Secret Key Generation for Body-worn Devices by Inducing Artificial Randomness in the Channel

Girish Revadigar[1,2] Chitra Javali[1,2] Hassan Jameel Asghar[2]
Kasper B. Rasmussen[3] Sanjay Jha[1]

[1] School of Computer Science & Engineering
UNSW Australia, Sydney, Australia
{girishr,chitraj,sanjay}@cse.unsw.edu.au
[2] National ICT Australia (NICTA), ATP Sydney, Australia
hassan.asghar@nicta.com.au
[3] Dept. of Computer Science, University of Oxford, Oxford, UK
kasper.rasmussen@cs.ox.ac.uk

Technical Report
UNSW-CSE-TR-201506
May 2015

THE UNIVERSITY OF
NEW SOUTH WALES

SCIENTIA
MANU ET MENTE

School of Computer Science and Engineering
The University of New South Wales
Sydney 2052, Australia

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, a.k.a. session key dynamically. These schemes have very low bit rate capacity, and, in the absence of node mobility, they 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. iARC induces artificial randomness in the channel by employing dual antennas and dynamic frequency hopping effectively on resource constrained devices. We conduct an extensive set of experiments in real time environments on sensor platforms to validate the performance of iARC. To the best of our knowledge, iARC is the first WBAN protocol to extract secret keys with good entropy and high bit rate in static channel conditions. iARC has 800 bps secrecy capacity and generates 128 bit key in only 160 ms.

Keywords: Wireless 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). WBANs typically consists of a central node called Control Unit (CU) and few miniature devices having wireless capability and equipped with sensors/actuators, which are either implanted in the human body, called Implanted Medical Devices (IMD) or wearable on body to monitor vital signals related to health. The CU and other sensor devices in WBAN communicate with each other through wireless link to collect and process health information. Additionally, in a remote health-care system, CU can communicate with the cloud based remote server for timely exchange of information.

Several wearable devices like FitBit Flex, JawBone's Up, and Nike+ FuelBand [2] 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 [8].

Although technological advancement has lead to wireless capability of tiny 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 tiny and resource constrained, the complex traditional cryptographic key establishment schemes would not be feasible. Instead, the devices need fast, secure, reliable, unbreakable, and lightweight security mechanisms. It is crucial for the devices to derive the shared secret key dynamically to avoid the threat of compromise and privacy leakage. The IEEE standard 802.15.6 for WBAN [3] has mandated the renewal of shared secret keys used by WBAN devices periodically in order to safeguard themselves against all possible attacks. The IEEE 802.15.6 Technical Requirements Document states, *"The mechanism should be energy efficient and lightweight. When supported, the highest level of security shall be equal to or stronger than that provided by AES (Advanced Encryption Standard) 128 bits (FIPS-197)"*. Hanlen et al. [16] have analyzed the above security requirement and recommend the 128 bit key renewal process every minute for the highest level of security in WBANs.

Recent studies [11, 12, 17, 20] have proposed schemes for generating shared secret keys using physical layer characteristics. It has been demonstrated that in a wireless network, two devices Alice (A) and Bob (B) exchanging a number of packets repeatedly can extract shared secret key from the observed variation in channel characteristics – received signal strength indicator (RSSI) or channel impulse response (CIR), which are highly correlated due to the reciprocity property of the wireless channel.

RSSI based security schemes are well suited for WBAN devices as it can be easily measured by every wireless device directly from the received packet without the need of special hardware. The existing schemes [9, 10, 24] 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 can be generated during the activities involving sufficient body movements. However, the above schemes have very low bit rate capacity. On the other hand, when the channel is static (i.e., in the absence of node mobility) the existing schemes fail to generate keys with good entropy [17]. An eavesdropper can easily reproduce the same key by observing the channel. This poses a major security threat. We demonstrate this security issue further in Section 3. 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., person at home/workplace), or sleeping on the bed (e.g., in home or critical care sections/wards of hospitals) are quite common, in which case the existing schemes cannot be used.

Prior schemes [9–11, 17, 20, 24] employ filters which selectively discard samples not contributing to the key generation and hence need a large number of samples to choose from. Also, reconciliation methods [12] have been employed for correcting discrepancy in the key generated. Thus, these procedures expect the devices to sample the wireless channel frequently by exchanging too many packets, resulting in significant overhead for resource constrained devices. Although prior schemes have demonstrated key generation in the dynamic channel, the challenge of generating robust secret keys in the absence of node mobility is still an open question.

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 study the effect of using dual antennas and frequency diversity for improving randomness of the channel samples in static cases. We present an RSSI based pair-wise shared secret key generation scheme and 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 pure static channel conditions. Our proposed scheme, iARC, completely eliminates the expensive steps of key generation: filtering, reconciliation and privacy amplification, which makes it 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) [26] 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 low powered, resource constrained and chip based without MIMO capability, hence, the protocols available for WiFi cannot be directly applied to WBAN. To the best of our knowledge, SeAK [18] is the only work in the literature which uses dual antennas for initial trust establishment of WBAN devices. 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 Opal [19], an RF231 radio based wireless sensor platform with multiple antenna architecture and Iris motes [4] operating in 2.4 GHz frequency band and used TinyOS [6] environment to program the devices. We have conducted extensive set of experiments to validate our protocol in different real-time environments.

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

- We prove experimentally that the existing schemes for secret key generation in WBAN are not suitable in the absence of node movement.
- We propose iARC – a novel, lightweight, RSSI based pair-wise 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 (i.e., static channel cases).
- We propose a multiple bit extraction algorithm to reduce the number of packets exchanged during key generation and overall time taken for generating perfectly matching shared secret keys.
- We demonstrate experimentally that, iARC achieves the highest bit rate capacity of 800 bps with high bit agreement between the two legitimate body-worn devices, and generates 128 bit key in 160 ms.

To the best of our knowledge, the work presented in this paper is the first mobility independent physical layer based pair-wise secret key generation mechanism for resource constrained devices of WBAN. We have evaluated the randomness of keys generated by our proposed protocol using NIST [5] 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. Section 2 explains the preliminaries required to understand the key generation process. An experimental analysis of existing schemes is presented in Section 3. The system model in Section 4 presents our assumptions and threat model. Section 5 explains our novel approach of inducing artificial channel randomness and key generation. Our implementations details are given in Section 6. Section 7 describes our experimental set-up, detailed evaluation of the proposed protocol iARC and results. In Section 8 we present the security analysis of iARC. Section 9 gives details about the related work and in Section 10 we give concluding remarks.

2 Preliminaries

In this section, we provide a brief overview of different stages involved in the secret key generation and evaluation metrics used.

2.1 Steps involved in secret key generation process

Following are the steps involved in secret key generation:
1. Channel sampling: Two legitimate communicating parties sample the wireless channel n times within a small duration of time t, and measure the same mutually agreed channel characteristics, e.g., RSSI [14,17,20], or CIR [20].
2. Quantization: A bit stream is extracted from the sampled measurements using approaches like level crossing [20], ranking [10], etc.

3. Reconciliation: Due to random noise in the channel and differences in the transceivers, there will be some discrepancy in the bit-stream generated by the two parties. This mismatch is corrected by using suitable error correction methods [12].
4. Privacy amplification: During information reconciliation the eavesdropper obtains partial information about the key. Hence to obtain the key which is independent of the eavesdropper's partial information privacy amplification is performed. The key entropy is increased by simple transformations like XOR operation, or by discarding mutually agreed bits.

2.2 Evaluation of key extraction mechanism

The performance of secret key extraction scheme is evaluated using the following metrics:
1. Bit rate: denotes the average number of bits generated/extracted from the channel per unit time and is usually measured in 'bits per second'.
2. Key agreement: represents the percentage of bits matching in the secret keys generated by two parties. Ideally this should be equal to 100% for legitimate devices.
3. Entropy: is the measure of uncertainty or randomness in the generated key. The entropy value of 1 denotes highest level of entropy for binary symbols.

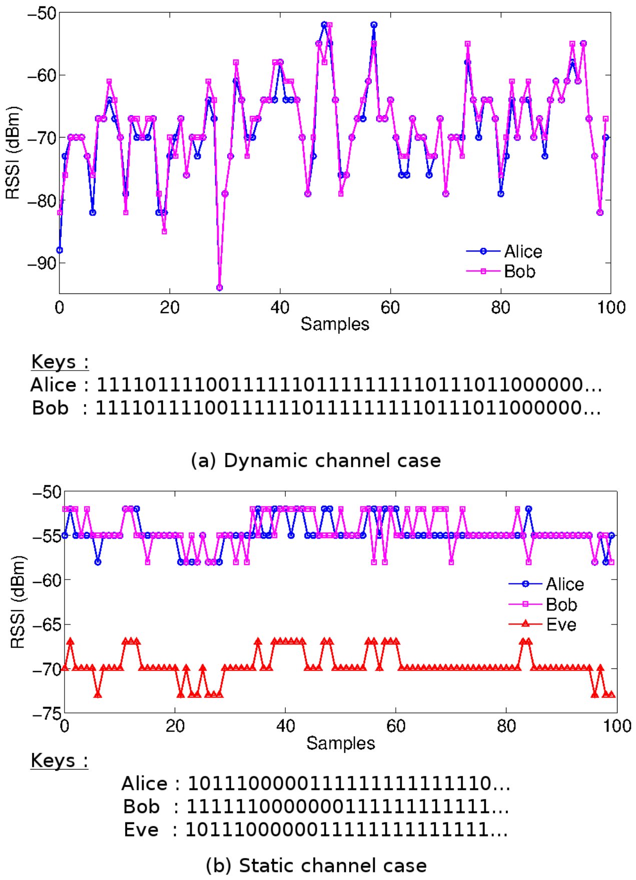
3 Analysis of mobility based key generation schemes

In this section we demonstrate that, existing secret key generation schemes [9,10] dependent on node mobility are not suitable for static channel conditions.

We implemented the existing secret key generation schemes using Iris motes. Two sensor nodes were placed on a subject's body, one on the waist and other on the right arm representing Alice and Bob respectively. Two separate experiments were conducted to evaluate the key generation (i) with node motion, and (ii) stable channel condition, i.e., without body movement. The experiments were conducted in an indoor environment with multiple cubicles.

In the first experiment, the subject wearing the devices was walking slowly at a speed of about 1 m/s. Alice broadcasts simple probe packets at an interval of 100 ms. Upon receiving a packet, Bob measures the RSSI and sends a reply packet. Alice measures the RSSI of the packet received. The test was conducted for about 5 minutes. Fig. 3.1a shows the variation in the RSSI observed by Alice and Bob during body motion. It can be observed that, the RSSI pattern has sufficient fluctuation and both the parties generate keys with good entropy by using level crossing algorithms.

In the second experiment, the subject was sitting on a chair and resting without performing any body movements, simulating a static channel condition. Another node acting as an eavesdropper (Eve) was placed on a nearby table in line of sight to body-worn devices at about 1 m from subject's position. Alice and Bob repeat the packet exchange process similar to first experiment. Fig. 3.1b shows the RSSI variations observed by Alice, Bob and Eve for the static channel test. It can be observed that, as the positions of Alice and Bob are fixed, the RSSI of all the packets received by Alice and Bob are nearly the



Keys :
Alice : 111101111001111110111111111101110110000000...
Bob : 111101111001111110111111111101110110000000...

(a) Dynamic channel case

Keys :
Alice : 1011100000011111111111110...
Bob : 1111110000000111111111111...
Eve : 1011100000011111111111111...

(b) Static channel case

Figure 3.1: Performance analysis of existing secret key generation schemes: Channel characteristics observed by different parties during dynamic channel with body motion show sufficient fluctuation required to get good entropy keys. However, in static channel case without node mobility, the keys generated will have low bit rate and low entropy, which an eavesdropper can reproduce easily.

same with little fluctuation. Thus, when both the parties generate keys using level crossing algorithm which uses local maxima and minima of RSSI samples, the keys generated will have very low entropy with long sequence of 0/1s. Many of the RSSI samples not contributing to key generation are discarded by the scheme, which results in the reduced bit generation rate. Now consider the RSSI variation observed by Eve. As Eve is also static and is present at a different location, even-though she receives degraded RSSI values, the channel variation observed by Eve will be highly correlated to that of legitimate devices. Fig. 3.1b shows the RSSI variation observed by Eve while Alice was transmitting the packets. Thus, Eve can also extract the same key with upto 85-90% accuracy using local maxima and minima of RSSI. As Eve has obtained sufficient information about the key generated by Alice-Bob, then by using her computational capability she can guess the remaining mismatching bits easily to generate the final key [20].

4 SYSTEM MODEL

Motivated by the incapability of existing schemes to generate keys during stable channel conditions, we propose our novel approach of inducing artificial channel randomness and protocol for key generation.

4.1 Assumptions

We assume that all the devices of WBAN have wireless networking capability in 2.4 GHz frequency band. There is one Control Unit (CU) which acts as an aggregator for the sensor data, and one or more wearable sensor devices (D) which can send/receive packets with the CU. We assume that the CU and D are in line of sight. The CU is present either on-body or off-body and is within the communicating range of the sensor devices, typically 1 meter. The CU is equipped with dual antennas, and the sensor devices (D) have single antenna. CU uses two different antennas A1 and A2 having different features. The antenna A1 has range equivalent to any Low Rate Wireless Personal Area Network (LRWPAN) devices, whereas A2 has a very short range to cover the WBAN of a person. CU uses A1 to communicate with the remote Base Station (BS) located in the room/building. In order to communicate with the devices of WBAN, CU may use either A1 or A2. CU uses both A1 and A2 during secret key generation with WBAN devices. The CU employs a pseudo-random number generator (PRNG) to generate a random bit string $r \in \{0,1\}^{128}$ which is 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. Our primary focus is to derive shared secret keys, a.k.a. session keys which are renewed periodically or after every session between a pair of devices, especially, between the CU and body-worn device D. It is assumed that the CU and other body-worn devices are not compromised.

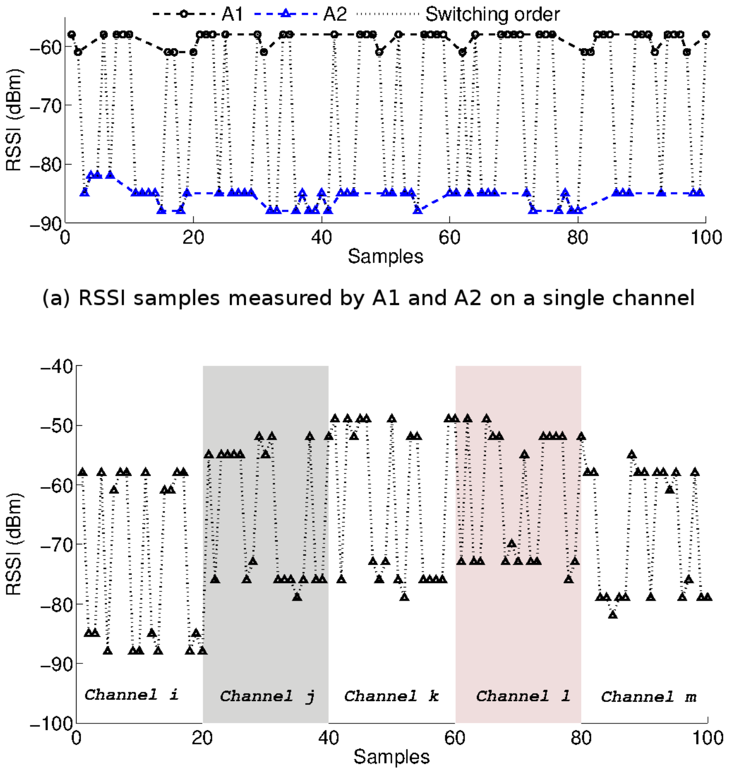
4.2 Threat model

We consider the presence of one or more on-body or 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 CU and the device D.

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.

5 PROTOCOL DESIGN

In this section, we present the details of our protocol for inducing artificial channel randomness and secret key generation.



(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 5.1: The CU induces artificial channel randomness by effectively combining random antenna switching and dynamic frequency (channel) hopping during channel sampling.

5.1 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 [21].

Our system uses dual antennas and frequency diversity for inducing artificial channel randomness required for secret key generation. The following subsections describe the steps involved in detail.

Employing dual antennas

In static channel conditions, for a fixed distance between CU and D, suppose that 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. 5.1a. 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 [22]. This PRNG is a cryptographically secure, NIST recommended random number generator which uses AES as the block cipher [23]. 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 [3], we use a 128 bit seed, i.e., $s \in \{0, 1\}^{128}$. From an attacker's point of view, guessing this 128 bit seed is highly improbable. Since this seed is changed every time during the key renewal, and given that the keys are renewed frequently, this becomes the problem of a moving target for an attacker, and hence *brute force attack* is infeasible.

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. 5.1a. Antenna switching improves randomness of the samples collected, and also the key generated. A detailed evaluation of key generation is discussed in Section 7.

Exploiting frequency diversity

iARC exploits frequency diversity by employing our novel *dynamic frequency hopping* scheme, which is explained in detail in Section 5.2. Our scheme adopts channel 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 [25]. 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 5.1 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. 5.1b and hence the secret key bits. The center frequency F_c (MHz) of each channel in 2.4 GHz is given by

$$F_c = 2405 + 5(\eta - 11) \tag{5.1}$$

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

Thus, the combined effect of random antenna switching and dynamic frequency hopping induces artificial channel variation between CU and body-worn device D, which boosts the entropy of channel and helps to extract good quality keys at both ends. On the other hand, an adversary located at a different place will not be able to follow the channel hopping pattern of CU/D and antenna switching order based on her channel observation, and cannot reproduce the secret key. A detailed security evaluation of the proposed protocol is presented in Section 7.

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

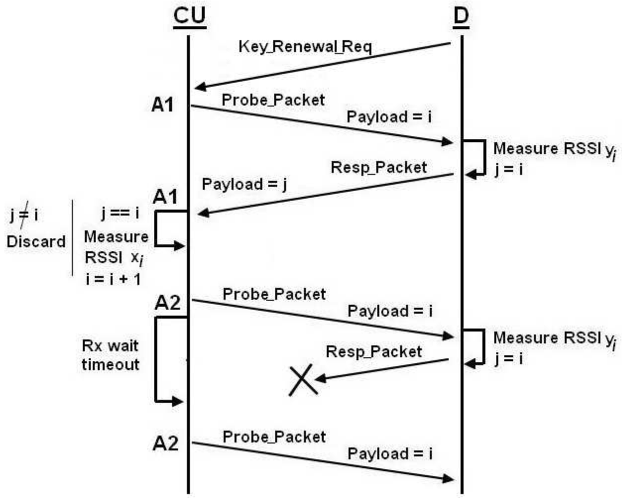


Figure 5.2: The protocol followed by the CU and D for channel sampling on a particular channel. The CU and D exchange multiple probe-response packets and measure the RSSI. The CU employs random antenna switching during channel sampling.

5.2 Key generation process

The secret key generation process consists of the following steps:

1. Channel sampling/measurements
2. Quantization and multiple bit assignment
3. 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 shown by the following equation:

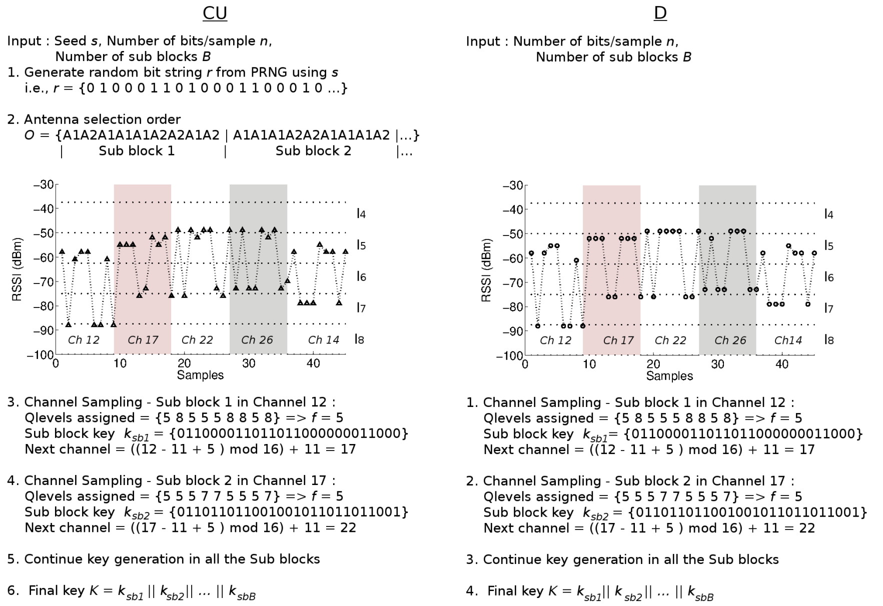
$$K = k_{sb1} \parallel k_{sb2} \parallel \ldots \parallel k_{sbB} \tag{5.2}$$

The CU and D perform channel sampling, quantization and frequency hopping repeatedly until the total number of probes N required for key generation are exchanged.

It is worth noticing that, prior key generation schemes [9, 10, 20, 24] employ additional steps like *Filtering, Reconciliation and Privacy amplification.* iARC eliminates the above mentioned expensive steps which makes it extremely lightweight.

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



CU

Input : Seed s, Number of bits/sample n,
Number of sub blocks B

1. Generate random bit string r from PRNG using s
i.e., r = {0 1 0 0 0 1 1 0 1 0 0 0 1 1 0 0 0 1 0 ...}

2. Antenna selection order
O = {A1A2A1A1A1A2A2A1A2 | A1A1A1A2A2A1A1A1A2 |...}
| Sub block 1 | Sub block 2 |...

3. Channel Sampling - Sub block 1 in Channel 12 :
Qlevels assigned = {5 8 5 5 5 8 8 5 8} => f = 5
Sub block key k_{sb1} = {011000011011011000000011000}
Next channel = ((12 - 11 + 5) mod 16) + 11 = 17

4. Channel Sampling - Sub block 2 in Channel 17 :
Qlevels assigned = {5 5 5 7 7 5 5 5 7} => f = 5
Sub block key k_{sb2} = {011011011001001011011011001}
Next channel = ((17 - 11 + 5) mod 16) + 11 = 22

5. Continue key generation in all the Sub blocks

6. Final key $K = k_{sb1} \| k_{sb2} \| \ldots \| k_{sbB}$

D

Input : Number of bits/sample n,
Number of sub blocks B

1. Channel Sampling - Sub block 1 in Channel 12 :
Qlevels assigned = {5 8 5 5 5 8 8 5 8} => f = 5
Sub block key k_{sb1}= {011000011011011000000011000}
Next channel = ((12 - 11 + 5) mod 16) + 11 = 17

2. Channel Sampling - Sub block 2 in Channel 17 :
Qlevels assigned = {5 5 5 7 7 5 5 5 7} => f = 5
Sub block key k_{sb2} = {011011011001001011011011001}
Next channel = ((17 - 11 + 5) mod 16) + 11 = 22

3. Continue key generation in all the Sub blocks

4. Final key $K = k_{sb1} \| k_{sb2} \| \ldots \| k_{sbB}$

Figure 5.3: Secret key extraction in iARC : The CU generates a random bit string r from PRNG using secret seed s to determine the antenna switching order. The CU and D perform channel sampling, quantization and dynamic frequency hopping to derive sub block keys. The final key K is then obtained by the concatenation of all the sub block keys.

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 values 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 CU may use the same antenna or switch to another antenna for the next probe packet transmission based on the random string r. If CU does not receive any reply from D within timeout interval t_o, CU retransmits the probe packet with the index i. D updates y_i with the RSSI of latest packet received. Fig. 5.2 shows the protocol for channel sampling.

Let $h_{cd}(t)$ denote the channel related information estimated by D on its antenna d at time t for the packet sent by CU on antenna c, where $d = \{1\}$ and $c = \{1, 2\}$ are antenna numbers. Similarly, let $h_{dc}(t')$ represent the channel estimation by CU on its antenna c (used for packet transmission at time t) at time t' for the response packet sent by D using antenna d. When CU and D exchange multiple probe/response packets, the sequences $\mathbf{h}_{cd} = [h_{cd}(t_\tau)]$ and

$\mathbf{h}_{dc} = [h_{dc}(t'_\tau)]$ represent the channel estimates by CU and D required for key generation, where $\tau = \{1,\ 2,\ \ldots,\ T\}$. As the two parties sample the channel in quick succession, the estimates $h_{cd}(t)$ and $h_{dc}(t')$ will be highly correlated due to channel reciprocity.

On the other hand, consider an eavesdropper located at a distance more than half the wavelength of radio signal being used from CU/D. Let $e = \{1\}$ represent the antenna number of eavesdropper. The channel estimates by eavesdropper from overheard packets sent from CU, are calculated as $\mathbf{h}_{ce} = [h_{ce}(t_i)]$ which will be uncorrelated with the estimates of CU/D as the channel characteristics between the CU and eavesdropper will be different than those between the CU and D because of multi-path effects and noise in the environment. Thus, despite possessing knowledge of the channel sample, eavesdropper cannot compute meaningful estimates of the channel between the CU and D.

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 explained below:

- 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 $L = 2^n$.
- Each level l is assigned a code word c of n bits, i.e., $c \in \{0,1\}^n$. For e.g., for binary coding and $n = 3$, the levels can be coded as 000 (l_8) to 111 (l_1).
- Categorize all the RSSI samples collected into two separate groups, each with nearly same RSSI [2]. Calculate the mean of the samples in each group to decide its level l in the quantization process.
- Each sample is assigned the code word based on its level l, and the sub block key k_{sb} is constructed.

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:

$$New\_Channel = ((Cur\_Channel - 11 + f) \bmod 16) + 11 \tag{5.3}$$

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 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.

[2] The RSSI of packets exchanged using A1 and A2 on a particular channel will have two distinct levels.

As we have used devices with RF230 radio, the RSS of packets exchanged are in the range of 0 to -100 dBm. The secret key generation process in iARC is illustrated in Fig. 5.3 by considering channel 12 as the initial channel, number of bits/sample $n = 3$ with binary coding, and the number of sub blocks $B = 5$. For 128 bit key, the total number of samples required are $N = 43$, and 9 samples are exchanged in each sub block.

5.3 Theoretical analysis

In this section, we present theoretical analysis of entropy, bit rate, and bit agreement improvement achieved by employing dual-antennas and frequency hopping.

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 [26]:

$$E = -\sum\nolimits_{\widetilde{h}} p(\widetilde{h}) \log_2 p(\widetilde{h}) \tag{5.4}$$

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 values collected on a particular antenna on each channel will be assigned a unique n bit code word. For e.g., all the samples collected on antenna 1 on channel 16 are assigned the same n bit code word, though the individual samples may have 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 only one antenna and operating on a single static channel:* Let the symbol s_1 denote the individual channel sample captured by the CU on one particular channel though their actual RSSI vary slightly. It is evident that the resulting set of channel samples S consists of same symbol s_1, i.e., $S = \{s_1, s_1, s_1, ...\}$. Since the probability of occurrence of s_1 is 1, the *estimated entropy* of such set is: $-((1)log_2(1)) = 0$, 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, which cannot be used for practical applications.

(ii) *Effect of frequency hopping:* Now, let us consider that the CU uses single antenna and two channels for channel sampling, say channel 11 and channel 20. All the individual RSSI of channel 11 can be mapped to symbol s_1 and all individual RSSI on channel 20 are mapped to symbol s_2. Now the resulting set of channel samples consists of two symbols s_1 and s_2. Thus, considering equal probability of occurrence for each symbol, the maximum *estimated entropy* is: $E = -(p(s_1)log_2p(s_1) + p(s_2)log_2p(s_2)) = -((0.5)log_2(0.5) + (0.5)log_2(0.5)) = 1$. Thus the symbols 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 samples s_1 and s_2. Similarly, for 3 channels, S consists of symbols s_1, s_2, s_3 and the maximum *estimated entropy* = 1.58. Thus, 2 bits are required to encode each symbol s_1- s_3. This further improves the entropy of final key and as more number of bits are generated per sample, the bit rate also improves compared to all previous cases. As the CU employs more channels for channel sampling, the resulting set of samples S consists of different symbols $\{s_1, s_2, s_3, ... s_c\}$ corresponding to RSSI on c different channels. The maximum *estimated entropy* also increases which means that more bits can be assigned per channel sample.

(*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 the set of channel samples, 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 all the 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 set-up, when the CU uses dual-antennas and frequency hopping for channel sampling, the resulting set of channel samples S still consists of same number of symbols $\{s_1, s_2, s_3, ... s_c\}$ corresponding to RSSI on c different channels. This has no improvement compared to the CU with single antenna, as both the identical antennas are placed very close, they measure nearly the same RSSI while operating on same channel. 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. Now by carefully selecting a pair of antennas which satisfy this condition, we can obtain double the number of symbols in channel sample set compared to single antenna case i.e., $S = \{s_1, s_2, s_3, ..., s_c, s_{c+1}, s_{c+2}, ..., s_{2c}\}$. This dramatically improves the maximum *estimated entropy* of channel samples and the secret key rate.

As there are 15 channels available in 2.4 GHz, the RSSI measured on some channels may have similar values as other channels [25]. 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. 5.4 shows the theoretical estimation of maximum entropy and code word length for increasing number os symbols in channel sample set S.

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 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

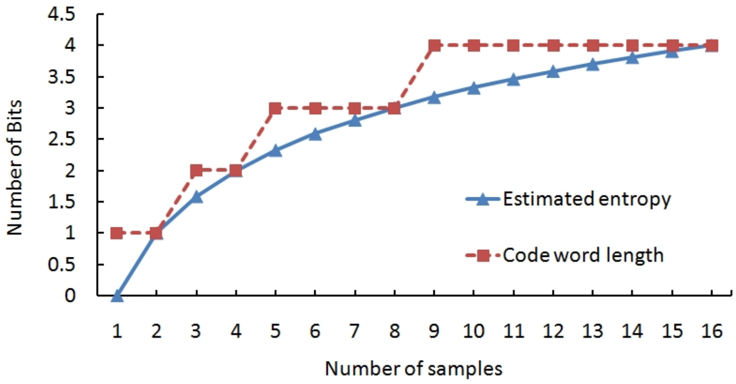


Figure 5.4: The maximum *estimated entropy* of channel sample set S increases as the number of different samples corresponding to RSSI on each channel increases. The number of bits required to encode each symbol also increases which dramatically improves secret bit rate.

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.

6 IMPLEMENTATION

This section describes the implementation details of our proof of concept.

We have used Opal sensor boards [19] to implement the CU and eavesdroppers with dual antennas. Iris motes [4], one of the commercial off-the-shelf (COTS) sensor platform operating in 2.4 GHz were used for wearable devices D and eavesdroppers with single antenna. TinyOS [6] environment was used to program both the platforms.

Opal sensor platform is based on RF231 radio [1] and supports dual antenna connectivity. Iris motes also have the same radio with single antenna.

One of the major challenges in our design was to operate Opal in a controlled dual antenna mode. Opal can be operated in single antenna mode or in dual antenna diversity mode. In the latter mode, the antenna with highest signal strength is used by the device for packet reception. As per our protocol design, CU should be able to select individual antenna for each packet transmission and reception and switch between the antennas on-the-fly while the radio driver software is already running in the TinyOS stack. This functionality is not available in the default TinyOS platform. In order to enable the CU to access and switch between its two antennas dynamically on per packet basis, we have incorporated software modifications to the RF231 radio's low-level device driver layer of TinyOS [18]. Fig. 6.1 shows the TinyOS stack with our implementations. No special software changes in TinyOS were required for Iris motes.

In iARC, as the CU employs dual antennas, one would like to know how this affects the battery life of the miniature devices. In our design, antenna selection is performed via application software. At any point of time during key

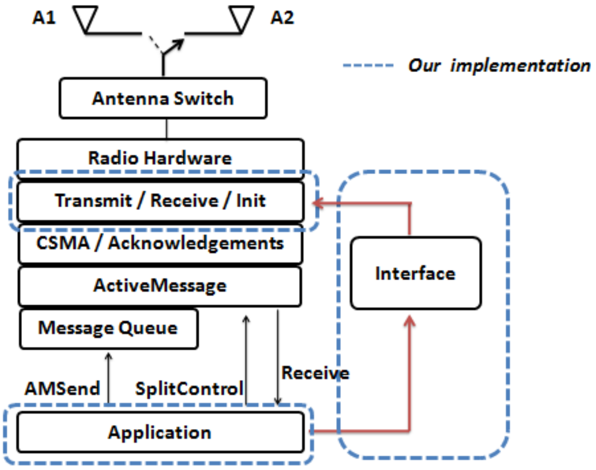


Figure 6.1: Software modifications implemented to the TinyOS low level device driver layer to enable dynamic antenna switching for the CU.

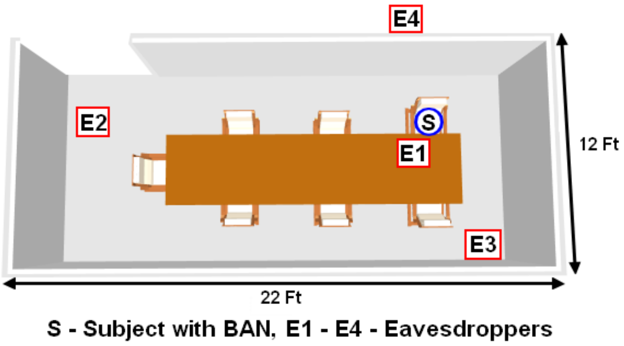


Figure 7.1: An indoor environment used for the experiments.

generation, only one antenna (either A1 or A2) will be active. Though iARC employs dual antennas, at any instant of time only one of the antennas will be active. Hence, the CU consumes same energy as a device with single antenna.

7 EVALUATION AND RESULTS

In this section, we discuss the experimentation details, results and security aspects of iARC.

We have validated the performance of our proposed key 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. For illustration purposes we provide the details of the experiments conducted in a conference room as shown in Fig. 7.1. 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

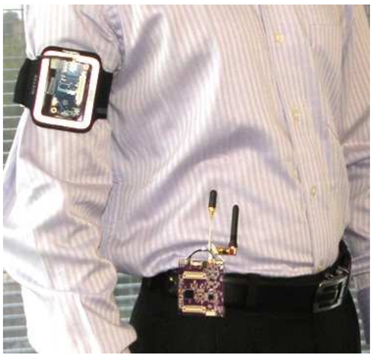


Figure 7.2: Subject wearing CU on the waist and Device D on the right arm.

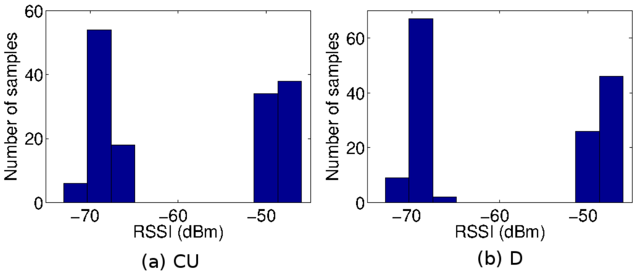


Figure 7.3: The histogram of RSSI samples collected by the CU and D on a single channel (channel 26) during channel sampling. The sub figures show that the samples of both CU and D will have same level l in the quantization process. Thus, the CU and D follow same frequency hopping pattern for subsequent channel sampling.

waist) and a body worn device D (on the right arm) as shown in Fig. 7.2 sitting on a chair without any body movement. We had placed multiple eavesdroppers at different positions inside as well as outside the conference room.

7.1 Secret key extraction

Let us examine the shared secret key extraction mechanism between CU and D by considering one of the data set from our experiments. Fig. 7.3 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. When both the devices derive secret key by using our proposed multi-level quantization scheme, they extract perfectly matching key when the size of the level selected by both the devices satisfies the requirement of the protocol.

Fig. 7.4 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 con-

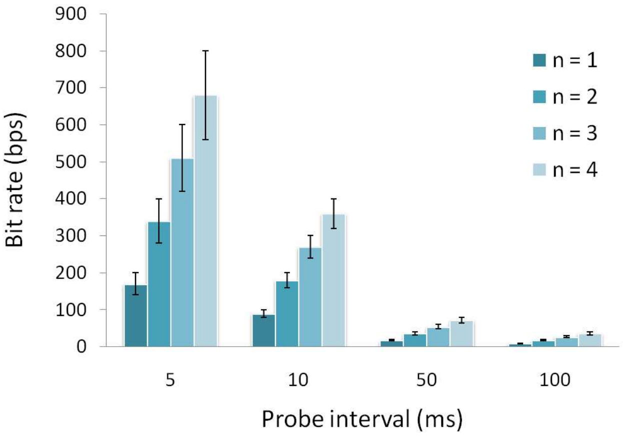


Figure 7.4: Secret key generation rate of iARC for different probe intervals.

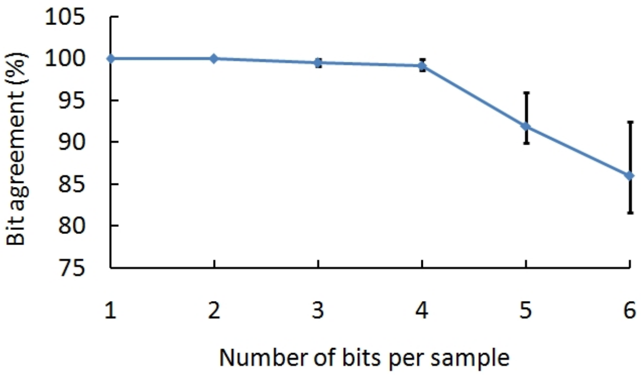
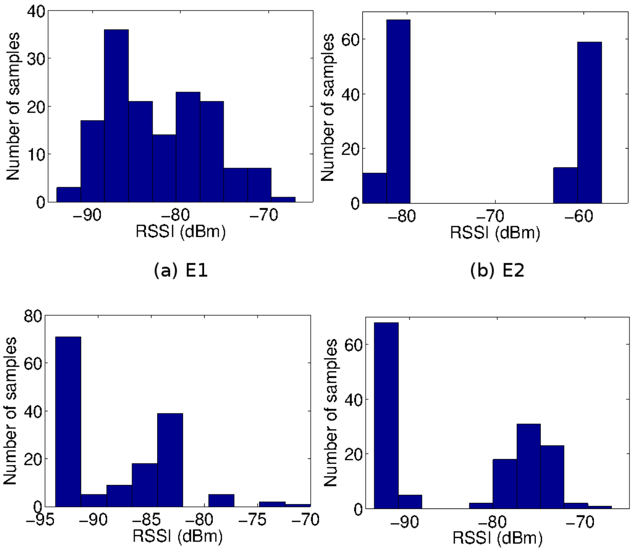


Figure 7.5: Bit agreement between the CU and D for different number of bits per sample assignment.

ducted for different inter packet intervals t, i.e., 250 ms, 100 ms, 50 ms, 10 ms, and 5 ms for the key generation. For each setting, we conducted 25 experiments with $N = 250$. We have validated the protocol performance for $n = 1$ to 4 bits per sample assignment scheme. Based on our observations, assigning 3 or 4 bits per sample is appropriate as it results in high entropy $\approx$ 0.92 to 0.99. 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 [24].

We have performed the NIST [5] entropy test to ensure that the keys generated by iARC have sufficient randomness. 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.

Fig. 7.5 shows the bit agreement for different number of bits per sample



(a) E1

(b) E2

(c) E3

(d) E4

Figure 7.6: The histogram of RSSI samples measured by different eavesdroppers on single channel (channel 26) during channel sampling. The sub figures show that the RSSI samples of eavesdroppers will have different levels than those of the CU and D as shown in Fig. 7.3. Hence the eavesdroppers fail to follow the dynamic frequency hopping pattern of CU/D.

assignments.

7.2 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 5.1, iARC employs random antenna switching based on the random string $r \in \{0,1\}^{128}$ generated by PRNG. Thus, before channel sampling only r is known 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.

7.3 Discussion

In this work, we have studied the effectiveness of combining frequency diversity and dual antennas to obtain path diversity and more channel variation (i.e., randomness to the channel samples), in order to improve the bit rate and the quality (entropy) of secret keys. From our experimental results we have noticed

Table 8.1: Comparison of mutual information between the CU and different nodes for various probe intervals.

Device		**Mutual information (bits)**		
		$t = 250$ ms	$t = 50$ ms	$t = 5$ ms
Sensor Device	D	0.9235	0.9393	0.9279
Passive eavesdropper with single antenna	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
Passive eavesdropper equipped with dual antennas	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

that the combined effect yields good randomness in the samples. However, in very few cases where the new channel after hopping (ch_{AH}) is not well separated from prior channel (ch_{BH}), which implies less channel spacing, then the samples collected on a single antenna in ch_{AH} and ch_{BH} might not have large/noticeable differences. This scenario does not help to get uncorrelated successive channel samples in case of single antenna systems [25]. On the contrary, as iARC employs dual antennas for channel sampling, even in such cases the observed entropy of final keys was > 0.9. In such cases, an additional step like XOR operation, can be employed to improve the entropy of final keys.

8 Security analysis

In this section we present the security analysis of iARC.

8.1 Estimation of shared randomness between the CU and D

The main factor influencing the performance of key generation is the shared randomness. This shared randomness can be quantified by computing the mutual information between the CU and D by using their channel estimates (i.e., RSSI). The amount of information between two observations X and Y is measured by the *mutual information I(X;Y)* [13] given by the following equation

$$I(X;Y) = H(X) + H(Y) - H(X,Y) \tag{8.1}$$

where *H(X)* and *H(Y)* are the entropy of X and Y respectively, and *H(X,Y)* is the joint entropy of X and Y.

A large mutual information implies more shared information between the two parties. Table 8.1 shows the average mutual information between the CU and all other nodes (D and eavesdroppers). From Table 8.1 it is clear that the mutual information between CU and D is ≈ 1 bit, which shows that CU and D have enough shared randomness to generate robust keys.

8.2 Passive adversary

The following sub sections describe the security against passive adversaries. For the evaluation purpose, we have considered the off-body adversaries only. However, iARC also provides security against on-body adversary who is situated away (> 6.25 cm) from the legitimate devices CU and D because of the unique spatio-temporal characteristics of wireless channel.

Passive eavesdropper with single antenna

In this section, we discuss the security aspect of our protocol in the presence of multiple adversaries with single antenna who try to intercept communication between the CU and D during secret key generation in static channel conditions. Iris motes were used as the eavesdroppers.

Consider Fig. 7.6 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 CU and D in Fig. 7.3. From Fig. 7.6 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 CU and D, she cannot follow the *dynamic frequency hopping scheme* used by CU/D, which is dependent on the level of RSSI samples 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.

Table 8.1 shows that the mutual information obtained by eavesdroppers is very minimal and is close to 0 in contrast to the high mutual information between CU and D. As the mutual information represents the upper bound on information content of the key that is leaked to an eavesdropper, it can be concluded that the eavesdropper cannot derive the same key as CU/D.

Passive eavesdropper equipped with multiple antennas

In this section we analyze the security of our design in the presence of passive eavesdroppers with multiple antenna. To evaluate this, we repeated the static channel experiments conducted in the conference room with the eavesdroppers E1 to E4 having two antennas. We replaced Iris motes used as eavesdroppers by Opal boards. We conducted these tests in two sets.

In the first set of experiments, eavesdroppers were equipped with two identical omni-directional antennas having same range and were programmed to operate in mode 2. In mode 2, the two antennas are separated by a distance $> \lambda/2$ (where $\lambda = 12.5$ cm is the wavelength of 2.4 GHz radio signal) and Eve receives the packets sent by CU on the antenna selected by internal diversity algorithm. However, due to multi-path effects, both the antennas of Eve observe different variation in the signals which further reduces Eve's correlation with CU/D, and dilutes the information about the secret key. From Table 8.1 it is clear that, even eavesdroppers with multiple antenna cannot get much useful information about the key generated by the CU and D.

In the second set of experiments, mode 2 operation was disabled on the Opal boards used as eavesdroppers. E1 to E4 were equipped with antennas similar to those of CU and followed the random antenna switching algorithm used by CU. In these experiments, we noticed that as the eavesdroppers had no information about the seed s used by CU for antenna switching, they used different seed and hence their correlation was further reduced by 40-60%.

Random guess attempt by adversary

In Section 8.2 and 8.2, we have discussed that the adversary cannot follow the dynamic frequency hopping pattern of CU/D and fails to capture subsequent packets. Additionally, it is also 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 = $1.469e^{-39}$ ($\approx 2^{-129}$). Similarly, if 16 levels are used for quantization (4 bits/sample), then the Eve's probability to reproduce the key is as low as $2.93e^{-39}$ ($\approx 2^{-128}$), which is negligible.

Collusion attack

One might question the performance of our scheme against an attack in which all the eavesdroppers combine their channel observation to guess the secret key. Table 8.1 gives mutual information obtained by different eavesdroppers E1 to E4 for various tests. Any attempts made by the eavesdroppers to process the received signal would further minimize their information about CU-D channel because of data processing inequality [13,20]. This shows that the eavesdroppers fail to get enough information about the key generated by the CU and D.

8.3 Active adversary

The following sub sections describe the security against active adversary.

Man-in-the-middle (MIM) attack

An active adversary may interfere during the process of key generation by CU and D, and can impersonate as one of the legitimate node. Adversary may send false packets with same packet index used by CU/D during probe packet exchange to extract the key used by legitimated devices. Such types of spoofing attacks can be prevented by employing the methods mentioned in prior work [20]. CU and D can use the 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 [26].

Jamming attack

An attacker with the capability to jam the wireless channel can cause denial-of-service (DOS) attack to disrupt the communication. In such situations CU and D employ frequency hopping technique to overcome the attack. Because of the jammed channel, CU and D cannot receive any packet or response from each other within the maximum time-out period (e.g., 1 minute) for key generation, then CU and D repeat the process after time-out. If similar problem is encountered, then both CU and D switch to another channel within 2.4 GHz. The CU and D can employ the method explained in Section 5.2 for channel hopping.

9 Related Work

Security mechanisms based on wireless channel characteristics have been proposed in previous work for WiFi systems. Authors in [20] have proposed secret key extraction methods using level crossing and quantization of the RSSI and CIR of the packets exchanged when one of the participating device is in motion. Researchers in [17] have studied the key extraction during dynamic channel cases in various indoor and outdoor environments and have employed reconciliation mechanism to correct the bit mismatch.

A fast and channel independent secret key generation mechanism specifically designed for OFDM systems is presented in iJam [15]. In iJam, the sender transmits a *salt* packet and its duplicate. Receiver jams one of the received packets and retrieves the secret bit from the other packet. As compared to iJam which requires $2 \times S_k$ number of probe exchanges for a key size S_k, e.g., 256 probe exchanges for generating 128 bit key, our system can generate multiple bits/sample and hence dramatically reduces the number of packets exchanged. For instance, iARC requires only 32 probe exchanges to generate 128 bit key when 4 bits/sample assignment scheme is employed. Additionally, WBAN devices are severely resource constrained and lack the capability to jam the signal. Hence, iJam is not suitable for WBANs.

An RSSI based key generation scheme for mobile WiFi devices with MIMO capability equipped with 3 antennas has been presented in MAKE [26]. MAKE is also dependent on the node/device mobility for key generation. Here, the packet transmitted by a sender is received on all the 3 spatially separated antennas at the receiver. Different transmitter-receiver antenna pair is selected for each sampling in a round robin fashion and spatial diversity is utilized for receiving different RSSI. In comparison with MAKE [26], our proposed system is not a MIMO, it is a chip based sensor platform in which transceiver allows only one antenna for the packet transmission and reception. Additionally, our design does not impose any constraints on the antenna separation, i.e., two antennas of CU can be placed together without any spatial separation which satisfies the design requirement of wearable devices with small form-factor[1].

[1] In multi-antenna wireless systems, in order to obtain uncorrelated channel characteristics, the antennas must be separated by a minimum distance $> \lambda / 2$, where λ = wavelength of the carrier signal. In case of 2.4 GHz, $\lambda = 12.5$ cm. On the other hand, in a practical

Recently, security mechanisms based on RSSI have been proposed for Wireless Body Area Networks. Authors in [16] have studied key generation in dynamic channel condition and achieved 2 bps bit rate in a simulation environment. Researchers in [9] have shown that the body-worn devices can generate secret keys during body motion of the person. The scheme has achieved a low bit rate of 0.24 bps and requires 15-35 minutes to generate a 128 bit key. An extended version in [10] takes 2 minutes to generate the same length key. Additionally, the work in [9,10] employ Savitzky-Golay filter and windowing to select a subset of RSSI samples for key generation and discard the remaining. The most recent RSSI based key generation scheme for dynamic channel cases presented in [24] has a bit rate of 8.03 bps.

One of the major drawback of existing secret key generation schemes based on RSSI in WBAN [9, 10, 24] is that key generation with good entropy requires dynamic channel conditions achieved by the body movement of subject wearing the devices. However, in case of a stable channel, the above schemes fail to derive keys with sufficient entropy. In addition, all the prior work [9, 10, 24] employ expensive techniques like windowing and filtering.

The most recent work closest to our work is SeAK [18], which 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 contrast, our proposed protocol iARC is for pair-wise 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 [25] 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 and quality of secret keys in static channel conditions.

Based on the literature survey, we believe that, our design is the first RSSI based secret key generation protocol which exploits dual antennas and freqnecy diversity effectively for inducing artificial channel randomness to derive the keys independent of node mobility.

10 Conclusion and future work

In this paper, we have demonstrated experimentally that the existing RSSI based schemes for secret key generation in WBAN are dependent on the channel randomness caused due to node mobility, have very low bit rate and low entropy, and hence are not suitable for the stable channel conditions present in many real world applications. We have presented a novel protocol – iARC for extracting

implementation based on our system, two surface mount chip antennas can be placed in a small 3.2×3.2 mm^2 area [7].

shared secret key in the absence of node mobility. iARC protocol employs dual antennas and frequency diversity (i.e., channel hopping) 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 [24, 25]. iARC substantially reduces the number of packets exchanged and the time required to derive a perfectly matching secret key in stable channel conditions. iARC generates 128 bit key 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.

Bibliography

[1] AT86RF231/ZU/ZF Datasheet. http://www.atmel.com/images/doc8111.pdf. Accessed: 27-October-2014.

[2] FitBit Flex. http://allthingsd.com/20130715/fitbit-flex-vs-jawbone-up-and-more-a-wearables-comparison/. Accessed: 27-October-2014.

[3] IEEE 802.15 WPAN Task Group 6 (TG6) Body Area Networks. http://www.ieee802.org/15/pub/TG6.html. Accessed: 27-October-2014.

[4] IRIS wireless sensor platform. http://www.memsic.com/wireless-sensor-networks/. Accessed: 27-October-2014.

[5] National Institue of Standards and Technology. http://csrc.nist.gov/groups/ST/toolkit/rng/index.html. Accessed: 27-October-2014.

[6] TinyOS. http://www.tinyos.net/. Accessed: 27-October-2014.

[7] Ultra small chip antennas. http://www.taoglas.com/. Accessed: 27-October-2014.

[8] Wearable device revenues to grow to USD 6B in 2018. http://mobihealthnews.com/25933/wearable-device-revenues-to-grow-to-6b-in-2018/. Accessed: 27-October-2014.

[9] 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.

[10] S. T. Ali, V. Sivaraman, D. Ostry, and S. Jha. Securing Data Provenance in Body Area Networks Using Lightweight Wireless Link Fingerprints. In *Proc. International Workshop on Trustworthy Embedded Devices (TrustED)*, 2013.

[11] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener. Robust Key Generation from Signal Envelopes in Wireless Networks. In *Proc. ACM Conference on Computer and Communications Security (CCS)*, 2007.

[12] G. Brassard and L. Salvail. Secret-key Reconciliation by Public Discussion. In *EUROCRYPT*, 1993.

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

[14] J. Croft, N. Patwari, and S. K. Kasera. Robust Uncorrelated Bit Extraction Methodologies for Wireless Sensors. In *Proc. ACM/IEEE Conference on Information Processing in Sensor Networks (IPSN)*, 2010.

[15] S. Gollakota and D. Katabi. Physical Layer Wireless Security Made Fast and Channel Independent. In *IEEE INFOCOM*, 2011.

[16] 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 *Proc. Conference on Body Area Networks (BodyNets)*, 2009.

[17] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy. On the Effectiveness of Secret Key Extraction from Wireless Signal Strength in Real Environments. In *MobiCom*, 2009.

[18] 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.

[19] 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.

[20] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik. Radiotelepathy: Extracting a Secret Key from an Unauthenticated Wireless Channel. In *MobiCom*, 2008.

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

[22] M. Rostami, A. Juels, and F. Koushanfar. Heart-to-Heart (H2H): Authentication for Implanted Medical Devices. In *Proc. ACM Conference on Computer and Communications Security (CCS)*, 2013.

[23] 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.

[24] 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.

[25] M. Wilhelm, I. Martinovic, and J. B. Schmitt. Secret Keys from Entangled Sensor Motes: Implementation and Analysis. In *Proc. ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2010.

[26] 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.