Theoretically, this corresponds to maximum entropy equal to 8 bits. For the on-body sensors nodes, the detection limit is equal to -95 dBm whereas the saturation limit equals -35 dBm. This sets the maximal entropy equal to $\log_2(60)$ = 5.90 bits, when all RSS values would have the same probability. However, since we are performing real-life measurements, the Most Significant Bits (MSBs) of the 8 bit RSS value will vary slower than the Least Significant Bit (LSBs), and are therefore more predictable. This implies that data, secured with these MSBs, is easier to decipher by an eavesdropper. Therefore, the bits that do not vary fast enough over time are not used to generate secret keys. The calculated entropy, presented in Table II, shows that $\mathrm{H}(\mathbf{X}) \in [4.765, 5.399]$ bits or $\mathrm{H}(\mathbf{X}) \in [5.295, 5.796]$ bits for the indoor and outdoor location, respectively.

TABLE II
ENTROPY (BIT)

Link	Indoor			Outdoor			
	1	2	3	1	1b	2	3
AB	5.248	5.391	4.765	5.551	5.796	5.633	5.297
BA	5.234	5.399	4.782	5.547	5.790	5.637	5.295

Table II also indicates smaller entropy when Alice and Bob are inside. As described before, at the indoor measurement location, a large number of possible reflectors are in the close proximity of Alice and Bob. Moreover, these reflectors are not only present on few specific locations, as for the outdoor scenario, but over the full 360° range around Alice and Bob. This implies that, during most of the time, many multipath components contribute to the RSS values, at Alice or Bob, which leads to a narrower RSS distribution for the indoor measurement scenario, as visualized in Fig. 5 for measurement scenario 3. In contrast, the potential reflectors at the outdoor measurement locations are not equally distributed around Alice and Bob. This implies that the RSS values could fluctuate more, heavily depending on the orientation of both Alice and Bob, because the number of arriving multipaths varies over time. This leads to a broader RSS range, as visualized in Fig. 5, and, hence, a higher entropy.

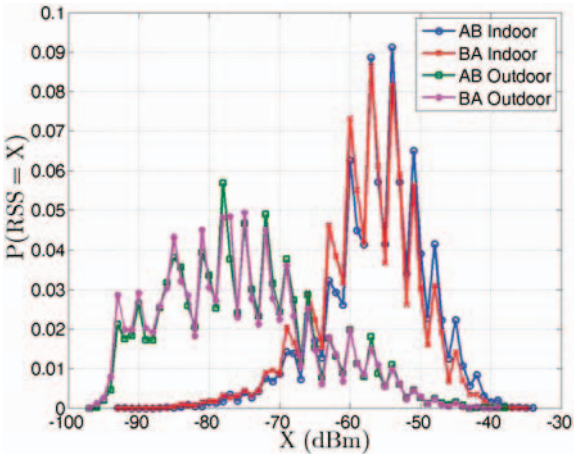

Fig. 5. RSS distribution for scenario 3 at both the indoor and outdoor measurement location

C. Mutual Information

Next to the correlation and the entropy, the mutual information is the third statistical parameter which indicates the potential strength of a secret key. The MI depends on the correlation and the entropy and is calculated as

$$\mathrm{MI}(\mathbf{X},\mathbf{Y}) = \sum_{i=1}^{N}\sum_{j=1}^{N} P(\mathbf{X}_i,\mathbf{Y}_j)\cdot\log_2\left(\frac{P(\mathbf{X}_i,\mathbf{Y}_j)}{P(\mathbf{X}_i)\cdot P(\mathbf{Y}_j)}\right). \tag{3}$$

The mutual information indicates how many information bits of the 8 bit RSS_{AB} can be estimated if the 8 bit RSS_{BA} value is known, or vice versa. It measures how the knowledge of RSS_{AB} reduces uncertainity about RSS_{BA}. Similar to the correlation, the mutual information should be high between RSS_{AB} and RSS_{BA} and low between $RSS_{AB,BA}$ and a potential eavesdropper. However, only a high correlation is not sufficient to guarantee high-level secret key. The combination of high correlation and low entropy, as for static body-to-body measurements, results in low MI. In contrast, if both the correlation and entropy are high, the mutual information is high, as for the AB-BA link in outdoor scenario 3, according to Table III.

TABLE III
MUTUAL INFORMATION (BIT)

Link	Indoor			Outdoor			
	1	2	3	1	1b	2	3
AB-BA	1.398	1.572	0.667	2.386	2.535	2.440	3.053
BA-AE	0.139	0.113	0.108	0.216	0.149	0.096	0.266
BA-BE	0.120	0.110	0.112	0.190	0.172	0.169	0.154
AB-AE	0.133	0.110	0.110	0.214	0.152	0.097	0.261
AB-BE	0.118	0.114	0.108	0.193	0.170	0.173	0.158
AE-BE	0.093	0.700	0.083	0.146	0.084	0.070	0.122

Table III indicates that at least one secret key bit, which will be the same at Alice and Bob, can be generated out of the 8 bit RSS value. However, this will be more difficult for the indoor scenario 3 where Eve is visible for both Alice and Bob, who do not see each other. Because of the fast(er) varying body-to-body channel in this specific scenario, the correlation and, hence, MI between RSS_{AB} and RSS_{BA} is lower. However, the correlation is expected to be higher if the round-trip time between Alice and Bob could be decreased. The mutual information shared with Eve is, in all scenarios, significantly lower than the mutual information between legitimate parties Alice and Bob. This implies that, even when the MI equals (maximally) 0.266 as in outdoor scenario 3, Eve is not able to estimate one secret bit that is shared by Alice and Bob [8]. Therefore, the unique received RSS sequences at Alice and Bob are proven very suitable for secret key generation for both indoor and outdoor WBANs.

IV. CONCLUSIONS

In this work, we have analyzed the correlation, entropy and mutual information of RSS streams, collected using wireless on-body sensor nodes, between two mobile legitimate parties, Alice and Bob, and a stationary evesdropper, Eve. These statistics, calculated for three indoor and four outdoor measurements, show that stream of RSS values could be used to create joint randomness between two mobile legitimate parties, Alice and Bob. The generated secret key will be (largely) unknown to a stationary intruder, called Eve, owing to the significantly smaller mutual information between the RSS values, received by Alice of Bob, and the RSS values received by Eve. Moreover, the mutual information between Alice and Bob is maximized when both the correlation and entropy are high. From our measurements, higher correlation is obtained for the outdoor measurement scenarios because of the smaller level crossing rate, indicating a larger coherence time. However, correlation in the indoor scenarios is expected to be higher if the round-trip time between Alice and Bob could be decreased. Additionally, due to the non-uniform distribution of potential scatterers in close vicinity of Alice and Bob in the outdoor measurement scenario, the distribution of the RSS values between two legitimate parties is broader, compared to the indoor RSS values for the same measurement scenario. This implies that outdoor locations could introduce higher entropy, compared to indoor scenarios, which lead to a higher mutual information, assuming high correlation.

V. FUTURE WORK

Future work involves the implementation of the following three algorithms to extract a high-level secret keys, with high randomness, out of the RSS streams between Alice and Bob [5], as also described in [8] for our indoor measurement scenarios. First, *data quantization* drops RSS values probabilistically, located between the RSS mean and the RSS mean $\pm$ threshold, to introduce higher entropy. This compensates for assymetric system parameters, such as a slightly different transmit power or receiver noise floor, at Alice and Bob. Next, *data reconciliation*, potentially implemented by an (X,Y) Hamming-code, ensures that the secret key, generated at both legitimate parties, is equal. Finally, *privacy amplification*, based on the 'leftover hash lemma' can be used to extract higher entropy secret keys when the output of the quantizer produces low(er) entropy keys. Additionally, this work can further be extended by measurements that consider a *mobile* eavesdropper, placed on Bob's (or Alice's) body, corresponding to the worst case scenario.

REFERENCES

[1] J. Miranda, N. Makitalo, J. Garcia-Alonso, J. Berrocal, T. Mikkonen, C. Canal, and J. Murillo, "From the Internet of Things to the Internet of People," *Internet Computing, IEEE*, vol. 19, no. 2, pp. 40–47, March 2015.

[2] T. Vilarinho, B. Farshchian, J. Floch, and B. Mathisen, "A Communication Framework for the Internet of People and Things Based on the Concept of Activity Feeds in Social Computing," in *9th International Conference on Intelligent Environments (IE)*, July 2013, pp. 1–8.

[3] J. Wei, "How Wearables Intersect with the Cloud and the Internet of Things : Considerations for the developers of wearables," *Consumer Electronics Magazine, IEEE*, vol. 3, no. 3, pp. 53–56, July 2014.

[4] G. R. Tsouri and J. Wilczewski, "Reliable Symmetric Key Generation for Body Area Networks Using Wireless Physical Layer Security in the Presence of an On-body Eavesdropper," in *Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL)*, 2011, pp. 153:1–153:6.

[5] R. Mehmood, J. Wallace, and M. Jensen, "Key establishment employing reconfigurable antennas: Impact of antenna complexity," *Wireless Communications, IEEE Transactions on*, vol. 13, no. 11, pp. 6300–6310, November 2014.

[6] S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "Secret Key Extraction from Wireless Signal Strength in Real Environments," *Mobile Computing, IEEE Transactions on*, vol. 12, no. 5, pp. 917–930, May 2013.

[7] P. Vanveerdeghem, P. Van Torre, C. Stevens, J. Knockaert, and H. Rogier, "Synchronous Wearable Wireless Body Sensor Network Composed of Autonomous Textile Nodes," *Sensors*, vol. 14, no. 10, pp. 18 583–18 610, 2014.

[8] P. Van Torre, T. Castel, and H. Rogier, "Encrypted Body-to-Body Wireless Sensor Node Employing Channel-State-Based Key Generation," in *Submitted for EUCAP 2016*.