DLINK: Dual Link Based Radio Frequency Fingerprinting for Wearable Devices

Girish Revadigar*†, Chitra Javali*†, Wen Hu*, and Sanjay Jha*
*School of Computer Science and Engg. UNSW Australia, Sydney, Australia
†National ICT Australia (NICTA), Sydney, Australia‡
Email: {girishr, chitraj, wenh, sanjay}@cse.unsw.edu.au

***Abstract*—Exploiting unique wireless channel characteristics like signal strength for secret key generation has been recently studied by researchers. These schemes are lightweight and suitable for resource constrained wearable devices. However, a major drawback of existing schemes is that the successive channel samples with small sampling interval will have high correlation in time. This reduces the entropy and bit rate of keys. In this paper, we present dual-link based Radio Frequency fingerprinting solution – DLINK, which dynamically identifies the suitable multipath link to generate secret keys with improved entropy and bit rate in fast as well as slow fading channel conditions. We conduct an extensive set of experiments with real sensor devices mounted on subjects in multiple indoor environments. Our results show that, DLINK reduces the correlation of successive channel samples by 67%, and has 5 times higher bit rate, and improved entropy in all channel conditions compared to existing solutions.**

Keywords*—Wearable devices, Secret key generation, Body Area Networks.

I. Introduction

In recent years, using tiny wearable devices for remote health monitoring and fitness/sports applications is increasing rapidly. A latest report based on market study has predicted that the wearable technology will reach $ 1.6 trillion business in the near future [2]. The devices like FitBit Flex, Nike+ Fuel band measure the person's physiological data, monitor activity and sleep quality, and sync wirelessly to the personal devices/base station (BS). The BS can then upload this data to a cloud based database to facilitate access by the hospital authority or caretakers for timely treatment. Securing the wireless link between wearable device and the BS is very important as the sensitive health related data transmitted is vulnerable to many types of attacks like eavesdropping, tampering the data e.t.c.. The secret keys used by these devices to encrypt the data must be generated dynamically and renewed periodically in order to provide robust security [1]. Key generation mechanisms used in high end systems e.g., Diffie-Hellman, are not feasible for wearable devices which are miniature and severely resource constrained. The security mechanisms for these types of devices should be extremely lightweight.

Recent studies have shown that the fading characteristics of wireless channel between two devices, e.g., received signal strength indicator (RSSI), can be leveraged to extract shared secret keys [10]. Wireless medium has a unique property that the channel characteristics/samples measured between two devices by exchanging a pair of probe packets in quick succession within a few milli seconds, will be nearly the same. The channel variation observed by these two parties by exchanging multiple such packets over a period of time will be highly correlated, which can be used for extracting the secret bits. In contrast, for an adversary located away from legitimate devices at a distance more than half the wavelength of radio signal being used, the channel measurements from overheard packets will be entirely different. The multi-path fading and attenuation factors alter the signal characteristics, and hence the adversary cannot extract the same bits as the two legitimate parties [9].

The important evaluation metrics used for measuring the performance of a key generation scheme are secret bit rate (measured in bps), which explains the number of bits extracted per second, and entropy (measured in bits), which is the measure of randomness of the secret bits. The existing secret key generation mechanisms for wearable devices based on RSSI are suitable only in case of fast fading channel caused during high mobility scenarios, e.g., walking. However, when there is a slow decaying channel, i.e., in the absence of sufficient body movement, the successive channel samples collected by the device cannot produce distinct and statistically independent bits, and produce low bit rate and low entropy keys [16], which poses a serious security threat.

In this work, we propose an RSSI based Radio Frequency (RF) fingerprinting scheme, a.k.a., secret key generation scheme based on dual-antennas architecture which dynamically identifies suitable multipath links with sufficient fluctuation connecting the BS and body-worn device. This improves entropy and bit rate in fast as well as slow fading channel. More than one antenna is commonly used in high end systems like WiFi with multiple input multiple output (MIMO) for better performance. However, using multiple antennas for security on resource constrained devices used in wearable applications is challenging and is not studied in the literature.

Our contributions are:

- We present theoretical analysis of the correlation of (i) channel samples captured by the BS and body-worn device D, and (ii) the successive channel samples at each party, in indoor mobile environments.
- We propose DLINK, dual-antennas based architecture, and demonstrate experimentally that our solution reduces the correlation of successive channel samples captured at the device by 67% compared to prior work.

‡NICTA is funded by the Australian Department of Communications and the Australian Research Council through the ICT Centre of Excellence program.

- We propose a novel dynamic link identification and bit extraction technique to generate secret keys with high entropy and improved bit rate in fast as well as slow fading environments. Our results reveal that DLINK's secrecy capacity is increased by 5 times when compared to existing schemes.

To the best of our knowledge, the work presented in this paper is the first one to propose dual-antennas based RF fingerprinting scheme (for session key generation in indoor mobile environments) on tiny sensor platforms suitable for Body Area Networks (BAN). The rest of the paper is organized as follows: Section II gives brief overview of existing literature. Section III describes our assumptions, adversary model and channel model. The implementation details and experimental set-up are presented in Section IV. We provide the details of our experimental study on decorrelating channel samples in Section V. The protocol design is explained in Section VI. The evaluation of proposed scheme is presented in Section VII, and Section VIII concludes the paper.

II. Related Work

RSSI based secret key generation mechanisms for BAN have been studied in prior work. Authors in [5] have used filtering to reduce the discrepancy between the channel samples at two ends and have proposed a scheme to extract approximately matching keys without using reconciliation methods. However, efficiency of the scheme is platform specific and bit rate is too low (0.14 bps). In ASK-BAN [14], static channel conditions are used for authentication and dynamic channel conditions during body motion are used for secret key generation. ASK-BAN has a maximum bit rate of 8.03 bps during body motion, and has a low bit rate and low entropy in slow fading channel conditions. In [16], researchers have studied the effect of channel hopping on key entropy in fast and slow fading channels. However, the work does not suggest a scheme suitable for practical applications. A limitation of this approach is that, synchronizing the channel hopping at two devices is difficult which leads to lots of packet losses. Since over-the-air packet exchange consumes more power/battery, it is an overhead for resource constrained devices of BAN. Also, fixed channel hopping strategies are not suitable for security in practical applications.

To the best of our knowledge, the most recent protocols SeAK [7] and iARC [12, 13] are the only BAN protocols in the literature which employ dual-antennas. In SeAK, authors use distance bounding protocol to authenticate a new wearable device with an existing BAN. It also generates a secret key which can be used later during communication. Nevertheless, the same mechanism cannot be used for session key renewal. The scheme works only for specific distance, e.g., < 15 cm. In iARC, authors have investigated the feasibility of generating secret keys for body-worn devices in static channel cases, and proposed a mechanism for inducing artificial channel randomness.

RSSI based key generation mechanism for WiFi devices with MIMO capability has been studied only in MAKE [18]. In this work, authors have used WiFi devices equipped with 3 antennas for channel sampling in mobile environments. A

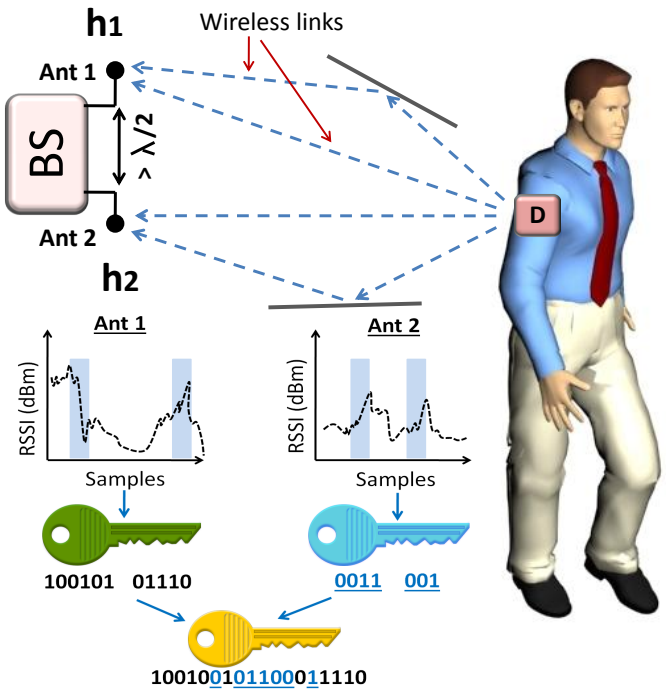


Fig. 1: DLINK dynamically identifies the suitable multipath link with enough fluctuation for secret key generation.

static node sends probe packet using one of its antennas and the mobile node receives the packet on all the 3 antennas simultaneously and records RSSI. Mobile node sends a response packet using one of its antennas which is captured by all the 3 antennas of static node. Different transmit-receive antenna pairs are used for each channel probing in a round robin fashion.

Our proposed solution is different than the existing ones for the following reasons: Prior work [5, 14] in BAN have been proposed for devices with single antenna. Our scheme is the first BAN protocol which employs dual-antennas on resource constrained devices to improve key rate and entropy in indoor mobile environments. As compared to MAKE, in our system, only one of the devices, i.e., the BS has the feature of dual-antennas, whereas tiny body-worn device has single antenna which is suitable for commercially available off-the-shelf sensor devices. It is important to note that, in our design, the BS is a non-MIMO sensor platform, i.e., only one of the antennas is used for packet transmission and reception at any time.

III. System Model

A. Assumptions and adversary model

Our system model consists of one body-worn device (D) and a BS as shown in Fig. 1. We assume the BS to be off-body and placed at a fixed location in the room. The BS has the feature of dual-antennas and alternately switches its antennas during channel sampling (i.e., packet exchanges), whereas D has a single antenna. The main focus of our protocol is renewal of session keys, as authentication can be addressed by existing schemes [7, 14].

Similar to prior work in physical layer security, we consider multiple passive eavesdroppers which are equipped with either

single or dual-antennas [1]. All the adversaries are off-body and static. Adversaries can listen to all the communication between the BS and D, and know the bit extraction algorithm. We assume that the eavesdroppers are not located very close to the BS and D, and are present at a distance of atleast a few multiples of the wavelength (λ = 12.5 cm for 2.4 GHz) of carrier signal being used.

B. Channel model

In this section, we present our channel model and theoretical analysis of the correlation of channel samples captured by the BS and D when (i) one antenna is used on the BS, and (ii) two spatially separated antennas are used on the BS.

Wireless signals propagating in multipath fading environment are attenuated by the following factors [15]:
(i) Path loss
(ii) Shadowing or large-scale propagation effects
(iii) Multipath fading or small-scale propagation effects.

In a typical indoor environment, for human activities involving body movement, the path loss and shadowing components cause slow changes in the wireless link signal over a number of packet transmissions. However, the multipath fading causes rapid signal variation whenever the device/node changes its position.

We consider *Rayleigh fading model* for modeling the indoor environment with multipath effects [6]. In Rayleigh fading, the spatial correlation of channel characteristics with respect to distance can be represented as

$$\rho = J_0(2\pi d/\lambda) \tag{1}$$

where J_0 is the zeroth order Bessel function of first kind, d is the spatial distance (from a reference point, e.g., a receiving antenna), and λ is the wavelength [6, 17]. The fading process associated with wireless channel decorrelates rapidly with distance in a rich scattering environment [17]. In particular, the correlation drops to nearly 0.5, i.e., 50% reduction in the correlation can be observed at a distance d = 0.25λ, which has been studied by other researchers also [9]. The correlation decreases further by increasing the distance d. Thus, in an indoor environment, the wireless signal characteristics will be entirely different at various locations. Unlike the existing schemes which rely on the channel samples observed at a single location (on the BS), our proposed scheme employs dual-antennas (separated by a distance $> \lambda/2$) at the BS, which helps to sample the channel at two different locations, and thus reduces the correlation of successive channel samples captured on two antennas by atleast 50%. A more detailed experimental study on this is presented in Section V.

Let us analyze the correlation between wireless channel characteristics observed by two communicating parties using same transmitter-receiver antenna pair. Let **h** denote the channel parameter of interest, i.e., the received signal strength (RSS), and *h(t)* its value at *t*. In order to estimate **h**, both the BS and D have to exchange known probe-response packets. Let $\mathbf{h}_1$ and $\mathbf{h}_2$ be the channel parameters of interest between the BS and D when the BS uses antenna 1 and antenna 2 respectively for packet exchanges as shown in Fig. 1. The channel estimate $\hat{h}$ of **h** (i.e., RSSI in our case) can be computed by both the parties by using received signal. Due to reciprocity property of wireless channel [6], the channel state between the BS and D will be same at a given instant of time. Because of the half-duplex nature of practical radios, D must wait until the probe packet from the BS is received before transmitting a response packet, and vice-versa. The channel parameter **h** varies slightly between probe-response packet exchanges and can be modeled by a probability distribution. The received signals at D and antenna 1 of the BS, i.e., $r_d(t)$ and $r_{bs}(t)$, for successive probe-response packet exchange can be represented as:

$$r_d(t_1) = p(t_1)h_1(t_1) + n_d(t_1) \tag{2}$$
$$r_{bs}(t_2) = q(t_2)h_1(t_2) + n_{bs}(t_2) \tag{3}$$

where t_1 is the time instant at which D receives probe packet $p(t)$, t_2 is the time instant at which the BS receives response packet $q(t)$, and n_d, n_{bs} are the independent noise processes at D and the BS respectively. After successful packet exchange on antenna 1, the BS switches its antenna for the next pair of packet exchange. Thus, the received signals at D and antenna 2 of the BS are given by:

$$r_d(t_3) = p(t_3)h_2(t_3) + n_d(t_3) \tag{4}$$
$$r_{bs}(t_4) = q(t_4)h_2(t_4) + n_{bs}(t_4). \tag{5}$$

Both the parties can then compute estimate of **h**, i.e., $\hat{h}$ from Eq. (2) and Eq. (3) as:

$$\hat{h}_{1d} = h_1(t_1) + z_d(t_1) \tag{6}$$
$$\hat{h}_{1bs} = h_1(t_2) + z_{bs}(t_2) \tag{7}$$

where z_d and z_{bs} are the noise terms added due to n_d and n_{bs} after applying the function which computes $\hat{h}$. The estimates $\hat{h}_{1d}$ and $\hat{h}_{1bs}$ may not be identical because of the time lag and the independent noise added. However, the estimates can be highly correlated if the BS and D exchange probe-response packets at a faster rate within the channel *Coherence time* (τ) (i.e., $t_2 - t_1 < \tau$), which is typically a few milliseconds depending on the node mobility. Suppose the BS and D exchange n probe-responses on antenna 1, then they can generate the sequence of channel estimates given by:

$$\underline{\hat{h}}_{1d} = \{\hat{h}_{1d}[1], \hat{h}_{1d}[2], \hat{h}_{1d}[3] \ldots \hat{h}_{1d}[n]\} \tag{8}$$
$$\underline{\hat{h}}_{1bs} = \{\hat{h}_{1bs}[1], \hat{h}_{1bs}[2], \hat{h}_{1bs}[3] \ldots \hat{h}_{1bs}[n]\}. \tag{9}$$

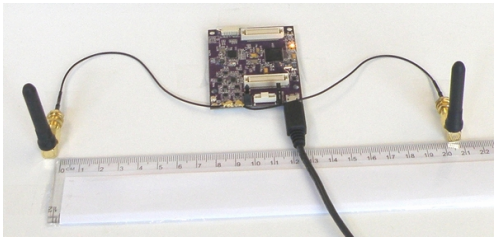
Similarly, the channel estimates for packets exchanged using antenna 2 of the BS are given by:

$$\hat{h}_{2d} = h_2(t_3) + z_d(t_3) \tag{10}$$
$$\hat{h}_{2bs} = h_2(t_4) + z_{bs}(t_4) \tag{11}$$

and the sequence of estimates for m probe-response exchanges on antenna 2 of the BS can be represented as:

$$\underline{\hat{h}}_{2d} = \{\hat{h}_{2d}[1], \hat{h}_{2d}[2], \hat{h}_{2d}[3] \ldots \hat{h}_{2d}[m]\} \tag{12}$$
$$\underline{\hat{h}}_{2bs} = \{\hat{h}_{2bs}[1], \hat{h}_{2bs}[2], \hat{h}_{2bs}[3] \ldots \hat{h}_{2bs}[m]\}. \tag{13}$$

[1] In oder to protect from active attackers with directional antennas, collusion attack, man-in-the-middle (MITM) attack, and jamming, the methods described in [10, 14] can be employed along with DLINK.



(a) Base station

(b) Body-worn device

Fig. 2: Experimental set-up: The BS was placed at a fixed location in indoor environment, whereas the body-worn device D was placed on the subject's right arm.

Due to reciprocity, the sequence of estimates $\hat{h}_{1d}$ will be highly correlated to $\hat{h}_{1bs}$. Similarly, $\hat{h}_{2d}$ and $\hat{h}_{2bs}$ will have strong correlation as they are captured within channel coherence time using the same transmitter-receiver antenna pair. However, as per the model discussed above (i.e., the correlation in Rayleigh fading), the sequence of channel estimates at the BS and D which use antenna 1 of the BS will be decorrelated with those collected at the two parties using antenna 2 of the BS when the antennas of the BS are separated by $> \lambda/2$ distance, i.e., the estimates $\hat{h}_{1d}$ will be decorrelated to $\hat{h}_{2d}$ and statistically independent of each other. Likewise, $\hat{h}_{1bs}$ and will be decorrelated to $\hat{h}_{2bs}$.

IV. Implementation and Experimental Set-up

We have used Opal sensor platform [8] with two external identical omni-directional antennas for the BS. Iris mote with single antenna, one of the commercially available off-the-shelf sensor platform was used for the body-worn device (D). Fig. 2 shows both the platforms used for our prototype. We have used TinyOS [4] environment to implement our system. Both the BS and D were programmed to execute the protocol described in Section V-A for channel sampling. In order to select a particular antenna for packet exchanges on the BS, we have incorporated the low-level device driver changes to TinyOS stack as suggested in [7].

In all our experiments, nodes acting as eavesdroppers (E1, E2 and E3) were placed at different locations. An Opal board having dual-antennas was used as E1, whereas Iris motes were used for programming E2 and E3. The receiver diversity algorithm was enabled on E1 to enable best packet reception. All the eavesdroppers were also programmed to perform bit extraction similar to the BS and D. All the devices were operating in 2.4 GHz frequency band. We have selected the above sensor platforms for our prototype as they are compatible

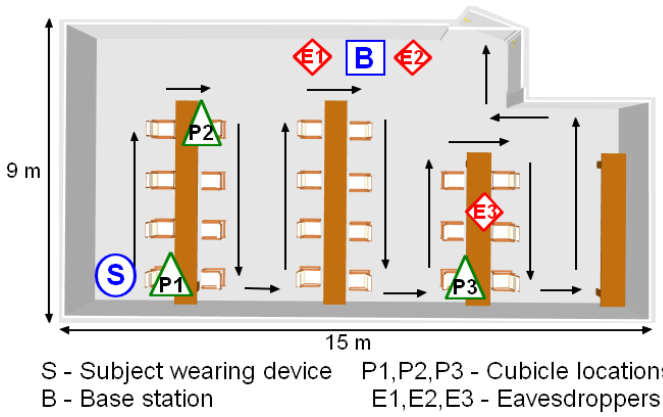


Fig. 3: Indoor environment used for experiments.

with the actual wearable sensor devices operating in 2.4 GHz, e.g., SensiumVitals patch (disposable wireless sensor) [3].

We have conducted an extensive set of experiments by involving two subjects, one male and one female, in a large room with multiple cubicles as shown in Fig. 3. There were 3-4 people other than the subjects sitting in different cubicles or walking in the room, similar to the normal office environment. Separate set of experiments were conducted for different user activity scenarios. For *high mobility* scenario, the subject was walking at a normal speed ($\approx$ 1 m/s), and for the *low mobility* scenario, the subject was sitting in a cubicle and working with a PC/laptop without much body movement, occasionally getting up and walking in the room. Additionally, the *low mobility case* experiments were repeated for subject sitting at different cubicle locations (P1 to P3) in the room (Fig. 3).

For each mobility case (i.e., *high* and *low*), experiments were conducted by varying the distance between two antennas of the BS, namely, for d = 1, 5, 10, 20 and 30 cm. The inter-packet interval t was set as 100 ms. Each experiment was conducted for about 10-15 minutes. All the experiments were repeated for two subjects.

V. Decorrelating the Channel Samples

Before applying any processing technique to the RSSI samples for key extraction, the first important step is to ensure that the captured RSSI samples corresponding to two antennas of the BS are highly distinct and decorrelated. This is required to extract keys with high entropy and good bit rate. In this section we study the correlation of channel samples with respect to the spatial separation of antennas on the BS for different user activity scenarios.

A. Channel sampling

This is the stage in which both D and the BS exchange a number of packets and measure the channel characteristics. Following is the sequence of operations followed by the BS and D for channel sampling

1) The BS sends periodic probe packets to D at an interval of t ms. The BS inserts 'packet index' and 'antenna number' in the payload of probe packet.

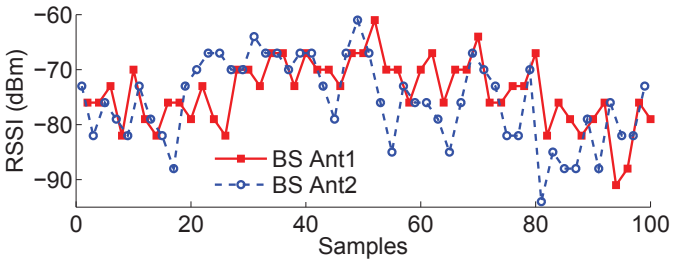


Fig. 4: RSSI samples collected by two antennas of the BS in one of the *high mobility* cases for d = 30 cm.

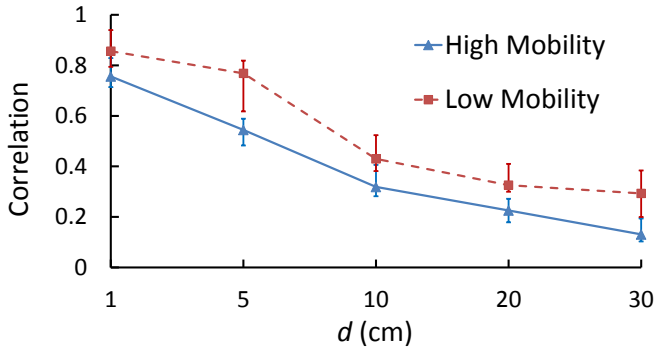


Fig. 5: The correlation of channel characteristics corresponding to two antennas of the BS for different user activity cases decreases with increasing distance d between the antennas.

2) The BS selects one of its antennas for transmitting a probe packet and receiving corresponding response packet from D.
3) After receiving the probe packet, D measures the RSSI and sends a response packet immediately by appending the index and antenna number of the received probe packet in the payload.
4) Upon receiving the probe response, the BS measures RSSI and checks if the index of the probe response matches with its own index. If the index matches, then its value is incremented by one. The new index is used for next probe transmission.
5) If the BS does not receive any probe response from D within the timeout interval (e.g., 10 ms), it re-transmits the probe packet with same index.
6) The BS switches its antenna for next probe packet exchange.
7) The BS and D exchange a total of N probes (probe and its response packets) where N is the configurable parameter in the algorithm.

After channel sampling, the BS and D will have set of RSSI values which can be processed further for bit extraction.

B. Understanding the correlation

In this section we study the correlation of channel samples collected by the BS and D for different experimental scenarios described in Section IV.

First, let us consider the channel samples at the BS. Fig. 4 shows the RSSI samples captured by antenna 1 and antenna 2 of the BS for d = 30 cm and t = 100 ms in one of the *high mobility* scenarios. It can be observed that the channel samples on antenna 1 and antenna 2 are distinct and independent of each other. In other words, we can say that the samples on two antennas do not have correlation. In order to quantify the correlation of channel samples, we use Pearson correlation coefficient (r), a well known statistical method to calculate correlation of two variables, given by the following equation:

$$r = \frac{\sum_{i=1}^{n}(X_i - \bar{X})(Y_i - \bar{Y})}{\sqrt{\sum_{i=1}^{n}(X_i - \bar{X})^2}\sqrt{\sum_{i=1}^{n}(Y_i - \bar{Y})^2}}. \quad (14)$$

The coefficient r returns a value in the range [-1, 1], i.e., 1 if the two sets X and Y are perfectly correlated, -1 if the sets are anti-correlated, and 0 if there is no correlation. We consider the sets X and Y to be the RSSI samples collected by the BS on its antenna 1 and antenna 2 respectively.

Researchers in [16] have experimentally verified and reported that the correlation of successive channel samples collected by single antenna devices when operating in a single channel (i.e, channel 26) on 2.4 GHz is ≈0.78, and have studied different channel hopping schemes to decorrelate successive samples. The authors were able to minimize the correlation up to 0.44 for a particular channel hopping order. However, they mention that the correlation cannot be reduced further (to 0) even by employing maximum channel spacing. We consider these results as the benchmark to measure the performance of our system.

Fig. 5 shows the correlation coefficient r calculated for the data collected in our experiments. For *high mobility* cases, a very high correlation (0.714 to 0.829) can be observed when the distance between two antennas is 1 cm. As the distance d is increased, the correlation drops dramatically by 43% for d = 10 cm (0.282 to 0.406), after this distance, the value decreases gradually. The lowest correlation observed is from 0.103 to 0.194 for d = 30 cm, which is a drastic reduction by nearly 62.5%. Similar trend in the reduction of correlation is observed for *low mobility* cases also. The correlation in *low mobility* cases is more compared to that for *high mobility* cases for all d. This is justifiable as the channel fading is dependent on how fast the node is moving [6]. Rapid body movements in *high mobility* cases result in quick channel fading, whereas in *low mobility* scenarios, the channel fades slowly. We are the first to investigate this effect practically in the unique context of BANs.

Our observations show similar behavior as the channel model we have discussed in Section III-B (recall that the correlation of channel characteristics decreases by ≈50% at a distance of 0.25λ from a reference point). Theoretically, the rate at which the channel varies is represented by *Doppler frequency* (f_d), and the duration for which the channel condition is stable is represented by *Coherence time* (τ). The f_d and τ for typical indoor environments in 2.4 GHz with the velocity (v) of mobile device = 1 m/s, (assuming the devices with single antenna) is given by the following equations:

$$f_d = \frac{v}{\lambda} \sim \frac{2.4 \times 10^9}{3 \times 10^8} = 8Hz; \quad \tau = \frac{1}{f_d} = 125ms. \quad (15)$$

From Eq. (15) it can be concluded that, in order to get successive samples which are almost independent, the

samples must be separated in time by atleast a *coherence time* interval. This implies that as $\tau \propto 1/f_d$, sampling the channel at a rate significantly greater than f_d cannot possibly produce random/uncorrelated samples [10]. This justifies the high correlation observed between channel samples of antenna 1 and antenna 2 for d = 1 cm in Fig. 5, where the channel is sampled at two points very close to each other ($< 0.5\lambda$) in quick succession. With increasing distance d, though the sampling frequency is smaller than τ, as the channel is sampled at two different points (at the BS) spatially separated by $> 0.5\lambda$, the correlation observed is smaller. The above analysis given for samples of the BS holds good for the channel samples collected at D also.

Based on the above discussion, our proposed dual-link based solution rapidly decreases the correlation of successive samples by approximately 67% compared to the prior work [16], even when operating in the same channel. Thus, DLINK helps to extract secret keys with high entropy and good bit rate. It should be noted that, we do not consider the static channel case, i.e., stationary devices in this work, as our model is not applicable for such scenarios. Investigating the static channel conditions is a separate problem to be addressed.

VI. DLINK Protocol

In this section, we present our protocol for RF fingerprinting. Channel sampling is the first step in key establishment. After channel sampling, the BS and D extract secret bits from the RSSI samples collected by performing filtering and quantization process as explained in following sub-sections.

A. Filtering

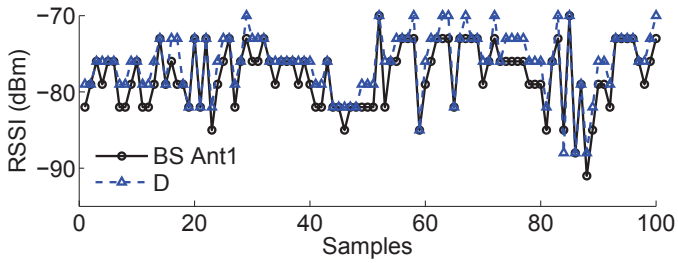
The small scale fading and noise components affect the signal characteristics, especially in case of slow changing channel, which may lead to a discrepancy in the channel measurements at both the parties. In order to minimize this error, we apply Savitzky-Golay filter to the RSSI samples collected at the BS and D before quantization. The cut-off frequency of the filter can be determined by the following equation

$$f_{cut-off} \approx \frac{(K+1)}{1.6F - 3.6}. \quad (16)$$

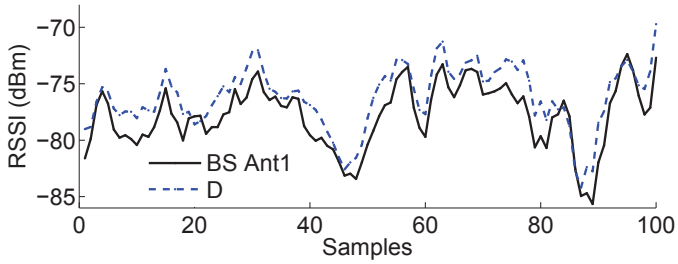
We select 5^{th} order polynomial (K = 5) and window size (F) as 11 for the filter parameters, similar to prior work. Fig. 6a shows RSSI samples collected at the BS (antenna 1) and D from one of our experimental traces. The filtered samples, also called as *low frequency component* are shown in Fig. 6b. Fig. 6c shows corresponding *high frequency component* of the samples, which is obtained by subtracting low frequency component from the unfiltered signal.

B. Identifying the activity region for bit extraction

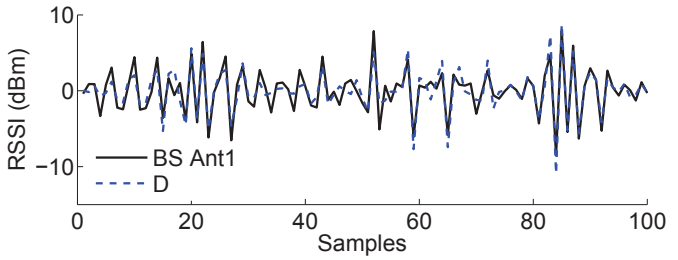
Let us first consider *low mobility* scenario in order to understand activity region selection and its significance. In *low mobility* cases, the channel characteristics exhibit very low fluctuation and noise components can cause bit mismatch at both the ends. To overcome this, we dynamically identify the activity region with sufficient energy, i.e., set of RSSI



(a) Unfiltered RSSI samples



(b) Low frequency component

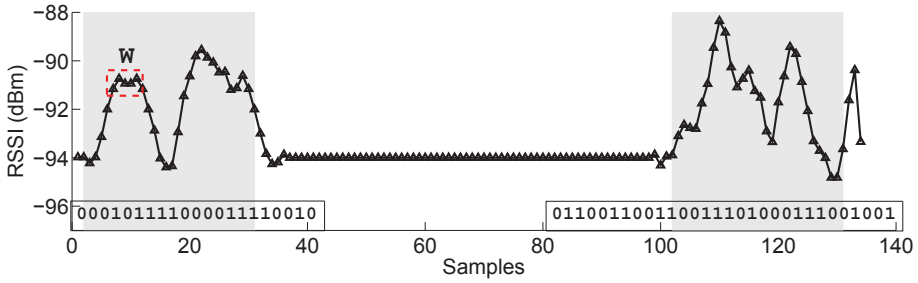


(c) High frequency component

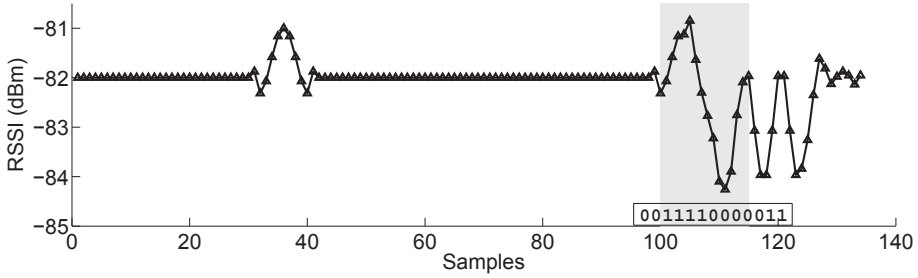
Fig. 6: Filtering technique is applied to RSSI samples to decompose into low and high frequency components.

samples suitable for the generation of keys. We measure the RMS energy (in dB) of high frequency component of the samples (obtained by filtering) by considering non overlapping successive blocks of 10 samples each. Fig. 7a and 7b show the filtered RSSI samples (i.e., low frequency component) and RMS values calculated for corresponding high frequency component (with block size = 10 samples) respectively for one of the *low mobility* scenarios. It can be observed that sufficient variation in low frequency component (shaded part in Fig. 7a) results in *high energy* in the high frequency component, which in turn yields high RMS values (Fig. 7b). Thus, we can detect the channel variation easily by observing the changes in RMS values. In order to ensure that there is sufficient channel variation, we set a particular threshold for the RMS values. Only the regions of low frequency component corresponding to RMS $>$ threshold are selected. Fig. 7a shows dynamically selected regions of filtered samples for RMS threshold of 1 dB. The RSSI samples of selected regions are processed by quantizer for bit extraction.

In our protocol, RMS based region selection is applied to both *low* and *high mobility* cases. However, in case of *high mobility*, the channel variation shows sufficient randomness and high amplitude as shown in Fig. 6a. As a result, higher number of activity regions (or sometimes all the samples) will

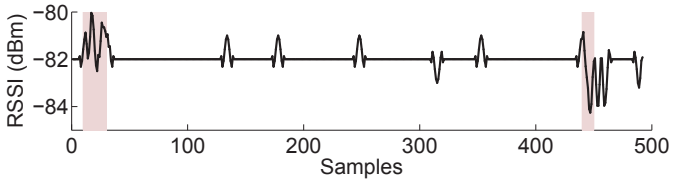


(a) Secret bit extraction from RSSI samples corresponding to antenna 1

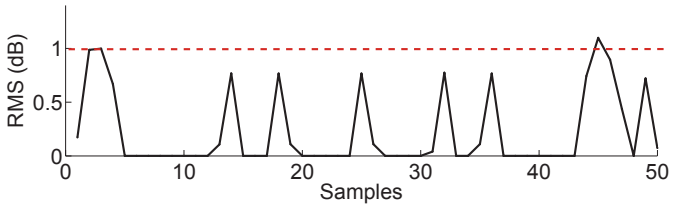


(b) Secret bit extraction from RSSI samples corresponding to antenna 2

Fig. 8: Secret bit extraction mechanism: The RSSI samples selected based on the dynamic region selection are quantized to extract secret bits.



(a) Regions of filtered RSSI samples



(b) RMS threshold for W = 10 samples

Fig. 7: An example of identifying the activity region based on RMS threshold in a very *low mobility* case.

be selected for bit extraction compared to *low mobility* case.

C. Quantization and key generation

We have employed the quantization scheme used in [5, 10] with moving window size W = 5 and scaling factor α = 0.5 for our analysis. In order to generate the bits, two thresholds q_+ and q_- are calculated as follows:

$$q_+ = \mu + \alpha * \sigma; \quad q_- = \mu - \alpha * \sigma \tag{17}$$

where μ and σ are the mean and standard deviation of RSSI samples in a particular window selected respectively. The RSSI

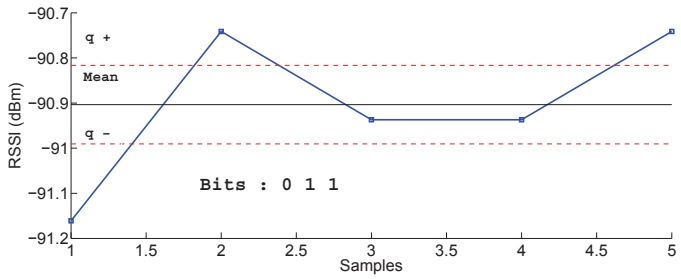


Fig. 9: Secret bit extraction in a window of W = 5 samples.

samples $> q_+$ are encoded as bit 1, and samples $< q_-$ are encoded as bit 0.

We perform filtering, identifying activity region, and bit extraction for the samples captured on antenna 1 of the BS and D. The same steps are repeated for samples collected on antenna 2 of the BS and D. At the end of this process, two separate bit streams K_1 and K_2 are extracted from the samples corresponding to antenna 1 and antenna 2 of the BS. The final key K is thus obtained by interleaving the two bit streams in time domain as given below:

$$K = K_1 \,|||\, K_2. \tag{18}$$

Once the key K is extracted at both the ends, there may be some bit mismatches due to noise or multipath effects. This is because the samples discarded during quantization at one end may be different than those at the other end. To increase bit agreement, the BS and D exchange their sequence of packet indexes. Only the bits corresponding to common packet indexes are retained by both the parties to get final key.

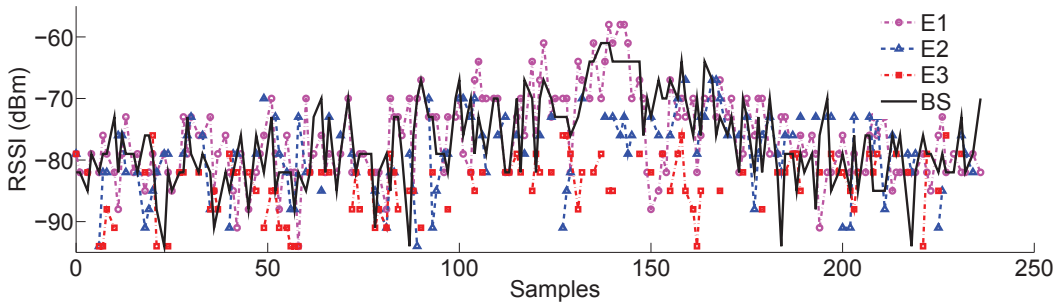
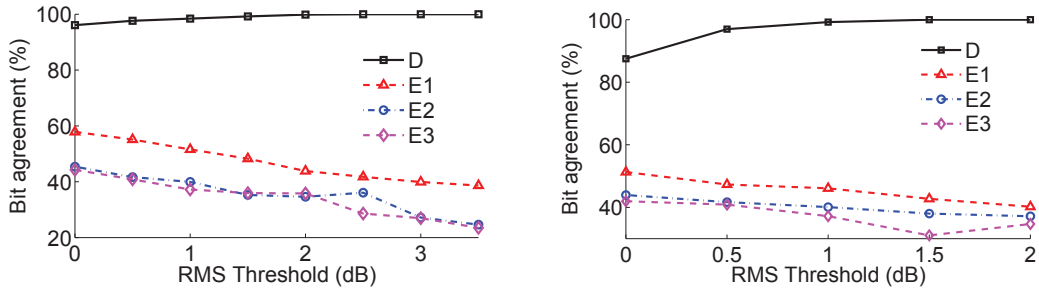


Fig. 10: Unfiltered RSSI samples captured by all the parties in one of the *high mobility* case. The channel characteristics observed by eavesdroppers will be entirely different compared to the BS due to multi-path effects in indoor environments.



(a) Bit agreement with the BS in *high mobility* case

(b) Bit agreement with the BS in *low mobility* case

Fig. 11: Performance of key generation with d = 30 cm spacing between antennas of the BS. The bit agreement improves as the RMS threshold is increased in both *high* and *low mobility* cases.

The bit extraction is explained clearly in Fig. 8, by considering the RSSI samples captured by the BS in one of the *low mobility* cases. Fig. 8a and Fig. 8b show filtered RSSI samples captured by antenna 1 and antenna 2 and dynamic regions selected for key generation. Fig. 9 shows the bit generation in a single window (W) with 5 RSSI samples captured on antenna 1 of the BS (selected window W in Fig. 8a). From Fig. 8a and Fig. 8b, it can be observed that, the two link characteristics corresponding to antenna 1 and antenna 2 show different behavior (due to multipath effects) and result in two different bit strings $K1$ and $K2$. The final key K is then obtained by interleaving the two strings in time domain.

In this section, we have shown the bit extraction in case of *low mobility* only as it is clear to understand. It should be noted that, the samples outside the shaded area in Fig. 8b and Fig. 8c are discarded, which reduces the bit rate in *low mobility* case. In case of *high mobility*, the channel samples corresponding to two antennas of the BS will have sufficient random fluctuation and yield more secret bits in $K1$ and $K2$, which improves the total bit rate. Thus, the bit rate depends on user mobility which produce quick changes in multipath components of the signal.

VII. Evaluation and Results

In this section, we evaluate the performance of our proposed protocol in different indoor environments and user activities. We consider the RSSI traces captured during the experiments described in Section IV for the analysis of key generation. Additionally, we have repeated the *high mobility* case experiments for d = 30 cm in another two indoor environments for two subjects, namely, in a busy corridor surrounding two lifts, and a long quiet corridor. In all the experiments, static eavesdroppers E1, E2 and E3 were placed at different locations.

We provide the detailed analysis of the traces captured for d = 30 cm, as this setting decorrelates the samples to yield high quality keys. Let us consider Fig. 10 which shows the RSSI samples captured by all the parties in one of the *high mobility* case. It can be observed that, the eavesdropper E1 equipped with dual-antennas and placed close to the BS was able to capture almost all the packets exchanged between the BS and D, whereas E2 and E3 missed some of the packets due to multipath effects as they had single antenna and were placed at other locations away from legitimate devices. It can be observed that the RSSI samples captured by eavesdroppers have no correlation with those of the BS and D. Fig. 11 shows the performance of DLINK for d = 30 cm. For both *high* and *low mobility* cases, setting the RMS threshold of 1 dB is sufficient to yield keys with 98.5-99.43% bit agreement between the BS and D as shown in Fig. 11a and Fig. 11b. A threshold of 2 dB results in 99.99-100% bit agreement. From Fig. 12, it can be observed that, in any mobility case, the bit rate decreases as the RMS threshold increases. From our observations we conclude that, setting a 1dB threshold is sufficient in many applications, whereas for achieving better key match, higher values of threshold are recommended. Fig. 13 depicts the entropy or randomness of the key bits generated for different distances d in various user activity conditions.

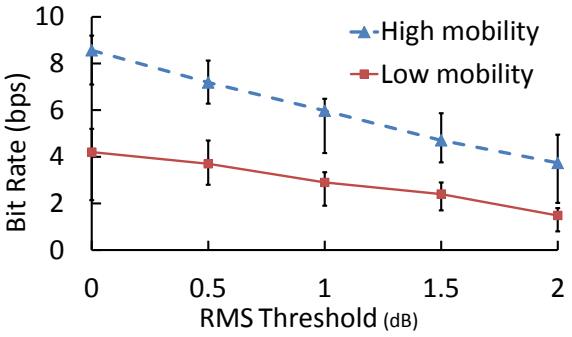


Fig. 12: Secret bit rate in different mobility cases.

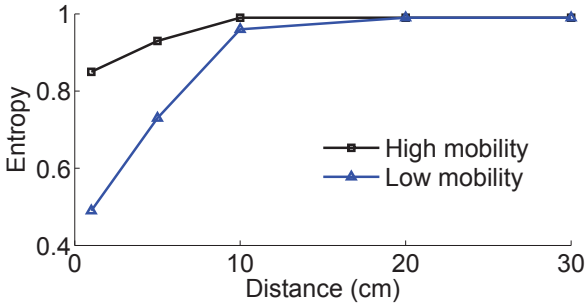


Fig. 13: Key entropy vs. spatial separation of antennas of the BS.

We have verified the randomness of the keys generated by our protocol using NIST [11] entropy test. Antenna spacing of 10 cm is sufficient for normal applications which yields entropy in the range of 0.94-0.97, whereas for more than 20 cm antenna spacing, the entropy achieved was 0.9 to 0.99. For t = 20 ms and d = 30 cm, the maximum bit rate achieved by DLINK in *high mobility* cases was about 44.32 bps, i.e., DLINK generates a 128 bit key in 2.88 s, which is nearly 5 times faster compared to the most recent scheme [14]. For *high mobility* cases, the performance of DLINK in all three different indoor environments was nearly the same. Though the bit rate observed in *low mobility* cases is less than that in *high mobility* cases, the rate achieved is comparatively more than the prior work as it combines the bit strings generated from independent samples captured corresponding to two antennas of the BS. Though our protocol employs dual-antennas, the power consumption of the BS is same as single antenna systems since only one of the antennas is used at any time for packet exchanges. Thus, DLINK is lightweight, efficient and suitable for practical applications.

VIII. Conclusion

In this paper, we have presented the theoretical analysis of correlation of channel characteristics in multipath fading indoor environments and proposed our scheme DLINK based on dual-antennas, which dynamically identifies the channel links with sufficient fluctuation for secret key generation. We have conducted an extensive set of experiments in various indoor environments. Our results reveal that DLINK has overall better performance, viz., as compared to existing work, DLINK decorrelates successive channel samples by 67% and has high bit rate (5 times more secrecy capacity) and entropy in slow as well as fast fading channels. In our future work, we intend to improve the performance and bit rate of DLINK by employing more than 2 antennas on the BS. In addition, we would like to investigate the key generation for WBAN devices having dual/multi antennas by employing smart wearable antennas, e.g., strip antennas, micro strip antennas, and patch antennas.

Acknowledgment

This work is partially supported by Australian Research Council Discovery grant DP150100564. The authors would like to thank Diethelm Ostry and Cong Huynh from ICT Centre, CSIRO, Australia for their valuable suggestions.

References

[1] "IEEE 802.15 WPAN Task Group 6 (TG6) Body Area Networks," http://www.ieee802.org/15/pub/TG6.html, Accessed: 24-July-2015.

[2] "Morgan Stanley: Wearable Technology A Potential USD 1.6 Trillion Business," http://www.wearabledevices.com, Accessed: 24-July-2015.

[3] "SensiumVitals Patch," http://www.sensium-healthcare.com, Accessed: 24-July-2015.

[4] "TinyOS," http://www.tinyos.net/, Accessed: 24-July-2015.

[5] S. T. Ali, V. Sivaraman, and D. Ostry, "Zero Reconciliation Secret Key Generation for Body-worn Health Monitoring Devices," in *Proc. ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2012.

[6] W. C. Jakes, *Microwave Mobile Communications*. Wiley, 1974.

[7] C. Javali, G. Revadigar, L. Libman, and S. Jha, "SeAK: Secure Authentication and Key Generation Protocol based on Dual Antennas for Wireless Body Area Networks," in *Proc. Workshop on RFID Security (RFIDsec)*, 2014.

[8] B. Kusy, D. Abbott, C. Richter, C. Huynh, M. Afanasyev, W. Hu, M. Brünig, D. Ostry, and R. Jurdak, "Radio Diversity for Reliable Communication in Sensor Networks," *ACM Trans. Sensor Networks*, vol. 10, no. 2, pp. 32:1–32:29, Jan 2014.

[9] R. Liu and W. Trappe, *Securing Wireless Communications at the Physical Layer*, 1st ed. Springer Publishing Company, Incorporated, 2009.

[10] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a Secret Key from an Unauthenticated Wireless Channel," in *MobiCom*, 2008.

[11] NIST, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, 2010.

[12] G. Revadigar, C. Javali, H. Asghar, K. Rasmussen, and S. Jha, "iARC: Secret Key Generation for Resource Constrained Devices by Inducing Artificial Randomness in the Channel," in *Proc. ACM Symposium on Information, Computer and Communications Security (ASIACCS)*, 2014.

[13] ——, "Secret Key Generation for Body-worn Devices by Inducing Artificial Randomness in the Channel," *Technical Report UNSW-CSE-TR-201506, UNSW Australia*, 2015.

[14] L. Shi, J. Yuan, S. Yu, and M. Li, "ASK-BAN: Authenticated Secret Key Extraction Utilizing Channel Characteristics for Body Area Networks," in *Proc. ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2013.

[15] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge University Press, 2005.

[16] L. Yao, S. T. Ali, V. Sivaraman, and D. Ostry, "Decorrelating Secret Bit Extraction via Channel Hopping in Body Area Networks," in *IEEE Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, 2012.

[17] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically Secret Key Generation for Fading Wireless Channels," *ACM Trans. Information Forensics and Security*, vol. 5, no. 2, pp. 240–254, Jun 2010.

[18] K. Zeng, D. Wu, A. Chan, and P. Mohapatra, "Exploiting Multiple-antenna Diversity for Shared Secret Key Generation in Wireless Networks," in *IEEE INFOCOM*, 2010.