ABSTRACT
In this paper, we undertake experiments to assess the feasibility of generating common secret keys between two body-worn devices using the near-body channel. Deriving secret keys using the wireless channel is a practical and lightweight alternative to public-key key-agreement approaches. Our results indicate that key generation is good for dynamic scenarios where communicating devices are placed in non-line-of-sight positions on the body. Furthermore, we enhance existing key generation mechanisms by proposing a filtering method to reduce bit mismatch.

Categories and Subject Descriptors
C.2.0 [General]: Security and protection

General Terms
Security, Experimentation, Measurement, Performance

Keywords
Secret Key Agreement, Body Area Networks, RSSI

1. INTRODUCTION
In the recent years there has been increasing application of body area networks for healthcare. In such applications, body-worn wireless medical sensor devices measure the patient’s vital signs such as heart rate, temperature, blood glucose level, etc. Since these devices collect and communicate medical data, there are stringent ethical and legal implications, and security of this data is a critical concern. However, due to severely constrained computational and energy resources, these miniature sensor devices are not suited to run resource-intensive security solutions such as those based on public key cryptography. Instead, some researchers are working on new lightweight alternatives for small devices.

The problem we examine in this paper is that of key generation. For secure communication, two parties need to be in possession of a shared secret. The Diffie-Hellman key exchange is typically used for this purpose, but recent results have shown that it is resource and time consuming to perform on small devices. A promising alternative approach is to use the unique properties of the wireless channel between two communicating devices to generate secret keys [1].

Wireless communication is fundamentally insecure but the channel between two communicating parties is unique to them [2]. If one party, Alice, transmits to Bob, the signal traverses multiple paths, experiencing different degrees of attenuation and phase shift, and Bob receives the summation of these multipath signals. If Bob responds in the exact same conditions, Alice’s impulse response would be highly correlated to Bob’s. This correlated information can be used to generate a secret key. A third party, Eve, located at least half a wavelength away from either Alice or Bob, and listening in on all transmissions, is limited to measuring a different channel, and for a dynamic multipath environment, the impulse response would be very different and near-impossible to guess for the Alice-and-Bob channel.

In this work, we explore this approach for on-body networks and introduce a modification to improve performance. This paper makes the following contributions: (1) We assess the suitability of using the near-body wireless channel for key generation for various configurations of device placement on the body and different modes of activity, and (2) we suggest a filtering modification to reduce bit mismatch between two devices and validate results with simulation and experiment.

2. BACKGROUND AND PRIOR WORK
Secret key generation schemes in the literature typically comprise four stages: in the sampling phase, two communicating parties continuously exchange probe packets to estimate reciprocal channel state. These channel estimations are then converted to key bits in the quantization step. However, mostly due to small-scale noise effects (that are random and uncorrelated for both parties) some generated bits are liable to disagree between the two parties, and information reconciliation is used to correct the mismatch by exchange of feedback. Additionally some of the bits may be correlated and a transform operation, i.e. privacy amplification is used to minimize this advantage for an eavesdropper who may acquire knowledge of some key bits.

In [3], the authors describe a method to extract key bits from a statistical Gaussian channel. They validate this key generation mechanism using the 802.11 platform, and gener-
3. FEASIBILITY OF KEY GENERATION IN ON-BODY NETWORK

3.1 Experimental Setup

We performed experiments in an indoor office space consisting of multiple cubicles, as shown in Fig.1(b). We use MicaZ motes running TinyOs, operating in the 2.4 GHz band. Two communicating devices, Alice and Bob, are mounted on the body (1(a)), and transmit probe packets at 0 dBm power at a rate of 50 packets/s, and sample the channel continuously. Two passive eavesdroppers are present: Eve1 is also mounted on the subject’s body, and Eve2 is off-body.

We collect RSS traces for four scenarios listed in Table 1, categorized by subject’s activity (Walking or Resting) and placement of devices on body. For walking scenarios the subject walks randomly around the office at about 1 m/s. Readings are collected over a span of 3 ~ 5 minutes.

Table 1: Experimental Setup

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Alice’s Location</th>
<th>Bob’s Location</th>
<th>Eve1’s Location</th>
<th>Eve2’s Location</th>
<th>User’s Motion</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>L Waist</td>
<td>R Arm</td>
<td>L Arm</td>
<td>Desk</td>
<td>Resting</td>
</tr>
<tr>
<td>b</td>
<td>L Waist</td>
<td>R Arm</td>
<td>L Arm</td>
<td>Desk</td>
<td>Walking</td>
</tr>
<tr>
<td>c</td>
<td>L Waist</td>
<td>R Leg</td>
<td>L Arm</td>
<td>Desk</td>
<td>Walking</td>
</tr>
<tr>
<td>d</td>
<td>L Waist</td>
<td>L Chest</td>
<td>L Arm</td>
<td>Desk</td>
<td>Walking</td>
</tr>
</tbody>
</table>

3.2 Experimental results

Fig. 2 shows RSS traces for the four scenarios. For clarity, we only show readings over a period of 10 seconds and eavesdroppers’ measurements are only plotted for Scenario (b) in Table 1. As can be seen, the channel state variation is very dependent on mode of activity and device placement. We make the following observations:

- During resting (Scenario (a)), the channel state has minimal variation, and the correlated information that can be extracted for bit generation will be very low.
- For Scenarios (b) and (c), the transmission between Alice and Bob is non-light-of-sight (NLOS) due to antenna placement and because the subject is moving, there is significant channel variation which is excellent for key generation.
- For Scenario (d), the antennas for Alice and Bob have line of sight (LOS) due to placement on the chest and waist, and their distance is roughly constant. The channel variation is much smaller compared to Scenario (b) and (c). We suggest that this is because the line of sight ensures that the RSS is dominated by the path loss component which is relatively steady in this case, whereas for NLOS scenarios (b) and (c), multipath propagation dominates the channel variation.
- Eavesdroppers, due to their placement, measure a different channel and their results are uncorrelated to those of Alice and Bob (Fig. 2(e)).

We employ the Pearson correlation coefficient to estimate the correlation for different parties. A value of 1 indicates perfect correlation, 0 denotes no correlation and -1 implies anticorrelation. For dynamic scenarios, the RSS correlation between Alice and Bob for LOS (Scenario (d)) is 0.8513 and for NLOS (Scenarios (b) and (c)), it is higher at 0.9825 and 0.9831. The higher the correlation, the more likely the resulting keys are to agree between Alice and Bob.

Existing research [3] indicates that small-scale effects negatively affect the correlation. These are due to uncorrelated white noise at both endpoints, and asynchronous sampling. Most radios have half-duplex modes of communication which do not permit simultaneous sampling of the channel by both endpoints. Instead both devices sample the channel in quick succession and in this time interval, the channel is likely to vary by a small amount. To minimize these small-scale effects for better bit agreement, we propose filtering using an averaging technique.

4. FILTERING TO IMPROVE KEY MATCH

4.1 Filtering: idea and analysis

To convert RSS measurements to secret key bits, we adapt a quantizer originally proposed by Mathur et al.[3] and modified by Jana et al.[2]. In Mathur’s quantization scheme, two
thresholds $q^+$ and $q^-$ are determined over a block of readings of size $f$ such that:

$$q^+ = \mu + \alpha \cdot \sigma; \quad q^- = \mu - \alpha \cdot \sigma$$  \hspace{1cm} (1)

where $\mu$ and $\sigma$ denote mean and standard deviation of the sampling values and $\alpha$ is a configurable parameter such that $\alpha \geq 0$. If $m$ successive values lying above $q^+$ or below $q^-$ are encountered, a single bit 1 or 0 are encoded, respectively. Samples lying within the thresholds are dropped.

In our modified quantizer (depicted in Fig. 3), we still calculate the $q$ thresholds using Eq.(1), but we perform averaging of the sample values over a window size $w$ to minimize the small-scale uncorrelated effects for both parties. Instead of waiting for $m$ successive values, if any resultng value is greater than or less than the $q^+$ or $q^-$ respectively, we encode to a 1 or 0. In this case, block size $f = n \cdot w$.

We provide a theoretical justification of our approach: assuming Gaussian estimation of channel state and independent successive sampling values, the secret bit mismatch ($p_{bm}$) and secret bit rate ($R_{sb}$) of the quantization result are expressed in Eqs.(2) and (3).

$$P(A = 1, B = 0) = P(A = 1, B = 0) + P(A = 1, B = 1)$$

$$= \frac{1}{2\pi \sigma_x \sigma_y \sqrt{1-\rho^2}} e^{-\frac{1}{2(1-\rho^2)}}$$

$$z = \frac{(x_i - \mu_x)^2}{\sigma_x^2} + \frac{(y_i - \mu_y)^2}{\sigma_y^2} - 2 \rho (x_i - \mu_x)(y_i - \mu_y)$$

$$P_{bm} = \frac{1}{w} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(x_i, y_i) dx_i dy_i$$

$$\int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(x_i, y_i) dx_i dy_i + \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(x_i, y_i) dx_i dy_i$$

$$R_{sb} = \frac{f}{w} \cdot \left[ P(A = 0, B = 0) + P(A = 1, B = 1) \right]$$

$$= \frac{1}{w} \cdot 2 \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(x_i, y_i) dx_i dy_i$$

$$f(x, y) = \frac{1}{2\pi \sigma_x \sigma_y \sqrt{1-\rho^2}} e^{-\frac{1}{2(1-\rho^2)}}$$

$$R_{sb} = \frac{f}{w} \cdot \left[ P(A = 0, B = 0) + P(A = 1, B = 1) \right]$$

Figure 2: 10 seconds RSS measurements

Figure 3: A sample of our quantization with $w = 2$ and $n = 5$.
Secret Bit Rate (bits/second)

Bit mismatch (%)

Figure 4: Analytical and simulation results, mismatch of all three, thereby validating our approach.

(a) Bit mismatch against window size for different correlation values

(b) Secret bit rate against window size for different correlation values

Figure 4: Analytical and simulation results, $\alpha = 0.2$ and $f_s = 50$Hz

- Secret key bits are generated at a high rate with a low secret bit mismatch for NLOS links. We noted earlier that there was high correlation between Alice and Bob for NLOS links.

- Key bit mismatch is higher for the LOS link. We predicted this when we computed correlation for the different links in Section 3.2. In this case, increasing window size incrementally will reduce bit mismatch.

We use the last instance, the LOS link to compare the performance of our modified quantizer with that of Mathur and Jana, since that shows the highest bit mismatch. Results are depicted in Table 3. The individual parameters for the different quantizers are set as shown such that they yield equivalent secret bit rate ($3.75 \sim 3.85$ bits/s). We observe that our quantizer performs best by giving the lowest bit mismatch of all three, thereby validating our approach.

Table 2: Experimental Results for Moving Scenarios: $w = 2, n = 5, \alpha = 0.5$

<table>
<thead>
<tr>
<th>Valid Mote Location</th>
<th>Secret Bit Rate(bits/s)</th>
<th>Secret Bit Mismatch</th>
</tr>
</thead>
<tbody>
<tr>
<td>L Waist R Arm(NLOS)</td>
<td>13.10</td>
<td>0.13%</td>
</tr>
<tr>
<td>L Waist R Leg(NLOS)</td>
<td>13.90</td>
<td>0.0%</td>
</tr>
<tr>
<td>L Waist L Chest(LOS)</td>
<td>8.42</td>
<td>7.37%</td>
</tr>
</tbody>
</table>

Table 3: Experimental Result: LWaist-LChest

<table>
<thead>
<tr>
<th>Quantization</th>
<th>Secret Bit Rate(bits/s)</th>
<th>Valid Mote Mismatch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mathur</td>
<td>4.81</td>
<td>2.73%</td>
</tr>
<tr>
<td>Jana</td>
<td>3.76</td>
<td>5.13%</td>
</tr>
<tr>
<td>Ours</td>
<td>3.84</td>
<td>1.46%</td>
</tr>
</tbody>
</table>

5. CONCLUSION

In this paper we have demonstrated the feasibility of extracting secret keys from the wireless channel in on-body networks. Our experimental results confirm that human motion causes high channel variation to generate secret keys at a fast rate with high agreement, especially for NLOS links. Eavesdroppers are unable to replicate the secret key even if they are placed within a moderate distance of the communicating parties. Furthermore, we enhance existing quantization techniques with a filtering function to minimize random noise effects and improve secret key agreement. For future work, we intend to optimize quantizer design and address the issue of authentication of bodyworn devices.

6. REFERENCES