# Improving Robustness of Key Extraction from Wireless Channels with Differential Techniques

Bin Zan Marco Gruteser Fei Hu *
WINLAB, Rutgers University
671 Route 1 South, North Brunswick, NJ 08902-3390
{zanb, gruteser}@winlab.rutgers.edu
*Department of Electrical and Computer Engineering, The University of Alabama
*101 Houser Hall, Tuscaloosa, AL, 35487-0286
*fei@eng.ua.edu

***Abstract*—Secure wireless communications typically rely on secret keys, which are difficult to establish in an ad hoc network without a key management infrastructure. Theoretically, the channel reciprocity and spatial decorrelation properties can be used to extract secret key, especially in a Rayleigh fading channel. However, as shown in some prior work by inserting or removing intermediate objects between the communication nodes, the strength of the secret key generated through such methods is low. Furthermore, the impact of small fluctuations also reduces the bit matching rate of such key agreement methods. In this paper, we propose a differential approach which uses the relative difference between two RSS values to determine the value of a secret bit. Additionally, the moving average method can be more easier and properly adapted to the differential approach which reduces the impact of small fluctuations. Experiment results and numerical evaluation show the proposed method has higher security strength, speed and matching rate comparing to a baseline from prior research work.**

## I. Introduction

Key agreement, the process through which two parties share a secret key, is a fundamental challenge in networking security. Traditional approaches rely on infrastructure with online trusted third parties (TTP) [1], such as the well-known Kerberos [2] scheme and Otway-Rees protocol [3]. However, in mobile ad hoc networks, the lack of infrastructure implies that there is no central authority that can be referred to when it comes to make trust decisions about other parties in the network and when that accountability cannot be easily implemented. Furthermore, since the node mobility is unrestricted, the topology may be unpredictable making central authority assumption infeasible. On the other hand, cost-effective processors with limited computational abilities make public-key cryptography, such as Diffie-Hellman key establishment [4] almost impractical for wireless ad hoc and sensor networks.

Prior work on key agreement in sensor networks and ad hoc networks has largely focused on pre-distribution protocols (e.g., [5], [6]). In such protocols, a large pool of symmetric keys is chosen and a random subset of the pool is distributed to each node. Thus, two nodes can establish a session key if they share a common key. However, the strict requirement for pre-distribution might not be always available. For example, in a mobile ad hoc network, the nodes or the users (sharing no prior secret information) may just meet on the spot where there is likely no single trustworthy proxy or TTP for key pre-distribution.

"When two antennas A and B have no non-linear components radiate identical signals, the outputs of the antennas due to their excitation by the signal originating at the other antenna will also be identical" [7], this behavior is known as the reciprocity theorem. On the other hand, as a result of the rapid spatial decorrelation properties of the wireless multi-path channel, even a small distance between two receive-nodes can lead to a quite different channel response. Based on above two properties, Hershey et al. [8] first present the concept of using physical layer characteristics for key management. Recently, in [9], the authors exploit the idea by using level-crossings and quantization to extract bits from wireless channels. However, the secret bit generating rate is much lower than theoretically expected. In [10], the authors exploit the differences of arrival time among the direct wave and the delayed wave as the shared information between authorized users in a UWB Systems. Using Espar (Electronically Steerable Parasitic Array Radiator) antenna to measure the RSSI, [11] generates secret key bits based on the median value of the RSSI profiles. In Zang et al.'s key dissemination protocol [12], channel state is used to XOR with secrete key oriented from one of the users.

All of the previous attempts are suffering from the active attack described in [13]. In such an attack, the adversary tries to control the channel characteristic by inserting or removing intermediate objects to decrease or increase the wireless signal. In addition to that, small fluctuations due to the presence of noise, interferes and hardware limitations reduces the effect of channel reciprocity.

To overcome above issues, we propose a method which uses the relative difference between two channel impulse response or simply received signal strength (RSS) values to determine the value of a secret bit. We call it differential key agreement. Comparing to previous work, it generates stronger secret key in a shorter time period.

The remainder of this paper is organized as follows. Section 2 describes the system model. Section 3 introduces the main

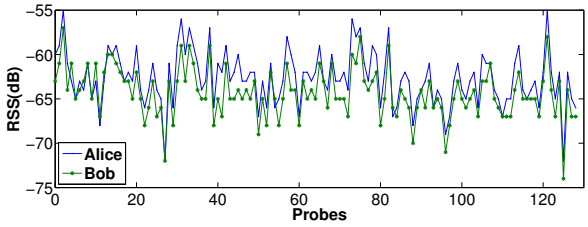


Fig. 1. Channel reciprocity theorem.

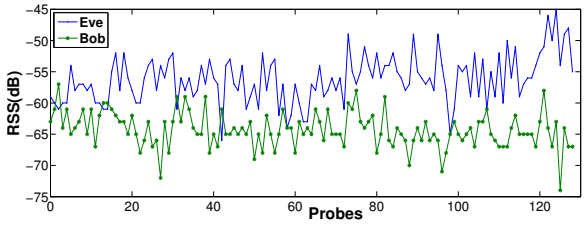


Fig. 2. Spatial decorrelation property.

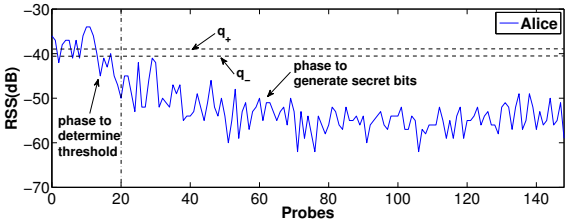


Fig. 3. Pre-probe method. The thresholds $q_+$ and $q_-$ are calculated as shown in [9].

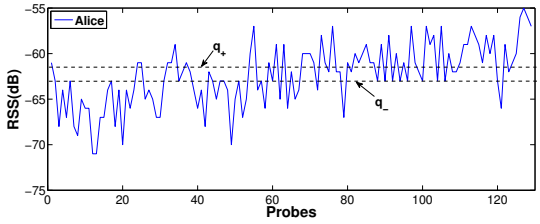


Fig. 4. Post-probe method. The thresholds $q_+$ and $q_-$ are calculated as shown in [9].

algorithm and its theoretical background. Section 4 evaluates the proposed algorithm through experiments and numerical analysis. Section 5 concludes.

## II. System Model

In this model, we assume that in a mobile ad hoc network, all mobile nodes are equipped with half duplex wireless transceivers. Each node can measure the channel between itself and others. When two legitimate mobile nodes (Alice and Bob) plan to set up a secure communication channel, they need to agree on some secret key first. However, there is no centralized server or TTP to help distribute secret keys among mobile nodes. A mobile eavesdropper (Eve) is assumed to be able to listen to all the communications between Alice and Bob. To avoid being detected by legitimate mobile nodes, Eve keeps a short distance to any of them. Eve won't prevent Alice and Bob from building the secret keys or modify any message exchanged by Alice and Bob. However, she has some basic abilities to influence the channel characteristic between Alice and Bob. For example, she can reduce the signal strength between them by inserting an intermediate object to block a large portion of the wireless channel. Due to the complexity of the multi-path Rayleigh Fading environment, Eve can't identify the impact of her action on the Alice/Bob channel during a coherence time. Finally, Eve can't restrict the movement of Alice and Bob.

## III. Differential Key Agreement

### A. Theoretical Background

The proposed differential secret key agreement is based on two fundamental principles: Channel Reciprocity and Spatial Decorrelation. As shown in Fig.1, channel reciprocity describes the phenomenon that the communication nodes at the two ends of a channel will observe identical channel characteristic, such as channel impulse response or received signal strength (RSS) value. On the other hand, due to the spatial decorrelation, Eve, who is at a different location from Bob, observes different RSS values for Alice-Eve channel comparing to Bob's observation of the Alice-Bob channel, as shown in Fig.2.

### B. Existing Problems

First of all, the key idea of most existing works to extract secret key from RSS values is Quantization, in which, one or two threshold values are either determined through a pre-probe phase such as in [9], [14] or a post-probe process [13], [11]. The value of a secret bit is obtained by comparing the RSS values with threshold values. However, as shown in [13], by inserting or removing intermediate objects between Alice and Bob, Eve can force the curve of detected RSS values to appear as the one shown in Fig. 3 or Fig. 4.

If we use entropy to evaluate the strength of a secret key as below:

$$H_i = -p_0 \log p_0 - (1 - p_0) \log(1 - p_0) \tag{1}$$

$$H_{total} = \sum_{i=0}^{i=N} H_i \tag{2}$$

where $N$ is the whole secret key length, $p_0$ is the posterior probability when the secret bit is 0 based on advesrary's knowledge. Then, it is easy to see that the strength of the final secret keys generated from both figures are low.

Second, it is known that small fluctuations reduce the effect of channel reciprocity. Especially when the real channel variations are smaller than the small fluctuations caused by noise, interferes etc. As an example, Fig.5 shows that when end users are static, small fluctuations dominate the RSS variations. Under such conditions, no secret bit can be extracted from

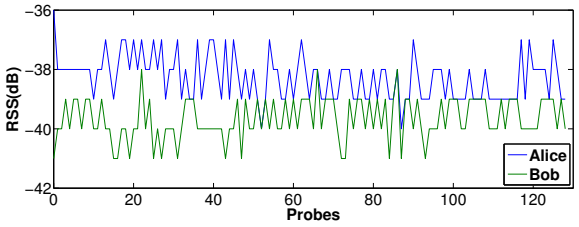


Fig. 5. Small fluctuations dominate the channel variations if users are static.

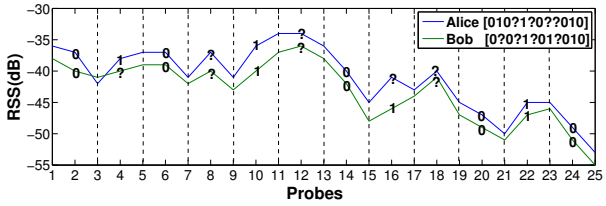


Fig. 6. Differential approach: fixed interval.

the channel. The proposed algorithm should be able to lessen the impact of small fluctuations.

### C. Main Algorithm

Instead of using absolute threshold values of RSS, the proposed differential approach uses the relative difference between two RSS values to determine the value of a secret bit.

The differential approach can be summarized in the following steps:

1) Sample collection: Both Alice and Bob collect a period $T$ of RSS values using their maximum probe rate.
2) Segments division: Divide the sequence of probes into segments by every $\tau$ number of probes.
3) Small fluctuations removal: Using moving average method to reduce the influence of small fluctuations by width $d$.

$$Y = \frac{x_1 + x_2 + x_3 + ... + x_d}{d} \tag{3}$$

4) Bit extraction: Secret bit is generated by comparing a RSS sample of each segment (for example the first RSS value of the segment). Set a bit to 1 if there is an increase by more than $\epsilon/d$, and 0 if there is a decrease by more than $\epsilon/d$. $\epsilon$ is an approximate estimate of the small fluctuations, it could be different for Alice and Bob[1]. Note, to reduce the computation load, we only need to calculate the moving average of one value in each segment.
5) Information exchange: Alice sends Bob only the positions of those probes which are used by her to generate secret bits. From those positions, Bob picks the ones he can also extract secret bits and replies back to Alice.

Fig.6 gives an example for the key agreement scheme. For the sake of simplicity, in this example, we assume the moving

[1]Different devices may have different accuracy on RSS value estimation.

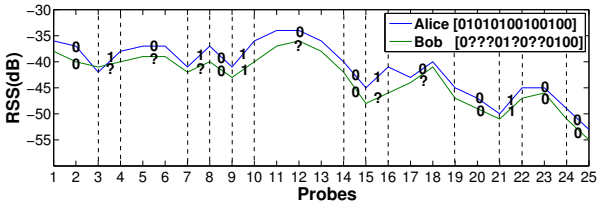


Fig. 7. Differential approach: dynamic method.

average width $d = 1$, $\tau = 2$ and the value of $\epsilon$ for both Alice and Bob is equal to 3. Alice obtains a sequence of bits 010?1?0??010 by comparing the first RSS value of each segment. She is not certain about the bit values at positions '4,6,8,9' in the sequence. Then she sends Bob a message to disclose these information. On the other hand, Bob obtains bit sequence 0?0?1?01?010. In addition to what Alice is not sure of, Bob adds position '2' to the uncertain bit list and informs Alice. After taking out the uncertain bits, both Alice and Bob obtain the final secret bit sequence 0010010[2]. To further improve efficiency, we introduce another parameter $\epsilon_2$ related to the small fluctuations, $\epsilon_2 = a * \epsilon$, $0 < a < 1$. When only one of Alice and Bob is not sure about a bit at a specific position, she/he uses $\epsilon_2$ instead of $\epsilon$ to identify a bit value. Through this way, more secret bits can be generated since $\epsilon_2$ is smaller than $\epsilon$. For the case in Fig. 6, assume $\epsilon_2 = 0.5 * \epsilon$, two more bits 1 will be generated at segment 2 and 8.

To further reduce parameter dependence, we propose a dynamic differential approach in which the fixed interval $\tau$ is removed. In this approach, we use a reference RSS value which is set to be the first probed RSS value at the beginning. Every RSS value starting from the second one will be compared with this reference until a difference bigger than $\epsilon/d$ is observed. A secret bit is generated depending on whether the difference is an increase or decrease and then the reference will be updated to the RSS value where the process has stopped. The balance RSS values will be compared with the new reference until the next big difference appears. In the end, Alice sends Bob the positions of all those particular RSS values which are used as references. Upon receipt, Bob compares his own RSS values at those positions to verify if there is big difference as well, and reply Alice with only the positions passing the verification.

In Fig. 7, we assume $d = 1$ and $\epsilon = 3$. Based on the method described above, Alice first generates a bit sequence 01010100100100. Then Bob obtains 0???01?0??0100 and recommends Alice to remove uncertain bits at position '2,3,4,7,9,10'. Therefore the final secret bit sequence is 00100100. If using two $\epsilon$ values, for example $\epsilon_2 = 0.5 * \epsilon$, the bit sequence Bob obtains becomes 0?0101001?0100. This changes the final common bit sequence to 001010010100.

[2]Note, the sequence of secret bits both Alice and Bob obtain are not necessarily to be the final bits order of the secret key. They could exchange the positions of any two bits and/or remove any bit from the sequence as they wish.

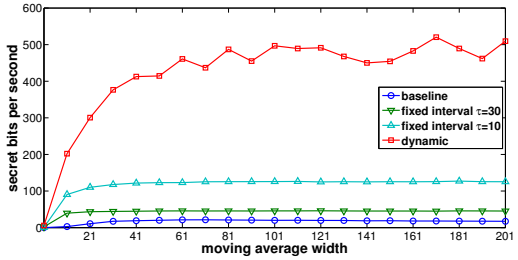


Fig. 8. Secret bit generating rate. For baseline, $\alpha = 0.125$, $m = 4$, for fixed interval $\tau = 30$ and for both fixed interval and dynamic scheme $\epsilon = 6$ and $\epsilon_2 = 3$

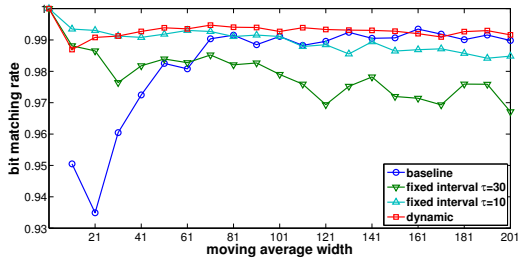


Fig. 9. Secret bit matching rate. For baseline, $\alpha = 0.125$, $m = 4$, for fixed interval $\tau = 30$ and for both fixed interval and dynamic scheme $\epsilon = 6$ and $\epsilon_2 = 3$

## IV. Experimental Results and Numerical Evaluation

In the evaluation section, we try to answer 1) how fast, 2) how reliable, and 3) how strong in security strength can our proposed algorithms achieve. Thus, we compare the bit generating rate, the bit matching rate and the high entropy secret bit generating rate of both differential approaches proposed in section III-C to the baseline scheme [9]. Additionally, we also study the effect of parameters selection, including the fixed interval value $\tau$, the moving average $d$ and the estimated small fluctuation value $\epsilon$. Due to page limit, we will only show results related to the parameter $\tau$ here. We conduct a real world experiment in an indoor (office) environment at our lab. In this experiment, two mobile nodes (Two Linux boxes both are equipped with Atheros AR5212 Mini PCI wireless interfaces), Alice and Bob, are moving in a multi-path fading channel environment and collecting 50000 RSS value samples at the same time.

The major advantages of using differential method is that it can prevent the attack described in section 3.1.2. For instance, if an adversary inserts a large object between the Alice-Bob channel which blocks a large number of reflection or refraction signals, all RSS values observed by Alice and Bob may become very small from then on. All previous methods will extract all-0 bit sequence from the channel. While, through differential method, secret bit can be 1 as long as the current segment has enough increase on RSS value comparing to a previous segment, even though both of them are actually very low from a global view. As an example, the baseline generates secret keys of extreme low entropy in Fig. 3 and

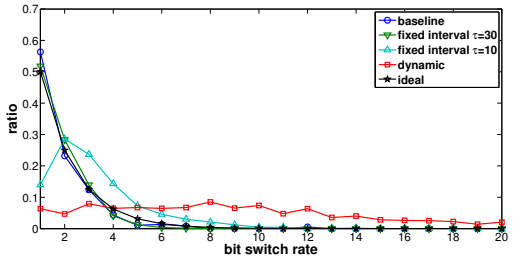


Fig. 10. Comparison of bit switch rate.

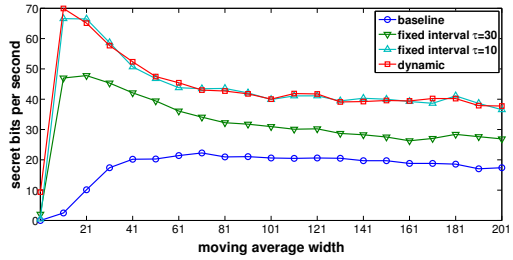


Fig. 11. The estimation of high entropy secret bit generating rate.

Fig. 4 (entropy $H_{total} \approx 0$). By setting $d = 10$ and $\epsilon = 3$, the proposed fixed interval algorithm generates $H_{total} = 22$ and $H_{total} = 14$ secret keys for Fig. 3 and Fig. 4, respectively.

In Fig.8, we compare the generating rates of secret bits among three schemes: baseline, fixed interval differential (interval $\tau = 10$ and interval $\tau = 30$) and dynamic differential while the matching rate of them are all high as shown in Fig.9. Note, the baseline is executed by adding a step to subtract moving average. To achieve a high bit generating rate, we set $\alpha = 0.125$ and $m = 4$ for the baseline. For the fixed interval scheme, we show two cases in which $\tau = 10$ and $\tau = 30$. The roughly estimated value of $\lambda/2v$ is around 25, which means under an ideal environment, an uncorrelated secret bit can be generated every 25 probes. As shown in the figure, all of the differential approaches perform better than the baseline. In both fixed interval cases, the smaller the value of $\tau$, the higher the generating rate. This is easy to be understood because small $\tau$ means more RSS values will be compared and consequently more large scale variations may be caught. However, the negative side is it may generate correlated bits that have low entropy. This fact is shown in Fig.10, where the $x$ value indicates the length of the continuous 1 or 0 bits, and the y value is the appearance ratio of each length. Comparing to the ideal case, the curve of $\tau = 10$ has higher ratio at large $x$ values. The dynamic approach has the highest bit generating rate as shown in Fig.8, but even lower entropy. In Fig.10, the trend of baseline and fixed interval $\tau = 30$ cases are closer to the ideal case. However we could convert low entropy bit sequence into high entropy bit sequence through some methods. For example, randomly pick bits from long and unique bit 1/0 sequence to convert them into shorter bit sequence. After conversion, as shown in Fig.11, the dynamic approach and the fixed interval with $\tau = 10$ still have the

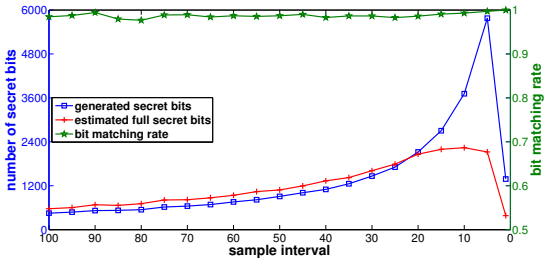


Fig. 12. Using moving average width 21, the maximum number of secret bits generated is 6492 out of 50000 samples, the bit matching rate is higher than 0.99. The maximum number of high entropy secret bits can be generated is 2239 still with a high matching rate.

highest bit rate even though it is reduced comparing to Fig.8.

From Fig.11, we see the actual effect of moving average width on different schemes. Both small and large moving average width lead to low bit generating rates. A small width makes it hard to remove small fluctuations for all schemes, while a large moving average width results in more low entropy bits as shown in Fig.10[3]. In our approaches, the width could be estimated as some value close to $\lambda/2v$. However, for the baseline it is hard to find a proper width to eliminate the large scale fading. Overall, the proposed algorithm can generate about 40 secret bits every second which leads to an almost 200% enhancement comparing to the baseline scheme.

Next, we study the bit generating rate for the fixed interval differential approach given different $\tau$ values. As discussed before, we set the width of moving average to 21, a value close to $\lambda/2v$ in this experiment. As shown in Fig.12, in general, the smaller the interval, the more secret bits can be generated, but when $\tau$ is too small, say equal to 1, the generating rate dramatically goes down. This is because small $\tau$ will not make room to generate enough difference between two neighbor segments. When $\tau$ is equal to 5, it generates more than 5777 secret bits, which is a lot more than what the maximum baseline generates (2595 bits with matching rate only 0.4906), while the bit matching rate is still higher than 0.99[4]. After converting the secret bit sequence into high entropy sequence, the maximum number, 2239, of secret bits happens at $\tau = 10$, is twice as for the baseline case. When interval $\tau$ is equal to 20, it generates more than 2000 bits. Another advantage of this approach over the baseline is that the parameter $\tau$ is easy to be determined by setting it as a value close to $\lambda/2v$.

## V. Conclusion and Future Work

In this paper, we have presented a secret key agreement scheme which relies on channel reciprocity and spatial decorrelation properties. Different from prior works, the proposed scheme is robust even when an active attacker tries to control the channel characteristic by inserting or removing intermediate objects between the communication nodes. The proposed scheme can remove the influence of small fluctuations through moving average more efficiently than prior works. Experiment results and numerical evaluation show that the proposed approach obtains fast secret bit generating rate, about 40 bits per second. Comparing to the baseline scheme, this is an almost 200% enhancement. In the future, we plan to develop a full dynamic piecewise regression scheme to further reduce parameter dependence.

[3]While the proposed differential methods can take advantages from large scale fading by using a little small moving average width, the baseline has to use large width. Otherwise, the baseline is completely exposed to the active attack mentioned before.

[4]Using information reconciliation, such as mentioned in [15]. higher matching rate can be further achieved by sacrificing some bits generating rate.

## References


[1] P. A, S. R, W. V, C. D, and T. J, "Spins: Security protocols for sensor networks," *Wireless Nets*, vol. 8, no. 5, pp. 521–534, 2002.

[2] J. Steiner and J. I. Schiller, "An authentication service for open network systems," in *Usenix Conference Proceedings*, 1988, pp. 191–202.

[3] D. Otway and O. Rees, "Efficient and timely mutual authentication," *SIGOPS Oper. Syst. Rev.*, vol. 21, no. 1, pp. 8–10, 1987.

[4] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, no. 6, pp. 644–654, 1976. [Online]. Available: citeseer.ist.psu.edu/diffie76new.html

[5] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *ACM Conference on Computer and communication Security(CCS)*, 2004.

[6] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *SP '03: Proceedings of the 2003 IEEE Symposium on Security and Privacy*. Washington, DC, USA: IEEE Computer Society, 2003, p. 197.

[7] R. Wilson, D. Tse, and R. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," in *Ultra-Wideband, 2007. ICUWB 2007. IEEE International Conference on*, Sept. 2007, pp. 270–275.

[8] J. Hershey, A. Hassan, and R. Yarlagadda, "Unconventional cryptographic keying variable management," *Communications, IEEE Transactions on*, vol. 43, no. 1, pp. 3–6, Jan 1995.

[9] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," in *MobiCom '08: Proceedings of the 14th ACM international conference on Mobile computing and networking*. New York, NY, USA: ACM, 2008, pp. 128–139.

[10] A. Kitaura, T. Sumi, K. Tachibana, H. Iwai, and H. Sasaoka, "A scheme of private key agreement based on delay profiles in uwb systems," March 2006, pp. 1–6.

[11] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *Antennas and Propagation, IEEE Transactions on*, vol. 53, no. 11, pp. 3776–3784, Nov. 2005.

[12] Z. Li, W. Xu, R. Miller, and W. Trappe, "Securing wireless systems via lower layer enforcements," in *WiSe '06: Proceedings of the 5th ACM workshop on Wireless security*. New York, NY, USA: ACM, 2006, pp. 33–42.

[13] 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 '09: Proceedings of the 15th annual international conference on Mobile computing and networking*. New York, NY, USA: ACM, 2009, pp. 321–332.

[14] 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*. New York, NY, USA: ACM, 2007, pp. 401–410.

[15] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data." Springer-Verlag, 2004, pp. 523–540.