

On Passive Inference Attacks Against Physical-layer Key Extraction*

Matthew Edman
Rensselaer Polytechnic
Institute
edmanm2@cs.rpi.edu

Aggelos Kiayias
University of Connecticut
aggelos@cs.uconn.edu

Bülent Yener
Rensselaer Polytechnic
Institute
yener@cs.rpi.edu

ABSTRACT

Physical-layer key extraction techniques attempt to derive a shared symmetric cryptographic key between two wireless devices based on the principle of channel reciprocity, which states that the signal envelope between two communicating devices is strongly correlated. A key security assumption made in previous literature is that the signal envelope observed by an adversary located greater than a half-wavelength away is uncorrelated with that shared between the two communicating devices; however, this assumption has yet to be rigorously evaluated in previous work on physical-layer key extraction. In this paper, we present an experimental analysis that examines the relationship between the channel measurements used to extract a symmetric key between two devices and those observed by one or more distantly located passive adversaries. We find that, contrary to previous assumptions, there does exist a strong correlation in measurements observed by adversaries located significantly greater than a half-wavelength away from two communicating wireless devices. Further, we provide initial results that show the extent to which the adversary is able to leverage such correlations to infer portions of the key extracted between two devices using previously published physical-layer key extraction techniques.

Categories and Subject Descriptors

C.2.1 [Computer-Communication Networks]: Network Architecture and Design—*Wireless communication*

Keywords

Wireless networking, physical-layer security, passive attacks

1. INTRODUCTION

Physical-layer key extraction between two wireless devices is based on the principle of *channel reciprocity* which states

*This work was supported by the National Science Foundation under award number CNS-0831366.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

EUROSEC'11 10-APR-2011, Salzburg, Austria

Copyright 2011 ACM 978-1-4503-0613-3/11/04 ...\$10.00.

that, in the absence of interference, both devices will observe the same signal envelope. The two parties can rapidly sample the wireless channel between them and use the resulting sequence of channel samples to independently extract a bit string via some previously agreed upon algorithm. The primary advantage of such physical-layer key extraction schemes over traditional key management protocols is that they allow any two wireless devices within transmission range of each other to negotiate a shared symmetric cryptographic key over a wireless broadcast channel without pre-shared keying material.

A key assumption underlying the security of physical-layer key extraction commonly made in previous literature is that the signal envelope observed by an adversary located greater than a half-wavelength away is uncorrelated with that shared between the two communicating devices [2, 10]. Yet, surprisingly, little attention has been given to understanding the possible threats posed by passive adversaries attempting to subvert the key extraction process in real environments. Our primary goal in this paper is to fill in this critical gap in security analyses from prior work and better understand how robust physical-layer key extraction really is in the presence of adversarial monitoring within various practical deployment environments. We consider how various factors, such as the environment type, number of eavesdropper nodes and node position impacts the adversary's ability to infer portions of the resulting cryptographic key.

2. RELATED WORK

Hershey et al. first explored the possibility of secure key exchange between two wireless transceivers based on the reciprocity of the channel between them [6, 5]. This concept has been further considered in the context of diverse hardware platforms, such as steerable parasitic array radiator antennae [1, 11], OFDM modulation systems [8], software-defined radio platforms [9] and even 60GHz millimeter-wave transceivers [4]. A number of techniques for deriving a bit-string from such correlated wireless channel measurements have been proposed. Tope and McEachen [13] devised a scheme for lognormal shadowed fading channels. A related scheme by Azimi-Sadjadi et al. [2] also used the pattern of *deep fades* observed by the two endpoints relative to the root mean square of the observed signal strength.

Rather than set a static threshold with which to convert instances of deep fades to bits, Mathur et al. developed a novel scheme that adapts to changing channel conditions by subtracting a windowed average from each channel sample [10]. Two devices—Alice and Bob—look for consecutive

sequence of samples above or below a dynamically-chosen threshold, which they define as an *excursion*. Alice and Bob publicly exchange the center indices of each excursion and derive a key based on whether each excursion in the intersection is positive or negative. Assuming a passive adversary’s signal strength measurements are uncorrelated with Alice’s and Bob’s, knowing the center index of each excursion does not yield additional information to the adversary. Jana et al. proposed an extension to Mathur et al.’s protocol called Adaptive Secret Bit Generation (ASBG) [7] in which Alice and Bob output one or more bits for every sample contained in an excursion, rather than simply one bit per excursion. ASBG also incorporates the “Cascade” protocol developed by Brassard and Salvail to perform key reconciliation and privacy amplification [3].

Our Contributions. Our focus, separate from previous work on active attacks [15, 14], is strictly on passive attacks against physical-layer key extraction in which the adversary observes an execution of the key extraction protocol between two parties without interfering. Mathur et al. briefly considered a passive adversary (say, Eve) who attempts to derive the same key as Alice and Bob using only her own channel measurements. The authors assumed that Eve simply applies the same thresholding algorithm as Alice and Bob. We, however, consider alternate strategies in this paper that a passive adversary can leverage in order to increase the probability of inferring portions of the key extracted between Alice and Bob in various types of real-world environments. Additionally, our work is the first to consider the possibility of multiple colluding passive adversaries and the impact they may have on the secrecy of Alice and Bob’s shared key.

3. NETWORK & THREAT MODEL

The network model is composed of two or more independent network devices that communicate with each other via some predetermined wireless communication protocol (e.g., the 802.15.4-based ZigBee standard). In our experiments, the network contains a stationary “base station” and one or more mobile nodes who wish to establish a secret key with the base station via a physical-layer key extraction protocol. We define a distinction between “honest” network nodes and “adversary” nodes. The honest network nodes make no attempt to disrupt or compromise the key extraction protocol executed between other honest nodes and the base station. The network may also contain one or more adversary nodes that are placed in the network by an attacker, whose objective is to determine the cryptographic key negotiated between the base station and a target legitimate node without revealing to the target that its key may be compromised. The adversary nodes are strictly passive in that they make no attempt to influence, intercept or otherwise interfere with the key extraction protocol executed between legitimate nodes.

As is typical in a security analysis of a cryptographic system, we assume the adversary possesses knowledge of all public parameters of the system. In our target scenario, these parameters include the frequency and protocol the legitimate network devices use to communicate, the bit quantization algorithm in use and its parameters. Further, the key extraction protocol itself may necessarily divulge public information, including ping sequence numbers and excursion indices as required by excursion-based key derivation algo-

gorithms [10, 7]. We further assume that all adversary nodes in the network are capable of communicating with any other adversary node via some out-of-band mechanism, thereby avoiding detection by the legitimate nodes. The out-of-band mechanism may be implemented as either a wired connection (e.g., Ethernet) or a wireless protocol not observed by the legitimate nodes (e.g., operating on a different radio frequency). The adversary nodes can thus exchange their own channel measurements with each other without detection.

4. EXPERIMENTAL PLATFORM

The hardware basis for our experimental platform was the Crossbow MICAz sensor mote, which is composed of an Atmel ATmega128L microcontroller and a Chipcon CC2420 IEEE 802.15.4-compliant RF transceiver. The RF transceiver operates at a user-configurable frequency within the 2.40-2.48 GHz ISM band (we used 2.48 GHz in our experiments) and with a data rate of 250 kbps. Transmit power is also programmable from -10 dBm to 0 dBm, which we have fixed at the maximum level of 0 dBm for each MICAz device in our test network.

The software portion of our experimental platform primarily consisted of a ping-like application that we implemented on top of the TinyOS operating system. Our implementation consists of three components: a base station (Alice), a mobile client (Bob) and an eavesdropper implementation (Eve). Bob sends a PING_REQUEST frame to Alice containing a 1-byte frame type field and a 4-byte sequence number, in addition to the standard 802.15.4 frame header. Upon receiving a ping request, Alice records the sender’s 1-byte address, sequence number and the received frame’s RSSI value as computed by the CC2420 transceiver. Alice then sends a PING_RESPONSE frame to Bob containing the sequence number from Bob’s original PING_REQUEST. Bob records the response frame’s RSSI value, increments the sequence number and repeats the above process. If Bob does not receive a response to his PING_REQUEST within 500ms, he will increment the current sequence number and transmit a new ping request.

The eavesdropper implementation, Eve, simply listens passively for any frames transmitted by any other nearby nodes. Eve records the source and destination addresses, frame type, sequence number and observed RSSI value for that frame. After the experiment is manually terminated, the recorded data is uploaded from each sensor mote via a serial connection to a laptop for further processing and analysis.

5. SIGNAL CORRELATION

In this section, we describe the results of our analysis of the correlations found in signal envelopes observed by passive adversaries. Our intent is to demonstrate that, contrary to assumptions in recent work [10, 2], the signal envelope observed by an adversary located several wavelengths away from Alice and Bob exhibits strong correlation with the envelope observed by Alice and Bob. Within each test environment, shown in Figure 1, we placed the eavesdropper nodes in various positions around the stationary base station in order to test the effects of distance from the base station, node placement and eavesdropper mobility on the adversary’s ability to observe the signal envelope between Alice and Bob. We discuss each of these factors in the following sections.

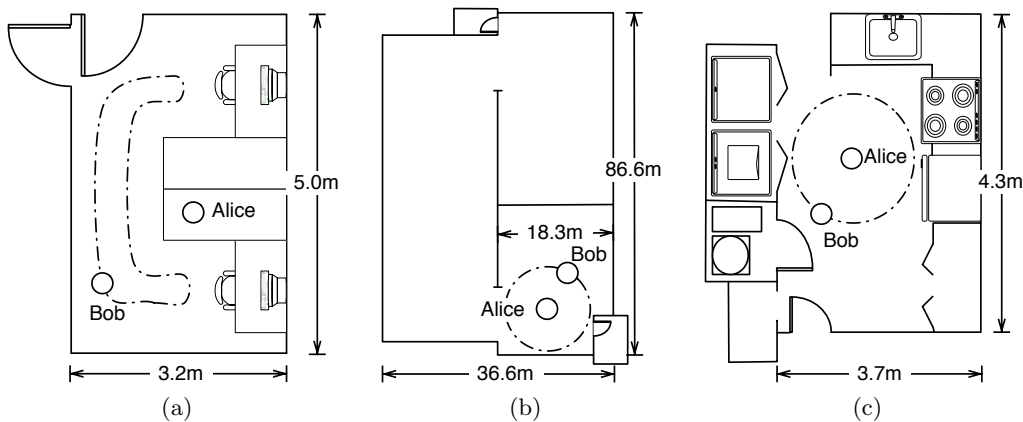


Figure 1: The three test environments in our evaluation included (a) a small, indoor academic office environment, (b) a large, open, outdoor environment on the room of a parking garage, and (c) a typical residential environment. The dot-dash line roughly indicates the path of the mobile node (Bob) relative to the stationary base station (Alice).

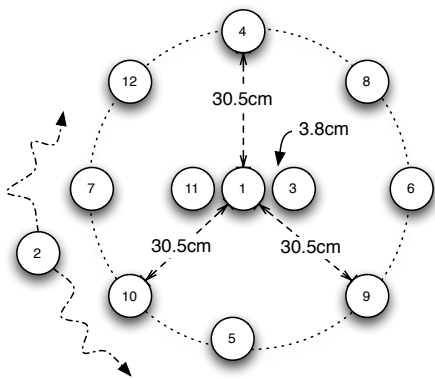


Figure 2: Eavesdropper nodes placed in a circle with a 30 cm radius around the stationary base station (ID 1). The mobile node (ID 2) moved arbitrarily around the test environments in Figures 1(a) and (b).

5.1 Node Placement

We placed 10 stationary eavesdropper nodes in a circular pattern around Alice, as shown in Figure 2. Eight of the nodes were located approximately 30 cm away from Alice, while two were placed only 3.8 cm away on both sides of Alice. In terms of wavelength $\lambda = \frac{v}{f}$, where our carrier frequency $f = 2.48 \times 10^9$ Hz, we have $\lambda = 12.1$ cm. Thus, two eavesdroppers are located within a half-wavelength from Eve while eight are more than five times farther than a half-wavelength away. Consequently, previous assumptions suggest that nodes 3 and 11 should be strongly correlated with Alice’s signal envelope whereas measurements from the remaining eavesdropper nodes should be entirely uncorrelated.

The eavesdropper nodes in the indoor environment shown in Figure 1(a) are arranged such that half of the nodes are between Alice and Bob during the experiment, while the other half are located on the opposite side of Alice. Alice and Bob executed the ping protocol described in the previous section for several minutes, resulting in over 17,000 channel samples collected by each node. Throughout this section, we use the metric of normalized *cross-correlation* [12]

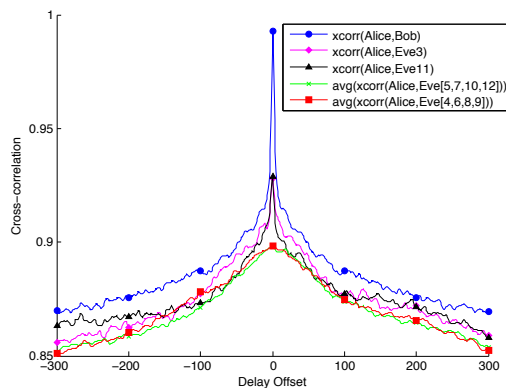


Figure 3: Cross-correlation of Alice’s measurements with those of Bob and the eavesdropper nodes. Even the nodes located multiple wavelengths away from Alice exhibited strong correlation.

to compare the similarity of observed sequences of channel measurements.

From Figure 3, we see the strongest cross-correlation between Alice and Bob, which is to be expected to due to the principle of reciprocity. The nodes exhibiting second and third highest cross-correlation with Alice’s measurements are nodes 3 and 11 (i.e., the nodes located less than a half-wavelength away). More interestingly, we observe that there is no significant difference in average cross-correlation between nodes located in the line-of-sight between Alice and Bob (nodes 5, 7, 10 and 12), and those located on the opposite side of Alice (nodes 4, 6, 8 and 9). These results suggest that even eavesdroppers located multiple wavelengths away from Alice and Bob can still observe a highly correlated signal envelope, regardless of whether they are located on a line-of-sight between Alice and Bob.

5.2 Indoor vs. Outdoor Environments

To evaluate whether the cross-correlation results from the previous experiment hold when moving to an outdoor environment, we also repeated the previous experiment with the node layout shown in Figure 2 on an open rooftop of a

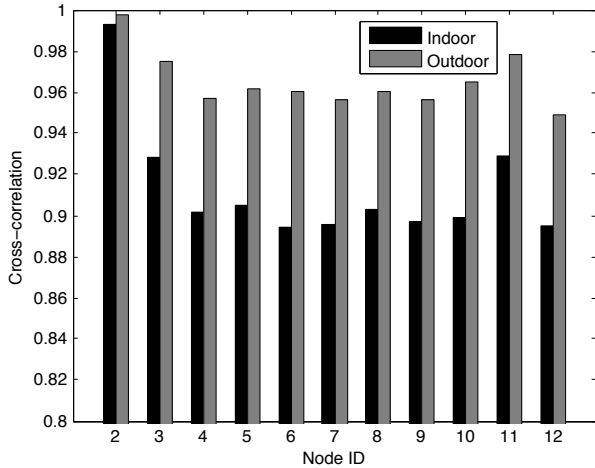


Figure 4: Comparison of eavesdropper cross-correlation between indoor and outdoor environments. We observed a higher average degree of cross-correlation in the outdoor environment, likely due to the absence of significant multipath effects or other interference from nearby transmitters.

large, empty parking garage as depicted in Figure 1(b). Alice and the eavesdropper nodes were again stationary, with Bob moving in an arbitrary pattern around their position. Slightly more than 20,000 samples were collected during the experiment. We then computed the cross-correlation Alice and Bob, as well as the cross-correlation between Alice and each of the eavesdroppers.

The results of this experiment compared with those of the previous indoor experiment are shown in Figure 4. While the cross-correlation between Alice and Bob was roughly similar in the two environments, we observed a significantly higher average degree of eavesdropper cross-correlation in the outdoor environment than in our indoor experiments. Much of this difference in signal cross-correlation is likely due to the absence of significant multipath effects resulting from fewer nearby reflective surfaces in the environment.

5.3 Eavesdropper Distance

We next consider the effect that distance can have on the cross-correlation between Alice’s signal envelope and that of an eavesdropper. Eleven eavesdropper nodes were placed in a pattern concentric circles around the stationary base station with an increasing distance. Four nodes were located 30 cm away, four nodes were placed 60 cm away and three nodes were placed about 90 cm away (we were limited by the number of hardware nodes available in our test infrastructure). These distances are equivalent to approximately 2.5, 5.0 and 7.5 wavelengths, respectively. As in previous tests, an experiment was conducted in the environment from Figure 1(b), resulting in slightly more than 20,000 channel measurements collected by each node.

We computed the cross-correlation of Alice’s channel measurements with those of the eavesdropper nodes located at each distance interval from Alice, the results of which are shown in Figure 5. We can see that as the distance between Alice and the eavesdroppers increases, the observed cross-correlation decreases rapidly within the first 30 cm. Fur-

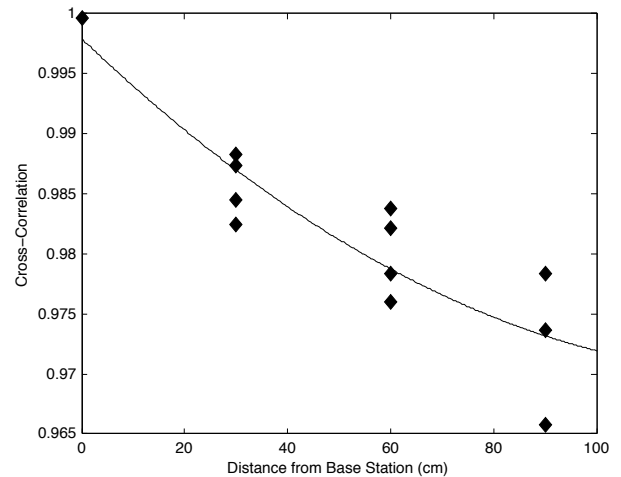


Figure 5: Observed signal strength cross-correlation as measured by eavesdropper nodes placed at an increasing distance from the base station in an outdoor environment.

ther, as the distance increases, the variance in eavesdropper cross-correlation measurements also increases. This suggests an eavesdropper should be located within approximately 1 meter from Alice to obtain a signal envelope strongly correlated with Alice’s. We note that it is possible, however, that an eavesdropper with a more sensitive receiver than was used in our experiments may still be able to obtain strongly correlated measurements at greater distances.

5.4 Stationary vs. Mobile Eavesdroppers

We also considered an alternate eavesdropper strategy in which a subset of eavesdropper nodes attempt to trail Bob as he moves about the environment. Within the indoor environment from Figure 1(c), we set up an experiment consisting of five stationary eavesdroppers and six mobile eavesdroppers arranged as shown in Figure 6(a). The mobile eavesdroppers were mounted on a movable platform with Bob so that their distance relative to Bob’s position was constant throughout the experiment, during which around 17,500 channel measurements were collected by each node.

The experiment resulted in a cross-correlation of 0.998 between Alice and Bob, indicating their signal envelopes were, as expected, strongly correlated. Further, the eavesdropper node located closest to Alice (node 9), exhibited a cross-correlation of 0.95, while the average cross-correlation for all stationary eavesdroppers was 0.939 which appears consistent with previous experiments. The results from the mobile eavesdroppers were more surprising. As shown in Figure 6(b), the two mobile eavesdroppers located closest to Bob (nodes 3 and 4) exhibited strongly negative cross-correlation, while those located farthest from Bob (nodes 7 and 8) showed strongly positive cross-correlation. Measurements from the two nodes mounted in the middle of the mobile platform (nodes 5 and 6) were uncorrelated with Bob. While these results were surprising and counter-intuitive, they were consistent and, we believe, warrant further examination.

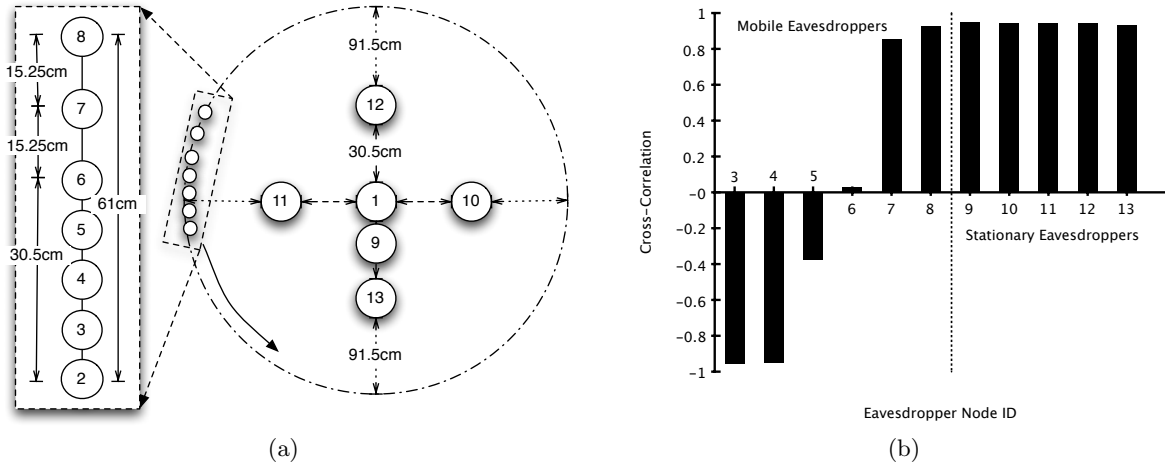


Figure 6: (a) Node placement for an experiment consisting of six mobile eavesdroppers and five stationary eavesdroppers, and (b) cross-correlation results for the stationary and mobile eavesdropper nodes. The mobile nodes closest to Bob observed a strongly negative cross-correlation while those farthest from Bob observed a strong positive cross-correlation.

6. COMPARISON OF KEY INFERENCE ALGORITHMS

Having shown that indeed correlations can be found in signal envelopes observed by passive adversaries across various environments and at varying distances from Alice and Bob, we now consider how such correlations can be leveraged to reduce the secrecy of the symmetric key extracted between Alice and Bob.

6.1 Inference Algorithms

We first briefly describe the seven inference algorithms we considered in our evaluation. We divide the algorithms into two categories—algorithms that can be implemented by an individual passive adversary, and those that combine measurements from multiple coordinating adversaries in an attempt to increase their inference accuracy. In each of the following descriptions, we let m be the minimum excursion length as defined by Mathur et al.’s algorithm and $w \geq m$ be the length (in samples) of the sliding window average subtracted from each new channel sample. Due to space limitations, we refer the reader to [10] for full details on excursion-based thresholding and its parameters.

Independent Adversaries

- **Nearest-neighbor Excursion (NNE).** Eve finds the nearest excursion by searching left and right in her own channel measurements from the observed excursion index. If the nearest excursion is positive, then output a 1. Otherwise, output a 0.
- **Average RSSI.** Compute the average observed signal strength over Eve’s set of channel measurements. For each excursion index i exchanged between Alice and Bob, Eve computes the average signal strength of the m samples in her observations centered about i . If the latter average is greater than the former, output a 1. Otherwise, output a 0.
- **Windowed Average RSSI.** For each observed excursion index i exchanged between Alice and Bob, Eve computes the average of w samples centered about i .

Eve then computes the average of m samples also centered about i . If the latter average is greater than the former, output a 1. Otherwise, output a 0.

Multiple Coordinating Adversaries

- **Weighted NNE.** For each eavesdropper node, find the nearest-neighbor excursion as in single-node NNE. If the nearest excursions observed by a simple majority of the eavesdropper nodes are positive, the adversary outputs a 1. Otherwise, output a 0.
- **Average NNE.** The adversary first computes an average signal envelope by averaging the signal strength of each ping frame as observed by all eavesdropper nodes. The adversary then applies the single-node NNE algorithm on the average eavesdropper signal envelope and outputs the result.
- **Multinode Average RSSI.** The adversary first computes an average signal envelope as in the previous algorithm. The adversary then applies the Average RSSI algorithm above to the average eavesdropper signal envelope and outputs the result.
- **Multinode Windowed Average RSSI.** The adversary first computes an average signal envelope as in the previous algorithm. The adversary then applies the Windowed Average RSSI algorithm above to the average eavesdropper signal envelope and outputs the result.

6.2 Results & Discussion

To evaluate the independent and coordinated inference algorithms described in the preceding sections, we first derived a shared key K_{ab} between Alice and Bob using the excursion-based approach from Mathur et al [10] with a minimum excursion length of $m = 4$ samples, sliding window size of $w = 50$ samples and an $\alpha = 0.5$, which is used to establish upper and lower signal strength thresholds. We then applied each of the previously described inference algorithms to both the indoor and outdoor experimental datasets described in Section 5 to derive an inferred keystring K_e for each algorithm.

Algorithm	Distance from Base Station				Overall
	< 6 cm	30 cm	60 cm	90 cm	
Nearest-neighbor Excursion (NNE)	81.97%	60.36%	61.58%	55.18%	62.25%
Average RSSI	79.13%	60.09%	60.07%	54.44%	62.78%
Average Window RSSI	76.52%	56.10%	54.08%	53.84%	59.07%
Weighted NNE	69.85%	65.74%	63.82%	56.36%	70.38%
Averaged NNE	73.83%	66.31%	62.94%	56.80%	68.93%
Multinode Average RSSI	81.10%	68.97%	64.47%	55.04%	74.11%
Multinode Avg. Window RSSI	78.96%	64.21%	57.02%	48.68%	71.82%

Table 1: Summary of passive key inference algorithm results expressed as the percentage of secret key bits correctly inferred by the adversary located at increasing approximate distances from the base station. The overall accuracy for single-node algorithms is the average accuracy over all individual nodes, while the overall accuracy for the multi-node algorithms is the accuracy of each algorithm using channel measurement data from all node distances as input.

We computed the Hamming distance between K_{ab} and K_e for each inferred key to identify how many bits differ between the two. The results for each algorithm were averaged across all datasets and are summarized in Table 1. The Average RSSI and related Multinode Average RSSI algorithms performed the best overall with an inference accuracy of 62.78% and 74.11%, respectively. When breaking the results down by environment type instead of eavesdropper distance, we found the Average RSSI method yielded an average accuracy of 58.37% in an indoor environment versus 66.21% outdoors. The Multinode Average RSSI method resulted in an average indoor accuracy of 69.67% and 77.90% outdoors. This coincides with our cross-correlation results in Section 5 showing that eavesdroppers in an open, outdoor environment have a higher level of signal strength measurement correlation with Alice and Bob.

7. CONCLUSIONS

In this paper, we have presented results showing that, contrary to assumptions in previous work, the signal envelope observed by an adversary located several wavelengths away from Alice and Bob exhibits strong correlation with the envelope observed by Alice and Bob. Further, we have also provided initial results that show a passive adversary is able to leverage such correlations to infer significant portions of the key extracted between two legitimate devices. Certainly there is room for development of more sophisticated algorithms that may result in improved key inference accuracy in both the single and multiple adversary scenarios, but these results demonstrate that a passive eavesdropper’s observations can result in the adversary being able to correctly infer a non-trivial fraction of the resulting key.

We also note that while an adversary can infer a significant portion of the key, he does not necessarily know *which* bits were correctly inferred. Thus, we envision a more probabilistic approach that assigns “confidence weights” to each bit output by the attacker that denotes the probability of that bit being correct, which can then be used to devise a prioritized brute force search such that keys with the highest aggregate confidence weight are tested first, hopefully reducing the average time required to find the correct key. This probabilistic approach is the focus of our current research.

8. REFERENCES

- [1] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka. Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels. *IEEE Transactions on Antennas and Propagation*, 53(11):3776–3784, November 2005.
- [2] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener. Robust key generation from signal envelopes in wireless networks. In *Proceedings of the 2007 ACM Conference on Computer and Communications Security (CCS '07)*, pages 401–410. ACM Press, 2007.
- [3] G. Brassard and L. Salvail. Secret-key reconciliation by public discussion. In *Proceedings of the 1993 Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology (EUROCRYPT '93)*, pages 410–423. Springer-Verlag, 1994.
- [4] M. A. Forman and D. Young. The generation of shared cryptographic keys through half-duplex channel impulse response estimation at 60ghz. In *Proceedings of the 2010 International Conference on Electromagnetics in Advanced Applications (ICEAA '10)*, pages 627–630, 2010.
- [5] A. A. Hassan, W. E. Stark, J. E. Hershey, and S. Chennakeshu. Cryptographic key agreement for mobile radio. *Digital Signal Processing*, 6:207–212, 1996.
- [6] J. Hershey, A. Hassan, and R. Yarlagadda. Unconventional cryptographic keying variable management. *IEEE Transactions on Communications*, 43:3–6, 1995.
- [7] S. Jana, S. N. Premnath, M. Clark, S. K. Kasper, N. Patwari, and S. V. Krishnamurthy. On the effectiveness of secret key extraction from wireless signal strength in real environments. In *Proceedings of the 15th Annual International Conference on Mobile Computing and Networking (MobiCom '09)*, pages 321–332, September 2009.
- [8] A. Kitaura and H. Sasaoka. A scheme of private key agreement based on the channel characteristics in ofdm land mobile radio. *Electronics and Communications in Japan, Part 3 (Fundamental Electronic Science)*, 88(9):1–10, 2005.
- [9] Z. Li, W. Xu, R. Miller, and W. Trappe. Securing wireless systems via lower layer enforcements. In *Proceedings of the 5th ACM workshop on Wireless Security (WiSec '06)*, pages 33–42, 2006.
- [10] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik. Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel. In *Proceedings of the 2008 ACM Conference on Mobile Computing and Networking (MobiCom '08)*, pages 128–139. ACM Press, September 2008.
- [11] T. Ohira. Secret key generation exploiting antenna beam steering and wave propagation reciprocity. In *Proceedings of the 2005 European Microwave Conference*, pages 9–12, October 2005.
- [12] J. G. Proakis and D. G. Manolakis. *Digital Signal Processing*. Pearson Prentice Hall, fourth edition, 2007.
- [13] M. Tope and J. McEachen. Unconditionally secure communications over fading channels. In *Proceedings of the 2001 Military Communications Conference (MILCOMM 2001)*, pages 54–58, 2001.
- [14] V. Yakovlev, V. Korzhik, and G. Morales-Luna. Key distribution protocols based on noisy channels in presence of an active adversary: Conventional and new versions with parameter optimization. *IEEE Transactions on Information Theory*, 54(6):2535–2549, 2008.
- [15] M. A. Zafer, D. Agrawal, and M. Srivatsa. Bootstrapping coalition manets: Physical-layer security under active adversary. In *Annual Conference of ITA (ACITA) 2009*, 2009.