Mobility Independent Secret Key Generation for Wearable Health-care Devices

Girish Revadigar*†, Chitra Javali*†, Hassan Jameel Asghar †,
Kasper B. Rasmussen, and Sanjay Jha*
{girishr,chitraj,sanjay}@cse.unsw.edu.au; hassan.asghar@nicta.com.au;
kasper.rasmussen@cs.ox.ac.uk

*School of Computer Science & Engineering, UNSW Australia, Sydney, AUSTRALIA
†National ICT Australia (NICTA), Australian Technology Park, Sydney, AUSTRALIA
Dept. of Computer Science, University of Oxford, Oxford, UK

ABSTRACT

Security in Wireless Body Area Networks (WBAN) is of major concern as the miniature personal health-care devices need to protect the sensitive health information transmitted in wireless medium. It is essential for these devices to generate the shared secret key used for data encryption periodically. Recent studies have exploited wireless channel characteristics, e.g., received signal strength indicator (RSSI) to derive the shared secret key during random body movement of subject wearing devices. However, in the absence of node mobility, these schemes have very low bit rate capacity, and fail to derive keys with good entropy, which is a big threat for security.

In this work, we study the effectiveness of combining dual antennas and frequency diversity for obtaining uncorrelated channel samples to improve entropy of key and bit rate in static channel conditions. We propose a novel mobility independent RSSI based secret key generation protocol – iARC for WBAN. We conduct an extensive set of experiments in real time environments on sensor platforms used in WBAN to validate the performance of iARC. iARC has 800 bps secrecy capacity and generates 128 bit key in only 160 ms.

Categories and Subject Descriptors

C.2.0 [**General**]: Security and protection; C.2.1 [**Network Architecture and Design**]: Wireless communication

General Terms

Security, Design, Protocol, Experimentation

Keywords

Body Area Networks, Physical layer security, Secret key generation

.

1. INTRODUCTION

One of the remarkable outcomes of rapid development in wireless technology is the emergence of a new paradigm for personalized health care, sports and fitness applications, known as Wireless Body Area Networks (WBAN). Several wearable devices like FitBit Flex, JawBone's Up, and Nike+ FuelBand [1] are gaining popularity in the healthcare sector. According to a recent survey from ABI Research, wearable device revenues are expected to grow more than USD $6 billion by 2018 [3].

Although technological advancement has lead to wireless capability of body-worn devices, there are a number of security threats that these devices may face, for example, eavesdropping of confidential data and injection of malicious commands which can cause adverse effects on a person's health. Since WBAN devices handle sensitive health information, securing them against such attacks is a major challenge.

As WBAN devices are resource constrained, the complex traditional cryptographic key establishment schemes would not be feasible. Instead, the devices need lightweight security mechanisms that are fast and reliable. The secret keys used by these devices to encrypt the data must be generated dynamically and renewed periodically to avoid the threat of compromise and privacy leakage.

Recent studies [4, 17] have shown that the wireless link characteristics, for e.g., Received Signal Strength Indicator (RSSI) can be exploited to generate shared symmetric keys. RSSI based security schemes are well suited for WBAN devices as it can be easily measured by every device directly from the received packet without the need of special hardware. The existing schemes [4, 17] for secret key generation in WBAN are dependent on the channel randomness caused due to node mobility during the body motion of a subject wearing devices. It has been shown that keys with good entropy and high bit rate can be generated during the activities involving sufficient body movements. However, in the absence of node mobility the existing schemes will have very low bit rate and low entropy, in which case an eavesdropper can easily reproduce the same key by observing the channel [13]. This poses a major security threat. It is worth noting that, in real-time applications such as hospital scenarios or remote-health monitoring systems in home/office environments, one cannot expect the patient/person to be always mobile. Indeed, many static channel cases like person sitting in a position without much body movement (e.g.,

BODYNETS 2015, September 28-30, Sydney, Australia

DOI 10.4108/eai.28-9-2015.2261446

person at home/workplace), or sleeping on a bed (e.g., in home or critical care sections/wards of hospitals) are quite common, in which case the existing schemes cannot be used.

Thus, there is a need for a robust and lightweight secret key generation scheme which is independent of node mobility to make WBAN resilient against possible threats.

The security issues related to WBAN discussed above are the motivation for our work presented in this paper. We present an RSSI based shared secret key generation scheme which involves a novel approach for inducing artificial randomness in the wireless channel using dual antennas and frequency diversity to yield keys with sufficient entropy even under static channel conditions. Our proposed scheme is lightweight and suitable for deployment in real world applications.

Although multiple antenna architectures have been extensively used in complex wireless systems like WiFi with Multiple Input Multiple Output (MIMO) capability, they have not been used in WBAN devices with small form factor. MIMO systems allow simultaneous reception of an incoming packet on all the antennas of the receiver node. Typically, WBAN devices are resource constrained without MIMO capability, hence, the protocols available for WiFi cannot be directly applied to WBAN. Our scheme demonstrates the use of multiple antennas effectively for shared secret key generation without adding extra cost to power consumption.

We have validated our system using real sensor platforms used in WBAN applications by conducting an extensive set of experiments in different real-time environments.

To summarize, **our contributions** are as follows:

- We propose iARC – a novel, lightweight, RSSI based secret key generation scheme for WBAN which *induces artificial channel randomness* by employing dual antennas and frequency diversity for generating keys with good entropy in the absence of node-mobility.
- We propose a multiple bit extraction algorithm to reduce the number of packets exchanged during key generation and overall time taken for generating shared secret keys.
- We demonstrate experimentally that, iARC achieves the highest bit rate of 800 bps with high bit agreement between the two legitimate body-worn devices, and generates 128 bit key in 160 ms, which is faster by an order of magnitude compared to existing mobility based schemes.

To the best of our knowledge, the work presented in this paper is the first mobility independent physical layer based secret key generation mechanism for resource constrained devices of WBAN. We have evaluated the randomness of keys generated by our proposed protocol using NIST [10] entropy test. The keys generated by our protocol pass the NIST test with entropy in the range: 0.92 to 0.99.

The rest of the paper is organized as follows. In Section 2 we discuss related work. Section 3 presents our system model and Section 4 explains our protocol design. Section 5 describes detailed evaluation of the proposed protocol and results. In Section 6, we provide the security analysis, and in Section 7 we present conclusion and future work.

2. RELATED WORK

Recently, security mechanisms based on RSSI have been proposed for Wireless Body Area Networks. Authors in [6] have studied key generation in dynamic channel condition and achieved 2 bps bit rate in a simulation environment. Researchers in [4, 17] have shown that the body-worn devices can generate secret keys during dynamic channel conditions caused due to the body movement of subject wearing the devices. The scheme in [4] has a bit rate of 0.24 bps and requires 15-35 minutes to generate a 128 bit key. Additionally, the work employs Savitzky-Golay filter and windowing to select a subset of RSSI samples and discard the remaining. The scheme in [17] has the bit rate of 8.03 bps. One of the major drawback of existing schemes [4, 17] is that, in case of a stable channel, the above schemes will have very low bit rate and fail to derive keys with sufficient entropy. Researchers in [7] have proposed a protocol for key generation between non-reachable nodes with the help of a trusted relay in mobile environments.

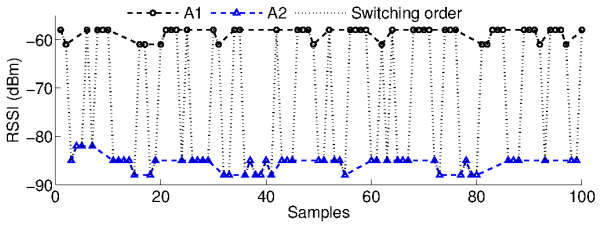
The most recent protocols closest to our work are SeAK [8] and DLINK [14]. SeAK has been proposed for secure device pairing during the bootstrapping phase of WBAN. SeAK exploits the spatial separation of dual antennas to perform authentication and initial key generation with a nearby device ($<$ 10-15 cm) aligned to one of its antennas prior to on-body deployment. In DLINK, an off-body base station exploits spatial separation of antennas for decorrelating the successive channel samples in mobile environments. In contrast, iARC is for session key renewal for the wearable devices after on-body deployment and is independent of antenna separation and device alignment.

To the best of our knowledge, the scheme presented in [18] is the only one to investigate secret key generation in static channel conditions. The authors have studied the effect of channel hopping to yield channel variation in static cases. It has been demonstrated on single antenna sensor platform that the basic channel hopping can provide a good source of correlated randomness at the two parties. However, as the channel decays very slowly in static cases, only a limited amount of meaningful information can be derived. On the contrary, in our work, we study the effectiveness of combining frequency diversity and random switching of dual antennas to obtain uncorrelated channel samples, and how this improves the bit rate, quality of secret keys, and bit agreement in static channel conditions.

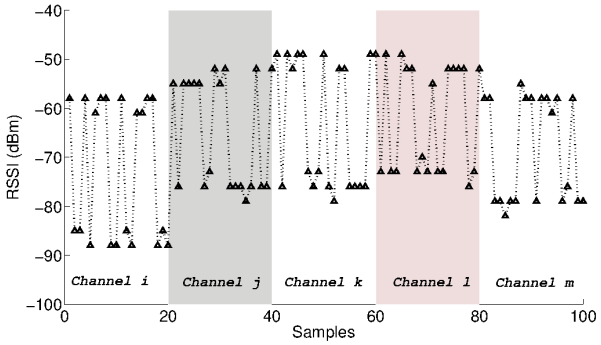
3. SYSTEM MODEL

3.1 Assumptions

We assume that all the WBAN devices operate in 2.4 GHz. There is one on-body Control Unit (CU) and one or more wearable devices (D) which are in line of sight with the CU. The CU is equipped with two omni-directional antennas A1 and A2 having different features, whereas the devices have single antenna. The CU employs a pseudo-random number generator (PRNG) to generate a random bit string $r \in \{0,1\}^{128}$ used for antenna selection. Only the CU knows the random antenna switching algorithm and the initial secret random seed of 128 bits, i.e., $s \in \{0,1\}^{128}$ required for the PRNG. We assume that the WBAN devices are authenticated and are not compromised. We consider static channel conditions only.



(a) RSSI samples measured by A1 and A2 on a single channel



(b) RSSI samples measured by A1 and A2 with antenna switching and dynamic channel hopping

Figure 1: The CU induces artificial channel randomness by effectively combining random antenna switching and dynamic frequency hopping.

3.2 Threat model

We consider the presence of one or more off-body adversaries located away from legitimate devices at a distance more than half the wavelength (i.e., 6.25 cm) of radio signal being used. The adversaries may be either in line of sight (LOS) or non-line of sight (NLOS) to the WBAN devices. We consider both passive and active adversaries. A passive eavesdropper can capture the packets exchanged between the CU and D and attempt to extract the secret key. Eavesdroppers can have single or dual antennas. Active attackers can jam the channel, or cause man-in-the-middle (MIM) attack. It is assumed that the adversaries have same radio capability as the WBAN devices to sample the wireless channel and are aware of the secret key extraction mechanism.

4. PROTOCOL DESIGN

4.1 Inducing artificial channel randomness

Our design is based on the wireless signal propagation characteristics. As the distance between two wireless devices communicating with each other increases, the radio signal strength degrades because of fading and multi-path effects. However, the channel characteristics will be unique and highly correlated between the two devices due to reciprocity property [11]. Our system uses dual antennas and frequency diversity for inducing artificial channel randomness required for secret key generation [12,13]. The following subsections describe the steps involved in detail.

4.1.1 Employing dual antennas

In static channel conditions, for a fixed distance between the CU and D, suppose that the CU uses a single default antenna, i.e., either A1 or A2 during channel sampling, then the observed variation in the RSSI samples will be as shown in Fig. 1a. The successive RSSI samples measured on a single antenna will be highly correlated and hence secret keys with good entropy and high bit rate cannot be obtained. Our design aims to extract uncorrelated successive channel samples. Thus, the CU employs dual antennas for channel sampling and randomly switches between the two.

In order to decide the antenna switching pattern, iARC employs a PRNG used in [15]. This PRNG is a cryptographically secure, NIST recommended random number generator which uses AES as the block cipher [16]. An initial secret random seed s required for the PRNG is generated offline and stored in the non-volatile memory of the CU.[1] This seed is updated every time the PRNG is run for subsequent key generation. As 128 bit keys are used in WBAN [2], we use a 128 bit seed, i.e., $s \in \{0,1\}^{128}$. The CU employs random antenna switching for channel sampling based on the random bit string $r \in \{0,1\}^{128}$ generated by the PRNG. The CU uses antenna A1 or A2 for probe exchange based on the order in which bit 0 and 1 appear in r respectively. An example of variation in the RSSI samples after antenna switching is shown by the dotted line in Fig. 1a.

4.1.2 Exploiting frequency diversity

iARC exploits frequency diversity by employing our novel *dynamic frequency hopping* scheme, which is explained in detail in Section 4.2.3. Our scheme adopts frequency hopping for two important reasons, primarily to avoid the leakage of useful information to the adversary, and second, to bring additional randomness in the samples collected [18]. In our design, the total number of probes N required for key extraction is divided into a number of sub blocks, and each sub block key is derived in a different channel. In each channel, the CU performs random antenna switching as explained in previous Section 4.1.1 for channel sampling. As there are 16 channels available in 2.4 GHz, when each sub block key is generated in a different frequency channel, the RSSI samples collected in different channels will be shifted based on the channel spacing, i.e., the current channel and new channel after hopping. This further improves the randomness of the samples as shown in Fig. 1b and hence the secret key bits. The center frequency F_c (MHz) of each channel in 2.4 GHz is given by

$$F_c = 2405 + 5(\eta - 11) \quad (1)$$

where $\eta = \{11, 12, \ldots, 26\}$ is the channel number.

4.2 Key generation process

The secret key generation process consists of following different steps: (i) Channel sampling, (ii) Quantization, and (iii) Dynamic frequency hopping.

In iARC, the total number of probes N required for key generation is divided into B number of multiple sub blocks of equal length and each sub block key k_{sb} is derived in a different channel. The final secret key K is obtained by the concatenation of all the sub block keys as:

$$K = k_{sb1} \parallel k_{sb2} \parallel \cdots \parallel k_{sbB} \quad (2)$$

The CU and D perform channel sampling, quantization

[1]In commercial devices, this seed can be placed at the time of manufacturing.

and frequency hopping repeatedly until the total number of probes N required for key generation are exchanged.

4.2.1 Channel sampling

During channel sampling, both the CU and D exchange multiple probe and response packets and measure the RSSI of incoming packet. The device D sends a `Key_Renewal_Req` packet to CU to initiate the key renewal process. The CU transmits a total of N number of `Probe_Packet` at an interval of t ms by adding an index number i in the payload to track successful packet reception, where $i = \{0, 1, \ldots, N\text{-}1\}$. Let X and Y denote the set of RSSI captured by the CU and D respectively. Once the probe packet is received, D measures the RSSI y_i and immediately transmits a `Response_Packet` by placing index i of the last received `Probe_Packet` in the payload. After receiving the `Response_Packet`, the CU checks if the index i of payload matches the value in the last probe packet transmitted, and if it matches, the CU measures the RSSI x_i of the packet. The CU uses the same antenna, i.e., either A1 or A2 for sending a probe packet and receiving the corresponding response packet with the same index i. After successful packet exchange for a particular index i, i is incremented and the CU may use the same antenna or switch to another antenna for the next probe packet transmission based on the random string r. If the CU does not receive any reply from D within timeout interval t_o, it retransmits the probe packet with the index i. D updates y_i with the RSSI of latest packet.

4.2.2 Quantization and multiple bit extraction

Once the CU and D have RSSI samples collected on a particular channel, they perform quantization and bit extraction process to generate the sub block key k_{sb} as below:
(i) Suppose n is the number of bits to be assigned per sample, then divide the whole range of RSS available for the devices into L levels - $l_1, l_2, \ldots, l_L$, arranged in the highest to lowest order, such that $L = 2^n$.
(ii) Each level l is assigned a code word c of n bits, i.e., $c \in \{0,1\}^n$, e.g., for binary coding and $n = 3$, the levels can be coded as 000 (l_8) to 111 (l_1).
(iii) Categorize all the RSSI samples collected into two separate groups corresponding to packets exchanged on antenna A1 and A2. Calculate the mean of the samples in each group to decide their level l in the quantization process.
(iv) Each sample in the group is assigned the code word corresponding to level l assigned to the mean, and the sub block key k_{sb} is constructed.

As we have used devices with RF230 radio, the RSS of packets exchanged are in the range of 0 to -100 dBm.

4.2.3 Dynamic frequency hopping

After quantization, the CU and D consider lowest of RSSI levels obtained to decide the next channel to hop as per the following equation:

$$\text{New\_Channel} = ((\text{Cur\_Channel} - 11 + f) \bmod 16) + 11 \quad (3)$$

where $f = i$, the lowest RSSI level (l_i) obtained in the quantization scheme. For instance, for 3 bits/sample assignment, the whole RSSI range is divided into 8 equal levels - l_1 to l_8. If the current channel is 26 and the lowest RSSI level obtained for the mean of samples is $l_4(4^{th}$ level), then the next channel to hop is calculated as:
New_Channel = ((26 - 11 + 4) mod 16) +11 = 14.

4.3 Theoretical analysis

4.3.1 Improvement in entropy and bit rate

The entropy of final secret key is dependent on the entropy of channel samples (i.e., RSSI). The *estimated entropy* of channel samples can be calculated by the following equation:

$$E = -\sum_{\widetilde{h}} p(\widetilde{h}) \log_2 p(\widetilde{h}) \quad (4)$$

where $p(\widetilde{h})$ is the probability of occurrence of channel sample $\widetilde{h}$ in the captured samples. As per our protocol, all the RSSI collected on a particular antenna on each channel will be assigned a unique n bit code word though the individual samples may show little fluctuation around the mean value. The *estimated entropy* gives an upper bound on the number of bits that can be assigned per sample during quantization. This is explained in detail as follows:
(i) *CU with one antenna and a single channel:* Let the symbol s_1 denote the individual channel sample captured. The resulting set of channel samples S consists of same symbol s_1, i.e., $S = \{s_1\}$. The maximum *estimated entropy* E_{max} will be: $-((1)log_2(1)) = 0$, which means that any one bit arbitrary value e.g., bit 1 can be used to encode s_1. Thus, the resulting secret key also will have entropy = 0.
(ii) *Effect of frequency hopping:* If the CU uses single antenna and two channels, e.g., 11 and 20, then all the individual RSSI of each channel can be mapped to symbols s_1 and s_2 respectively. Now $S = \{s_1, s_2\}$, and $E_{max} = 1$. Thus, s_1 and s_2 can be assigned 1 bit code, e.g., 0 and 1 respectively. Hence, the resulting secret key will also have entropy > 0, compared to previous case depending on the occurrence of s_1 and s_2. Similarly, for 3 channels, $S = \{s_1, s_2, s_3\}$ and $E_{max} = 1.58$. Thus, 2 bits are required to encode each symbol s_1, s_2 and s_3. This further improves the entropy of final key and bit rate. Hence, for C different channels, S = $\{s_1, s_2, s_3, \ldots, s_C\}$ and E_{max} also increases which means that more bits can be assigned.
(iii) *Effect of dual-antennas with frequency hopping:* From our experimental results we have noticed that using single antenna and frequency hopping though helps to get more symbols in S, it spans nearly 25-35% of the total RSSI range available for the devices. This limits the maximum bit rate and key entropy that can be achieved. Thus, in order to exploit complete RSSI range available for the devices, we employ another antenna on the CU. Now, consider the case of the CU having two antennas. If we consider both the antennas of the CU as identical, then they must be separated by atleast half the wavelength of radio signal being used, i.e., 6.25 cm for 2.4 GHz. As iARC is designed for miniature WBAN devices, we place both the antennas very close to each other without any gap in between. With this setup and frequency hopping we get $S = \{s_1, s_2, s_3, \ldots, s_C\}$, which has no improvement compared to the CU with single antenna, as both the antennas are placed very close, they measure nearly the same RSSI while operating on same channel [11]. Thus, we have selected two omni-directional antennas with different features such that even when placed close to each other, the difference in RSSI measured on both the antennas in a same channel should be more than atleast the total range of RSSI covered by a single antenna by frequency hopping. By carefully selecting a pair of antennas which satisfy this condition, we can obtain double the number of symbols compared to single antenna case i.e., $S = \{s_1, s_2, s_3, \ldots, s_C, s_{C+1}, s_{C+2}, \ldots, s_{2C}\}$. This dra-

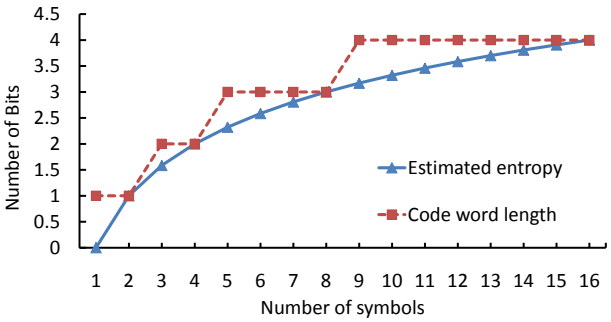


Figure 2: As the number of symbols increase, E_{max} and code word length also increase which improves the secret bit rate.

matically improves the maximum *estimated entropy* of channel samples and the secret key rate.

As there are 16 channels available in 2.4 GHz, the RSSI measured on few channels may have similar values as other channels [18]. Based on our experimental results, maximum 4 bits can be assigned per symbol (i.e., RSSI obtained on each channel on one antenna). Thus iARC dramatically improves *estimated entropy* of the channel samples (and hence the key entropy), and also the secret bit rate. Fig. 2 shows the theoretical estimation of maximum *estimated entropy* and code word length for increasing number of symbols in channel sample set S.

4.3.2 *Improvement in bit agreement*

In our scheme, the code to be assigned for each RSSI is decided based on the quantization level in which the 'mean' of all RSSI occur. Thus, practically when the RSSI samples are captured on the CU and D on a particular channel, though the RSSI are not exactly same, but the mean values calculated for both the devices occur in the same quantization level. This guarantees high bit agreement.

In rare cases due to sudden spikes in RSSI or for other reasons, the minimum of RSSI mean calculated on the CU and D for deciding the channel hopping may not be same, in which case the two devices may hop to different channels instead of hopping to same channel. In such cases, the devices notice if they do not get any probe/response packet on that particular channel. Thus, they can immediately terminate the key generation process and start from the beginning from the same channel as before. This ensures both the CU and D follow same channel hopping as well as both generate keys with high bit agreement.

5. EVALUATION AND RESULTS

We have used Opal sensor boards [9] to implement the CU and eavesdroppers with dual antennas. Iris motes, one of the commercial off-the-shelf (COTS) sensor platform were used for wearable devices D and eavesdroppers with single antenna. All the devices were operating in 2.4 GHz. TinyOS environment was used to program both the platforms. One of the major challenges in our design was to operate Opal in a controlled dual antenna mode. To achieve this, we have incorporated software modifications to the RF231 radio's low-level device driver layer of TinyOS. More details are available in our technical report [13].

We have validated the performance of our proposed key

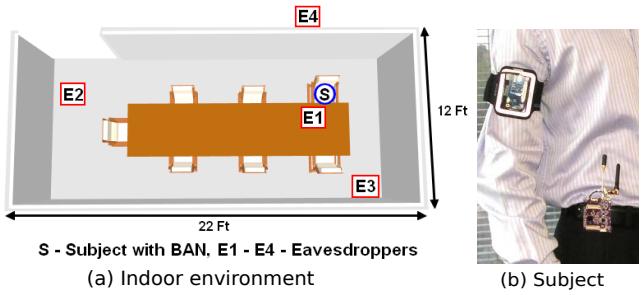


Figure 3: Experimental set-up.

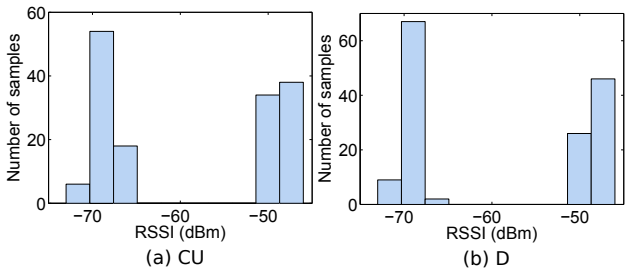


Figure 4: The histogram of RSSI samples collected by the CU and D on a single channel show same level l in the quantization process.

generation mechanism in different indoor environments, e.g., a medium sized conference room, cafeteria, and in a large room with multiple cubicles. In all these tests the performance of our protocol was nearly the same. In all these experiments the emphasis was to verify how our protocol performs in a static deployment scenario, e.g., a subject wearing the CU (on the waist) and a body worn device D (on the right arm) as shown in Fig. 3b sitting on a chair without any body movement.

5.1 Analysis of key extraction

Let us examine the shared secret key extraction mechanism between the CU and D by considering one of the data set from our experiments. For illustration purposes we provide the details of the experiments conducted in a conference room as shown in Fig. 3a. We had placed multiple eavesdroppers at different positions inside as well as outside the conference room (E1 was placed on the table). Fig. 4 shows the histogram of RSSI samples obtained by the CU and D on channel 26 during channel sampling in one of the experiments. We can notice that the total number of RSSI samples lying in the same range/quantization level l at both the legitimate devices are equal. Thus, both the CU and D follow same frequency hopping pattern for subsequent channel sampling. Both the CU and D derive secret keys with very high bit agreement when the size of the level selected by both the devices satisfies the requirement of the protocol.

Fig. 5a shows the secret bit rate of iARC for various probe intervals t and $n = 1$ to 4 (recall that n is the number of secret bits to be assigned per sample) in different indoor environments. In each environment, experiments were conducted for different inter packet intervals t, i.e., 100 ms, 50 ms, 10 ms, and 5 ms for the key generation. For each setting, we conducted 25 experiments with $N = 250$. Based

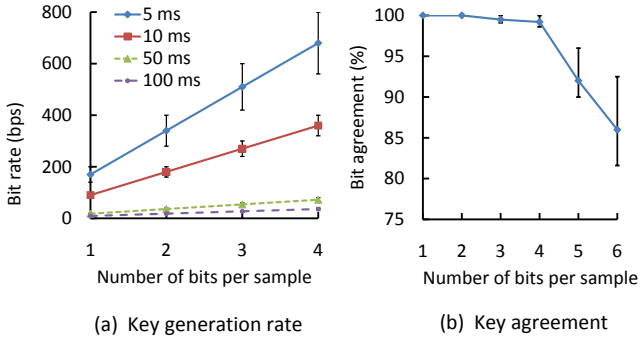


Figure 5: Performance analysis of iARC.

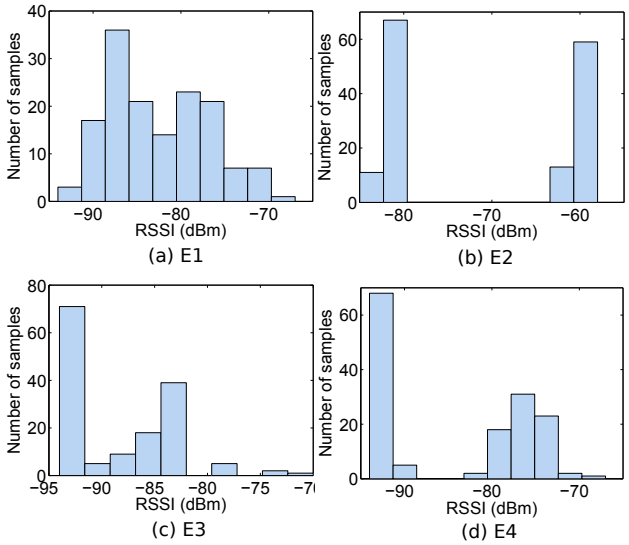


Figure 6: The histogram of RSSI samples measured by different eavesdroppers show different levels in the quantization than those of the CU and D.

on our observations, assigning 3 or 4 bits per sample is appropriate as it results in high entropy ≈ 0.92 to 0.99 and highest bit agreement as shown in Fig. 5b. However, the bit assignment $n > 4$ resulted in bit mismatches at the CU and D, and hence we have used 3 and 4 bit assignment scheme in all our tests. Thus, the maximum bit rate that can be achieved using our proposed protocol is 800 bits per second. Our protocol requires only 160 ms and 32 probe exchanges to generate a 128 bit key, which is nearly 100 times faster compared to the most recent scheme in WBAN [17].

We have performed the NIST [10] entropy test to check the randomness of keys. For $n = 3$ and 4, the keys generated by our protocol pass the NIST test with entropy varying from 0.92 to 0.99, which proves that our design is suitable to be employed in practical applications.

5.2 Secret key bits vs antenna switching

One might be interested to know whether learning the antenna switching pattern helps to guess the bits of final key. As explained in Section 4.1.1, iARC employs random antenna switching based on the random string $r \in \{0,1\}^{128}$ generated by PRNG. Thus, before channel sampling r is known only to the CU. Once the CU and D start exchanging probe/response packets, the RSSI value of packets exchanged depends on the distance between the CU and D and also on the channel being used. In iARC, since the final key is divided into multiple sub blocks and each sub block of the key is extracted in a different channel, the CU will not have any prior knowledge about the bits of final key. This is because, each RSSI sample is assigned 3 or 4 bits based on its level l in the quantization process. The final key K is extracted by the concatenation of the bit strings derived in each channel. Thus, the final key K is independent of r.

Table 1: Mutual information between the CU and different nodes for various probe intervals.

Device type		Mutual information (bits)		
		$t = 250$ ms	$t = 50$ ms	$t = 5$ ms
Single antenna				
	D	0.9235	0.9393	0.9279
	E1	0.0587	0.0147	0.0513
	E2	0.0766	0.0261	0.0156
	E3	0.0010	0.0816	0.0179
	E4	0.0449	0.0402	0.0029
Dual antenna				
	E1	0.0621	0.0253	0.0718
	E2	0.0545	0.0182	0.0491
	E3	0.0797	0.0374	0.0183
	E4	0.0358	0.0144	0.0216

6. SECURITY ANALYSIS

6.1 Estimation of shared randomness between the CU and D

The main factor influencing the performance of key generation is the shared randomness which can be quantified by computing the Mutual Information (MI) [5] by using channel estimates (i.e., RSSI). A large mutual information implies more shared information between the two parties. From Table 1 it is clear that MI between the CU and D is ≈ 1 bit, which shows that the CU and D have enough shared randomness to generate robust keys.

6.2 Passive adversary

Consider Fig. 6 which shows the RSSI samples captured by different eavesdroppers during channel sampling when all the parties (CU, D and eavesdroppers) were operating on the same channel (channel 26). It can be noticed that the RSSI samples in all the sub figures lie in different range/levels than those of the CU and D in Fig. 4. From Fig. 6 we can notice that the RSSI samples captured by the eavesdropper E2 situated in line-of-sight (LOS) with CU/D are well separated in two different ranges, similar to the CU/D, but will have different RSSI levels l in quantization process. On the other hand, for the adversaries which are in non-line-of-sight (NLOS) with the WBAN devices, RSSI values are scattered at various levels due to multi-path effect of the indoor environment on radio signal. Even if the eavesdropper succeeds to capture some of the initial packets exchanged between the CU and D, she cannot follow the *dynamic frequency hopping scheme* used by CU/D, which is dependent on the level of RSSI mean obtained. Thus, the eavesdroppers fail to capture subsequent packets exchanged by the CU and D and hence cannot reproduce the same key as CU/D.

In order to analyze the security in the presence of eavesdroppers with dual-antennas, we repeated the static channel experiments by replacing Iris motes used as eavesdroppers by Opal boards. More details are presented in our report [13]. Table 1 shows that the mutual information obtained by eavesdroppers is very minimal and is close to 0 in contrast to the high mutual information between the CU and D. It should be noted that, any attempt by the adversary to process the received signal would further reduce the MI, hence *collusion attack* is not possible [13]. Thus, the eavesdroppers cannot derive the same key as CU/D.

6.2.1 Brute force attack

It is important to analyze whether an adversary can guess the channel samples and reproduce the key by using her partial channel observations. As the eavesdropper has no information about the RSSI levels obtained by the CU/D and also the order in which the samples are captured on different antennas of CU, she can use her computational capabilities to reproduce the key by guessing the RSSI levels of channel samples to all possible options. However, the probability of an eavesdropper reproducing the same key as CU/D depends on the key length. Considering the 3 bits/sample assignment scheme, if the number of probes or samples exchanged is 1, then the probability of Eve cracking the key is 0.125 (i.e., 1/8). For a 128 bit key, the probability of Eve guessing the same key is very low $= 1.469 \cdot 10^{-39}$ ($\approx 2^{-129}$). Similarly, if 16 levels are used for quantization (4 bits/sample), then the Eve's probability to reproduce the key is as low as $2.93 \cdot 10^{-39}$ ($\approx 2^{-128}$), which is negligible.

6.3 Active adversary

In case of MIM attack, the CU and D can use information about RSSI of previous packets exchanged between the two when they detect a suspicious packet with large RSSI deviation, and discard if it is not within the expected range [13]. If channel jamming is encountered, the CU and D employ frequency hopping to continue key generation [13].

7. CONCLUSION AND FUTURE WORK

In this paper, we have presented a novel protocol – iARC, an RSSI based secret key generation scheme for wearable devices which is independent of node mobility. iARC protocol employs dual antennas and frequency diversity for inducing artificial randomness in the channel. Our experimental results reveal that the combined effect of dual antennas and frequency diversity improves performance of key generation by an order of magnitude as compared to the existing schemes [4, 17]. iARC substantially reduces the number of packets exchanged and the time required to derive the secret key in stable channel conditions. iARC generates 128 bit key with very high bit agreement in just 160 ms with a secrecy capacity of 800 bps. The keys generated by our protocol pass the NIST test for approximate entropy, which suggests that our scheme is suitable for practical applications.

Another possible direction to induce artificial randomness is to vary the power levels of transceivers. Designing such a scheme would require significant changes in the software stack and should be supported by the sensor platforms which we would like to explore in our future work.

8. ACKNOWLEDGEMENT

This work is partially supported by Australian Research Council Discovery grant DP150100564.

9. REFERENCES

[1] Comparison of wearable devices. http://allthingsd.com/. Accessed: 01-June-2015.

[2] IEEE 802.15 WPAN Task Group 6 (TG6) Body Area Networks. http://www.ieee802.org/15/pub/TG6.html. Accessed: 01-June-2015.

[3] Wearable device revenues to grow to USD 6B in 2018. http://mobihealthnews.com. Accessed: 01-June-2015.

[4] S. T. Ali, V. Sivaraman, and D. Ostry. Zero Reconciliation Secret Key Generation for Body-worn Health Monitoring Devices. In *ACM WiSec*, 2012.

[5] T. M. Cover and J. A. Thomas. *Elements of Information Theory*. John Wiley, 1991.

[6] L. W. Hanlen, D. Smith, J. A. Zhang, and D. Lewis. Key-sharing via Channel Randomness in Narrowband Body Area Networks: Is Everyday Movement Sufficient? In *BodyNets*, 2009.

[7] C. Javali, G. Revadigar, M. Ding, and S. Jha. Secret Key Generation by Virtual Link Estimation. In *Proc. EAI International Conference on Body Area Networks (BodyNets)*, 2015.

[8] 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 *RFIDsec*, 2014.

[9] R. Jurdak, K. Klues, B. Kusy, C. Richter, K. Langendoen, and M. Brünig. Opal: A Multi-radio Platform for High Throughput Wireless Sensor Networks. *IEEE Embedded Systems Letters*, 3(4):121–124, Nov 2011.

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

[11] T. S. Rappaport. *Wireless Communications: Principles and Practice* . Prentice Hall PTR, 2001.

[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 *ACM ASIACCS*, 2014.

[13] G. Revadigar, C. Javali, H. Asghar, K. Rasmussen, and S. Jha. Secret Key Generation for Body-worn Devices by Inducing Artificial Randomness in the Channel. *Technical Report UNSW-CSE-TR-201506, UNSW Australia*, 2015.

[14] G. Revadigar, C. Javali, W. Hu, and S. Jha. DLINK: Dual Link Based Radio Frequency Fingerprinting for Wearable Devices. In *IEEE LCN*, 2015.

[15] M. Rostami, A. Juels, and F. Koushanfar. Heart-to-Heart (H2H): Authentication for Implanted Medical Devices. In *ACM CCS*, 2013.

[16] S. S Keller. NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms. *NIST Technical report*, 2005.

[17] L. Shi, J. Yuan, S. Yu, and M. Li. ASK-BAN: Authenticated Secret Key Extraction Utilizing Channel Characteristics for Body Area Networks. In *ACM WiSec*, 2013.

[18] M. Wilhelm, I. Martinovic, and J. B. Schmitt. Secret Keys from Entangled Sensor Motes: Implementation and Analysis. In *ACM WiSec*, 2010.