MobiCom 2009 Poster: Secret Key Extraction in MIMO-like Sensor Networks Using Wireless Signal Strength

Sriram Nandha Premnath[a] **Sneha K. Kasera**[a] **Neal Patwari**[b]
nandha@cs.utah.edu *kasera@cs.utah.edu* *npatwari@ece.utah.edu*
[a]School of Computing, University of Utah
[b] Department of Electrical and Computer Engineering, University of Utah

In this work, we evaluate the use of multiple sensors for secret key extraction. We find that the key generation rate increases linearly with the number of nodes. We show that the use of multiple nodes causes a significant mismatch in the extracted bits. We address the high bit mismatch problem by adding an iterative distillation stage to the key extraction process.

I. 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, 3]. In our recent work [2], 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 [2] 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.

Wallace et al. [4] have recently proposed the use of multiple-input and multiple-output (MIMO) for enhancing secret key extraction. However, their work is an analytical study, presenting only the simulation results. Further, they assume that multiple antennas belong to the same node. However, due to size and power limitations, sensor nodes do not typically have multiple antennas. In this work, we propose to obtain the multi-antenna capability using multiple sensors.

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 in 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 the 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.

II. Experimental Setup

In our work, we use Crossbow TelosB wireless sensors for the experiments. As Wilson et al. [5][2] describe, the sensors, which form a token ring, take turn in exchanging probe packets and collecting RSS measurements. We use two sets of five sensors each representing Alice and Bob respectively. 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

[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.

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.

Nodes of Alice and Bob are arranged in two parallel rows, with each sensor separated from its neighbor by a distance of about 12 cm, which is greater than the de-correlation distance for signals transmitted in the 2.4 GHz band. We conduct our experiment in a student lab. Nodes representing Alice remain stationary in one corner of the lab while the other set of nodes (Bob) is carried around at normal walking speed. The distance between Alice and Bob is maintained between $2-8$ m. In this work, we use the multiple bit extraction method as described in [2], extracting 2 bits from each RSS measurement.

III. Prohibitively High Bit Mismatch

We define the bit mismatch rate as the percentage of bits that do not match between Alice and Bob. We find that the bit mismatch rate, when using multiple $802.15.4-$compliant sensors, is significantly higher in comparison to our experiments from our earlier work [2] that uses 802.11 single antenna systems. Note that for a mismatch rate of about 22%, the information reconciliation protocol essentially reveals all the bits. So, the collected measurements that exhibit very high bit mismatch are not useful in establishing a secret key.

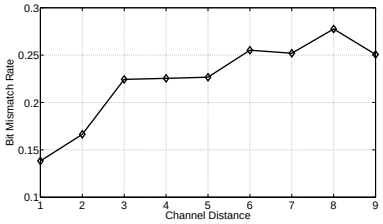

Figure 1: Bit Mismatch Rate vs Channel Distance

We identify the following reasons for such high mismatch rates. First, 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, and also reduces the probing rate on each channel. Both these factors contribute in increasing the bit mismatch rate. This is also verified in a plot of bit mismatch rate vs channel distance, where channel distance is the absolute difference between the node ids (as defined by the token ring order) of the transmitting and receiving sensors. Figure 1 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.

Second, channels in $802.15.4$ are much narrower in comparison to 802.11. A non-reciprocal deep fade (perhaps due to strong interference only at Alice) occurring on a narrow channel significantly reduces the average RSS computed at Alice while not affecting much at Bob. This results in a greater likelihood of asymmetry in measurements, and therefore higher bit mismatch when using narrow channel measurements.

IV. Distillation

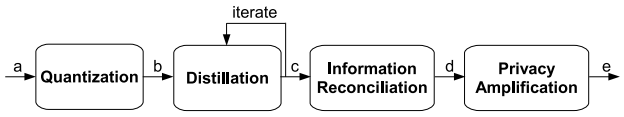

Figure 2: Secret Bit Extraction Process. a - RSS measurements, b - quantization interval labels, c - distilled bits, d - reconciled bits, e - secret bits.

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 2 shows the distillation stage in relation to the other stages of the key extraction process.

Plotting the measurements from channels with large channel distances, we find that a large fraction of consecutive measurements exhibit abrupt transitions from one quantization level to another resulting in asymmetry. The distillation stage seeks to iteratively eliminate such measurements causing abrupt transitions. If the mismatch is still too high even after one round of eliminations, it is necessary to eliminate further; in which case, the next best elimination candidates are those that follow the previously eliminated measurements. When this process is iterated over a number of times, it is guaranteed to improve the bit mismatch rate. Note that the number of iterations required depends on the *current expected mismatch rate* of the channel, which can be determined based on the *history of mismatch rate of the channel*. Algorithm 1 succinctly expresses the steps taken in each iteration.

Algorithm 1 assumes that the quantizer outputs the labels (e.g., a, b, c, d) of each quantization interval

Algorithm 1 Distill Input

```
while there is input do
  if current_label = previous_label then
    Output current_label
  else
    Output exclude_label
    previous_label ← current_label
  end if
end while
```

instead of the actual bit pattern assigned to each interval. $exclude\_label$ is a special label indicating an eliminated measurement. In each iteration, the distiller processes the input as shown in Algorithm 1. For the first iteration, the distiller gets its input from the quantizer; and for the successive iterations, the distiller's output becomes the input for the next iteration. In the last iteration, the distiller outputs the bit patterns corresponding to each quantization interval. The following example shows two iterations of distillation; the _ symbol represents the $exclude\_label$.

Distiller Input: $aaaaabbaaaabbbbbaaaa\cdots$
Iteration 1 output: $\_aaaa\_b\_aaa\_bbbb\_aaa\cdots$
Iteration 2 output: $\_\_aaa\_\_\_\_aa\_\_bbb\_\_aa\cdots$

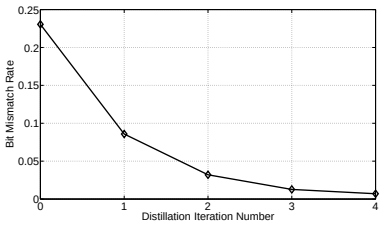

Figure 3: Effectiveness of distillation in drastically reducing the bit mismatch rate

Figure 3 shows the improvement in bit mismatch rate with each iteration for the 5×5 configuration. Without distillation, the average mismatch rate is about 23%, in which case information reconciliation leaks out all the bits. But two iterations of distillation reduces the mismatch rate to a sufficiently small value ($< 5\%$) for efficient information reconciliation.

V. Gain in Secret Bit Rate

We define secret bit rate as the average number of secret bits extracted per probe transmission. Figure 4 shows a plot of the secret bit rate as a function of number of nodes in each set (Alice/Bob). It can be clearly seen that the secret bit rate increases linearly with the number of nodes. We also measure the randomness of the extracted bit streams using NIST's approximate

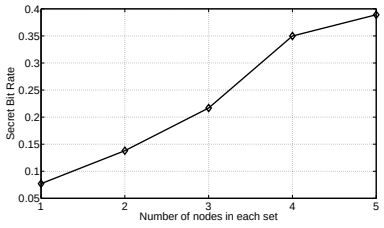

Figure 4: Secret bit rate vs Number of nodes

entropy test. We find that the entropy values for the extracted secret bit streams from all the $N \times N$ configurations ($1 \leq N \leq 5$) are close to 1, the ideal value.

VI. Conclusions

We created a simple MIMO-like sensor testbed to explore the possibility of using MIMO systems for improving the secret key extraction process. We obtained very promising and interesting initial results. Essentially, our experiments showed that the key generation rate 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 wireless nodes to establish a secret key where information reconciliation by itself cannot. We showed that just two iterations of distillation can progressively bring down a bit mismatch rate of about 23% to less than 5%. In the future, we will conduct a deeper exploration on using single-bit quantization for the MIMO case - while it yields lower *quantized bits per probe*, it also reduces the bit mismatch rate which may ultimately help in achieving higher secret bit rate in comparison to multiple bit extraction. In addition to RSS, we will also study the impact of using phase information, obtained from MIMO receivers, on 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 *ACM CCS*, 2007.

[2] 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*, 2009.

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

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

[5] J. Wilson and N. Patwari. Radio tomographic imaging with wireless networks. *IEEE Transactions on Mobile Computing*, 2009.