Secret Key Extraction in MIMO-like Sensor Networks Using Wireless Signal Strength

Sriram Nandha Premnath

Academic Advisors: Sneha K. Kasera, Neal Patwari

nandha@cs.utah.edu, kasera@cs.utah.edu, npatwari@ece.utah.edu
University of Utah

1 Problem and Introduction

Secret key establishment is a fundamental requirement for private communication between two entities. There is a growing interest in using spatial and temporal variations in wireless link characteristics for extracting secret keys[1,6]. In our recent work [5], we investigated the effectiveness of secret key generation using wireless received signal strength in real environments. However, our work used only single antenna, single input and single output (SISO) systems. Furthermore, our work used IEEE 802.11g wireless cards. Now, received signal strength (RSS) can also be measured using other wireless devices including sensor nodes. In this poster, in order to understand how our research [5] applies to sensor nodes, and in a multi-antenna, multiple input multiple output (MIMO) system, we first create a simple, yet flexible, MIMO-like testbed with the help of multiple sensor nodes. Next, we use this testbed to measure RSS, and extract secret keys from RSS variations. We find that our MIMO-like sensor environment has a much higher percentage of bit mismatches between the two parties (Alice and Bob), interested in establishing a secret key, in comparison to our earlier 802.11 SISO study. To solve this problem, we introduce a *distillation* stage [1] in our key extraction methodology comprising the quantization, information reconciliation, and privacy amplification stages. The distillation stage, introduced between the quantization and the information reconciliation stages, iteratively improves the output from the quantizer by eliminating measurements that are likely to cause mismatching bits at Alice and Bob. This stage ensures that the percentage of mismatching bits is low enough to be handled by information reconciliation without compromising security.

In summary, (i) we show how MIMO-like systems can benefit the key extraction process by improving the secret bit rate. Our results show that the rate at which the secret key bits can be generated increases linearly with the number of antennas used, (ii) we suggest adding a distillation stage to key extraction process that enables handling high secret bit mismatch rates. In fact, without the distillation stage, the information reconciliation stage by itself is unable to reconcile the bit mismatch.

2 Motivation

Public key cryptographic systems are computationally very demanding, which makes such systems unsuitable for resource constrained, battery-powered sensor networks. Therefore, secret key extraction approach that is based on inexpensive measurements of received signal strengths serves as a much better alternative for sensor networks.

Space diversity, or the use of multiple antennas (MIMO) allows secret key extraction process to measure several channels simultaneously, and which therefore is expected to contribute a significant increase in the rate at which secret key bits can be extracted.

3 Background and Related Work

3.1 Wireless Channel Properties

Radio waves traversing a medium undergo a number of changes that are caused by reflection, refraction, scattering, diffraction, mobility etc. There are three key properties of the wireless channel that enable a pair of wireless devices to establish a secret key between them.

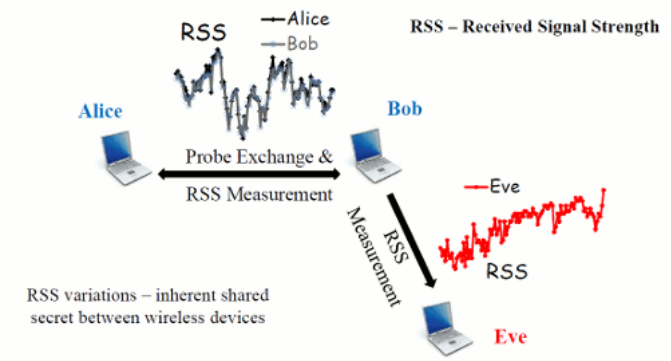

Figure 1: Properties of wireless channel - Reciprocity, Temporal & Spatial variations

- **Channel Reciprocity:** The multipath properties of the radio channel (gains, phase shifts, and delays) are *identical* on both directions of a wireless link, at any time instant, because signals from Alice to Bob & Bob to Alice, traverse along the same set of multipaths. Therefore, there is an inherent secret shared between any pair of wireless devices.
- **Temporal Variations:** Over time, the multipath channel undergoes various changes due to the movement of the wireless devices themselves, or the intermediate objects in the environment.

- **Spatial Variations:** The properties of the radio channel are unique to the locations of the pair of two communicating wireless devices. An eavesdropper at a third location more than a few wavelengths (on the order of a few centimeters for signals in 2.4 GHz band) away from either of these communicating devices will measure a different, uncorrelated radio channel [3].

Figure 1 depicts these three properties of the wireless channel.

3.2 Secret Bit Extraction Process

In our earlier work [5], we used a three stage process, comprising quantization, information reconciliation [2] and privacy amplification [4], for transforming a set of RSS measurements into secret key bits. In addition to the use of a new stage called *distillation* (described later) in this work, we also use these three existing stages. The purpose of each stage is described below.

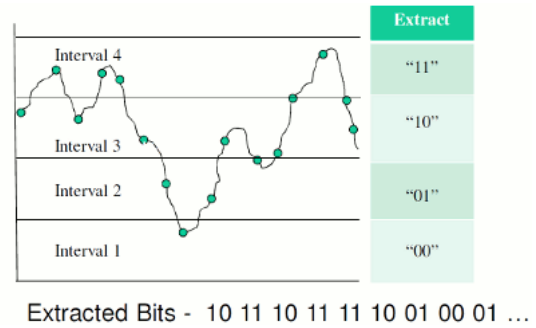

Figure 2: Quantization - Converting RSS Measurements into Bits

- **Quantization:** Given a set of RSS measurements, the quantization stage first divides the range of measurements into M equal sized intervals. Then depending on the interval in which a given measurement falls into, $\log_2 M$ bits are extracted from that measurement. Quantization with M=4 intervals is depicted in Figure 2.
- **Information Reconciliation:** Differences may arise in between the bit streams of Alice and Bob arise due to noise/interference, wireless hardware limitations, or the half-duplex nature of typical wireless devices. To handle the potential differences, in the information reconciliation stage, Alice and Bob exchange parity information of small blocks of bits. Then, all the blocks with mismatching parities are located. Proceeding in a binary search fashion for each such mismatching block, it is checked if a few bits can be changed to make the block match parity. These steps are repeated a number of times with different permutations of the bit streams to ensure a high probability of success.
- **Privacy Amplification:** There could be short-term correlation between subsequent bits when the channel probing rate is greater than the inverse of the coherence time of the wireless channel (which is very difficult to estimate). Further, information reconciliation reveals a certain fraction of bits to reconcile the differences in the bitstreams of Alice and Bob. Privacy amplification addresses both the bit correlation and bit leakage problems by applying 2-universal hash functions on the reconciled bits. This step reduces the length of the output bit stream but at the same time it also increases the per bit entropy of the extracted secret key bit stream.

3.3 Comparison to existing work

Our earlier work [5] is on key extraction among pair of laptops equipped with 802.11 wireless card having single antenna. 802.11 uses wide-band channel (20 MHz). In contrast, this work is on the evaluation of key extraction using sensor nodes that are based on the 802.15.4 standard. In comparison to 802.11, the 2.4 GHz band of 802.15.4 uses much narrow-band channel (2 MHz). Narrow band channels present unique challenges that we address in this work using a distillation stage in the key extraction process.

Wallace et al. [7] present a theoretical and simulation study on the use of multiple antennas available at each node for key extraction. In comparison, our work is based on a real-work experiments that we conduct on a flexible testbed using TelosB sensors. Typically, sensors are equipped with only one antenna; in our work, we achieve multiple antenna capability using multiple sensor nodes.

4 Uniqueness of our secret key extraction approach

All the existing approaches use the wireless channel variations between only one pair of nodes. However, we use the channel variations among multiple sensor nodes to efficiently extract secret keys. We show that the rate at which the secret bits are extracted can be improved significantly by increasing the number of nodes.

Secret key extraction using multiple nodes in a sensor network setting presents the following two unique challenges that contribute to prohibitively high mismatch rates -

1. large time difference between unidirectional measurement pairs
2. frequent non-reciprocal nulls in narrow 802.15.4 channels

We address these unique challenges by augmenting the existing 3-stage secret key extraction process with a distillation stage, which we describe in Section 4.4.

4.1 SISO Vs MIMO Measurements

Using one antenna at each endpoint, only one channel is realized in a single input single output (SISO) system.

However, with N antennas at each endpoint, N^2 channels are realized in a multiple input multiple output (MIMO) system.

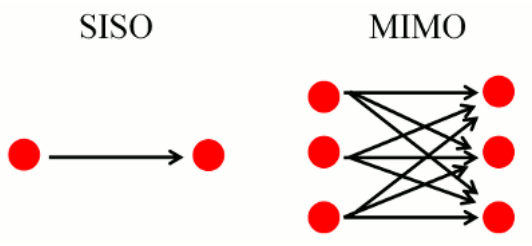

Figure 3: SISO vs MIMO measurements

For each probe packet transmission from Alice, Bob can record N measurements simultaneously. So, for a total of N probe transmissions from Alice, with one probe from each antenna, Bob can collectively record N^2 measurements. This is shown in Figure 3 for N=3 antennas. Since the number of channel measurements increases with the number of nodes, we expect a significant increase in the secret bit rates when using multiple nodes.

4.2 Experimental Setup

In our work, we use Crossbow TelosB wireless sensors for our experiments. TelosB mote is a low power wireless sensor module equipped with an IEEE 802.15.4-compliant RF transceiver (the TI CC2420), built-in antenna and a micro-controller. The motes are programmed to exchange probe packets and collect RSS measurements, as described by Wilson et al. [8][2]. This sensor network platform allows us to readily explore the impact of using multiple antennas on secret key extraction.

For our implementation, we could have possibly used devices equipped with 802.11n wireless cards based on the MIMO technology. However, these off-the-shelf wireless cards typically have 2-3 pre-installed antennas. In comparison, our MIMO-like configuration allows us to experiment with 1-5 antennas using the same setup in a flexible manner. Additionally, our platform also allows us to examine RSS-based key extraction in sensor networks.

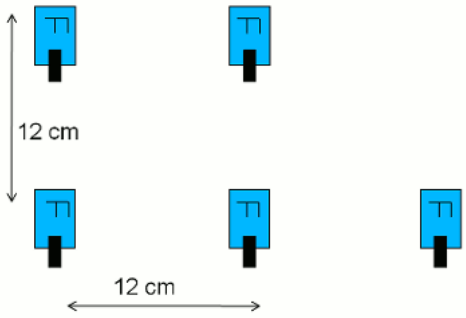

Figure 4: Experimental Setup of TelosB sensors

We use 10 sensors operating on batteries, divided into two groups of 5 each representing Alice and Bob. Another sensor connected to a laptop acts as a base station that collects data from all the other 10 battery powered sensors. Nodes representing Alice are numbered 0-4 and those representing Bob are numbered 5-9. With this setup, when one sensor, for example, node 0 which is part of Alice, transmits a probe packet, all the 5 nodes numbered 5-9, representing Bob can record RSS values simultaneously. Node numbered i+1, transmits a probe packet immediately after it hears a probe packet sent from a node numbered i. After node 9's transmission, node 0 pauses for 50 ms before starting the cycle again.

In each group of 5 sensors representing Alice/Bob, the sensors are arranged in two parallel rows as shown in Figure 4, with each sensor separated from another by a distance of no less than 12 cm, which is greater than the de-correlation distance for signals transmitted in the 2.4 GHz band. The same setup allows us to study various MIMO-like configurations NXN, for all N = 1 to 5. We conduct our experiment in a student lab. One group of motes representing Alice is kept stationary in one corner of the lab while the other group of motes is mobile, which is carried around in the lab at normal walking speed. During the course of the experiment, the distance between Alice and Bob is maintained between 5-25 ft. In this work, we use the multiple bit extraction method as described in [5], extracting 2 bits from each RSS measurement.

4.3 Prohibitively High Bit Mismatch Rates

We define the bit mismatch rate as the percentage of bits that do not match between Alice and Bob. Plotting the bit mismatch rate against various N×N configurations that we experiment with, we find that the bit mismatch rates are significantly higher in comparison to our experiments from our earlier work [5] that uses 802.11 single antenna systems operating on a wide-band channel.

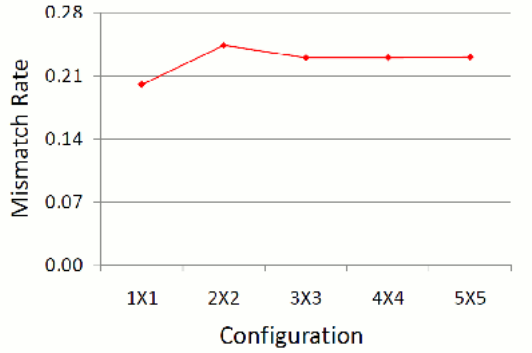

Figure 5: Bit Mismatch Rate vs Configuration

Figure 5 shows the very high bit mismatch rates in a plot of bit mismatch rate vs N×N configuration. At a mismatch rate of about 22%, the information reconciliation protocol essentially reveals all the bits. So, the collected set of measurements are not useful in establishing a secret key at all.

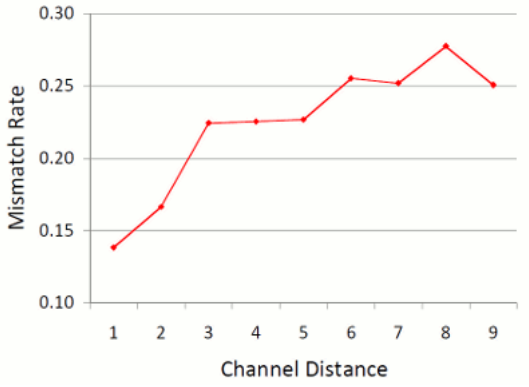

Figure 6: Bit Mismatch Rate vs Channel Distance

We identify the following reasons for such high mismatch rates -

1. when multiple nodes take turn in exchanging probe packets, it increases the average time-gap between any pair of measurements taken in each direction of a channel. Further, with increasing time-gap, it is more likely that the probing rate falls below the rate of change of the wireless channel. So when Alice and Bob measure the channel at increasing time gaps when using multiple antennas, it should increase the bit mismatch rate. This is also verified from a plot of bit mismatch rate vs channel distance (Figure 6), where channel distance is the absolute difference between the node-ids of the transmitting and receiving antennas. Figure 6 clearly shows the general increase in mismatch rate with channel distance. Time gap between each unidirectional measurement pairs is proportional to the channel distance. So, mismatch rate increases with channel distance / multiple antennas.
2. the channels in 802.15.4 are much narrower (2 MHz). A non-reciprocal deep fade occurring (perhaps due to strong interference affecting only one node), say for example at Alice, will significantly bring down the RSS computed at Alice, while not affecting much at Bob. Therefore, it is more likely for Alice and Bob to have significant differences in their recorded RSS variations, and consequently higher bit mismatch rate.

Notice the following important comparison w.r.t 802.11. The calculated RSS in 802.11 represents an average taken across 52 subcarriers occupying a 20 MHz channel. A non-reciprocal deep fade occurring on some specific subcarrier is not very likely to significantly affect the average computed across such a wider-band. Therefore, in 802.11 the RSS variations at Alice and Bob will be more-or-less the same resulting in lower mismatches, in comparison to 802.15.4.

4.4 Distillation – High Mismatch Handler

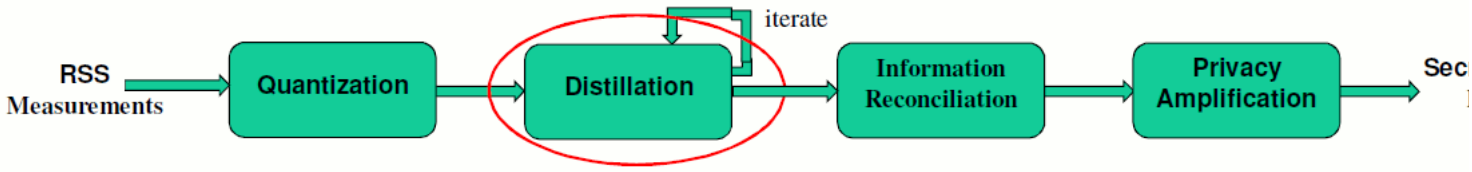

Figure 7: Secret Bit Extraction Process augmented with Distillation Stage

To address the problem of very high bit mismatch rates, we augment the secret key extraction process with the distillation stage. Distillation ensures that the percentage of mismatching bits is low enough for information reconciliation to correct the differences without revealing all the extracted bits. Figure 7 shows the distillation stage in relation to the other stages of the key extraction process.

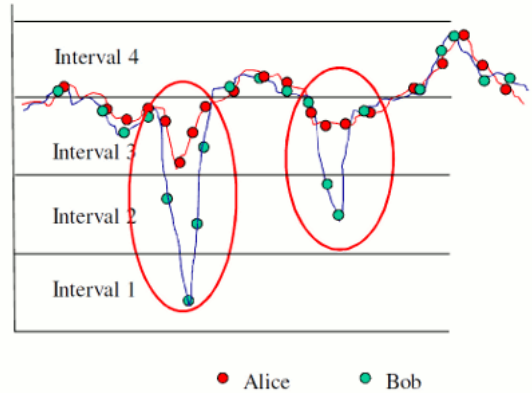

Figure 8: Non reciprocal abrupt variations

Plotting the RSS measurements of Alice and Bob in high bit mismatch scenarios, we find that a large fraction of consecutive measurements exhibit abrupt transitions from one quantization level to another. Figure 8 shows two sample non-reciprocal abrupt transitions occurring at Bob but not at Alice. Such abrupt transitions across quantization levels occur due to large channel distance, or deep fades, and result in high bit mismatch between Alice and Bob, as we discuss in Section 4.3. The distillation stage seeks to iteratively eliminate the set of measurements causing such abrupt transitions. This iterative process, along with an example is shown below.

Iterative Distillation

iteration 1: remove measurements following abrupt transitions

iteration 2-n: remove measurements following those that are removed in iteration i-1

	sequence of quantization intervals
distiller input:	aaaaaddaaaabbbbbaaaa ...
iteration 1 output:	_aaaa_d_aaa_bbbb_aaa ...
iteration 2 output:	__aaa____aa__bbb__aa ...

a-d represent quantization intervals 1-4

5 Results

In this section, we show the improvement in - (i) bit mismatch rate with each iteration of distillation, and (ii) secret bit rate with increase in the number of nodes.

5.1 Effectiveness of Distillation

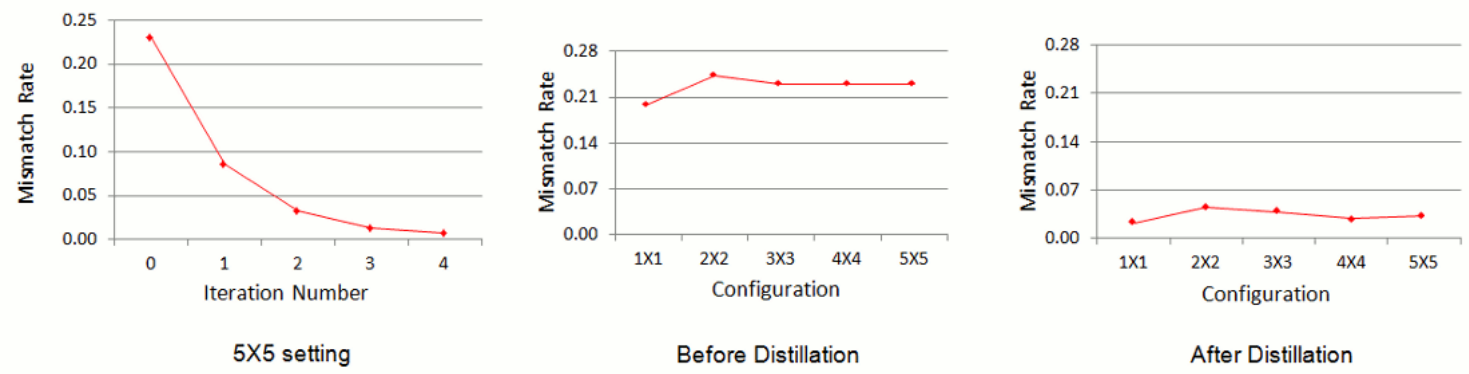

Figure 9: Effectiveness of distillation in drastically reducing bit mismatch rate

The first plot in Figure 9 shows that the bit mismatch rate improves with each iteration for the 5X5 configuration. Without distillation, the mismatch rate is about 23%. But after 2 iterations of distillation, the mismatch rate falls to less than 5%. Recall that for a mismatch rate of about 22%, information reconciliation leaks out all the information, and therefore no useful secret bits are extracted. However, with distillation the bit mismatch rate is brought down to sufficiently small value that can be handled by the information reconciliation stage, and so useful secret bits are extracted in the process. The second and third plots in Figure 9 show that distillation is very effective for measurements collected in all N×N configurations.

Number of distiller iterations: While distillation improves the bit mismatch rate with each iteration, the number of iterations needs to be chosen carefully. A small number of iterations might be enough for information reconciliation to work; but if the mismatch is still high enough, the number of useful secret bits extracted will be very less. Therefore, to achieve best performance, the number of distiller iterations should be selected depending on the current expected mismatch rate of the channel. This can be determined based on the history of mismatch rate of the channel. For the 5×5 setting, two iterations of distillation bring down the mismatch rate to less than 5%. For a different setting with a total of 4 nodes, i.e., a 2×2 configuration, just one iteration was enough to bring down the mismatch rate to less than 5% because, to begin with, this setting had less than 14% mismatch rate before distillation.

5.2 Secret Bit Rate Gain with Multiple Antennas

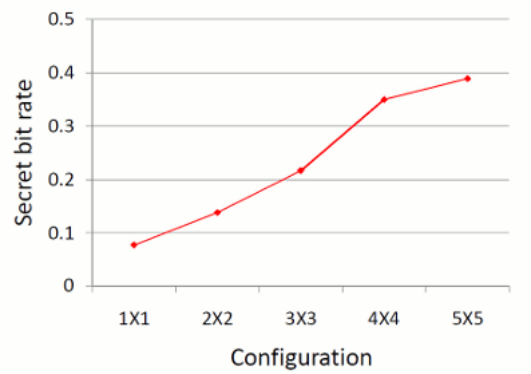

Figure 10: Linear gain in secret bit rate w.r.t the number of nodes

In this work, we define the secret bit rate as the average number of secret bits extracted per probe transmission. To show the improvement in secret bit rate with increasing number of nodes, we plot the secret bit rate vs various N×N configurations. As seen in Figure 10, the secret bit rate increases linearly with the number of nodes. Therefore, we can expect to extract secret keys at an efficient rate by increasing the number of nodes that are used in the secret key extraction process.

High entropy bits: To measure the randomness of the extracted bit streams, we calculate the per-bit entropy using the NIST's approximate entropy test. For the bit streams that we extract from all the N×N configurations, the calculated per bit entropy values for the extracted secret bit streams are close to 1, the ideal value.

6 Conclusions, Contributions, and Future Work

We created a simple MIMO-like sensor testbed to explore the possibility of using MIMO systems for improving the secret key bits generation rate using RSS variations as measured between two devices of our testbed. We obtained very promising and interesting initial results. Our contributions include the following.

Essentially, our experiments showed that the rate at which the secret key bits can be generated increases linearly with the number of antennas used. We showed that the prohibitively high bit mismatch in the MIMO-like sensor scenarios can be handled by the introduction of distillation stage in the key extraction process. Distillation helps the wireless devices in establishing a secret key where information reconciliation by itself cannot. We showed that just two iterations of distillation can progressively bring down a prohibitively high bit mismatch rate of about 23% to less than 5%.

Future work: We will extend our experimental study to different environments and other network configurations in the near future. MIMO receivers can gather phase information, apart from the amplitude of the received signal. In future, we will study how this additional information can be used in the key extraction process.

References

[1] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener. Robust key generation from signal envelopes in wireless networks. In *CCS '07: Proceedings of the 14th ACM conference on Computer and communications security*, pages 401-410, Nov. 2007.

[2] G. Brassard and L. Salvail. Secret key reconciliation by public discussion. *Lecture Notes in Computer Science*, 765:410-??, 1994.

[3] G. D. Durgin. *Space-Time Wireless Channels*. Prentice Hall PTR, 2002.

[4] R. Impagliazzo, L. A. Levin, and M. Luby. Pseudo-random generation from one-way functions. In *STOC*, pages 12-24, 1989.

[5] 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 *ACM MOBICOM Conference*, Sept. 2009.

[6] S. Mathur, W. Trappe, N. B. Mandayam, C. Ye, and A. Reznik. Radio-telepathy: extracting a secret key from an unauthenticated wireless channel. In *MOBICOM*, pages 128-139, 2008.

[7] J. W. Wallace, C. Chen, and M. A. Jensen. Key generation exploiting mimo channel evolution: Algorithms and theoretical limits. In *EuCAP*, Mar. 2009.

[8] J. Wilson and N. Patwari. Radio tomographic imaging with wireless networks - tech report. *http://www.eng.utah.edu/ jwilson/files/RTI.pdf*, Sep 2008.

Footnotes:

[1]The distillation stage as described in this work does not involve any exchange of parity information, and is different from the advantage distillation in quantum cryptography.

[2]We thank Joey Wilson for sharing his tinyos program for recording the RSS measurements.