A Robust Generation Technique of Common Information Based on Characteristic of Multipath Fading Channel by Shaking Handheld Devices

Tomohiro Iwamoto, Shigeaki Tagashira, Yutaka Arakawa, Akira Fukuda

Graduate School / Faculty of Information Science and Electrical Engineering
Kyushu University
744 Motooka, Nishi-ku, Fukuoka, Japan
{tomohiro, shigeaki, arakawa, fukuda}@f.ait.kyushu-u.ac.jp

Abstract: A rapid increase in handheld devices with wireless communication capabilities, such as cellular phones and smart phones, enables data communication in face-to-face situations. The easy realization of secure data communication in such situations is necessary for ensuring safe and reliable networking environments as short-range wireless networks become more popular. One approach involving the generation of secret keys in each communication device using variations of the received signal strength indication (RSSI) values has been proposed in literature. However, it has a problem in that there are positions where eavesdroppers are able to obtain RSSI values that are highly correlated with those of legitimate devices. To address this problem, we propose a filtering technique that eliminates eavesdroppable parts from RSSI variations. Additionally, it is important to shake either one or both of two legitimate devices to change the propagation, considering that the elimination exploits the periodicity of the shake. Furthermore, we implemented a prototype system realizing the proposed method and evaluated its effectiveness. The results indicate that the proposed method can increase the robustness of common information, which is generated into the secret key without degrading its generation speed.

1 Introduction

Recently, with the rapid proliferation of wireless-enabled applications and devices, such as cellular phones and smart phones, there is an increased opportunity for wireless connections to be made with bystanders. The public nature of wireless transmission for data communication has the potential to allow eavesdroppers easy access to the transmitted data. Therefore, many studies to realize secure communications, such as public key cryptography, quantum cryptography, have been proposed in literature. Among them, secret key cryptography is the most common because its processing speed is so high that computationally limited devices would have to process a large amount of encrypted data. However, it has a problem in that there may be leaks of the secret key during distribution and management. Therefore, the secret key generation technique that uses random fluctuations of the wireless channel between legitimate users has attracted considerable attention as a method that requires no distribution or management. This technique is based on the reciprocity of radio wave propagation. With this technique, two devices do not have to distribute the secret key because it is generated by each device without the need to send any information regarding it. In addition, there is also no need to manage the secret key because the devices generate a different secret key each time. Furthermore, one of the notable features is that we can change the length of the secret key based on the generation time. The generation of a secret key with a certain length requires modification of the radio propagation and extraction of its characteristics. Methods for changing the propagation have been proposed such as the use of an electronically steerable parasitic array radiator (ESPAR) antenna [1] and multi-antenna [2]. For extraction of the characteristics, techniques including ways to utilize the deviation of the arrival time between direct waves and multipath waves [3] and orthogonal frequency-division multiplexing (OFDM) model [4] have been also proposed. These schemes achieve precise and high-speed generations owing to special devices.

On the other hand, methods for generating the secret key from variations of the received signal strength indication (RSSI) values [5], which can be measured by non-dedicated wireless devices, have been recognized as beneficial for ubiquitous communication systems. However, this method has two problems: one is that the speed with which the secret key is generated is as low as a few bits per second. The other is that there are positions where eavesdroppers are able to obtain highly correlated variations of RSSI values for legitimate users in certain environments [6, 7]. To address the latter problem, we propose a filtering technique that eliminates eavesdroppable parts from variations of RSSI values. Additionally, it is necessary to shake either one or both of two legitimate devices to change the propagation, considering that the elimination exploits the periodicity of the shake. We implement a prototype system that realizes the proposed scheme and generates common information that is processed into the secret key using quantization and reconciliation techniques. In this study, the evaluation of the generated information with correlation coefficients shows the effectiveness of the proposed scheme. The results indicate that the proposed method significantly contributes in improving the robustness of the generated information without degrading the generation speed.

The rest of this study is organized as follows. In Section 2 , we describe the rationale behind the method that shares RSSI values of two devices and implement a preliminary experiment to confirm their effectiveness in real environments. Section 3 presents details of the proposed scheme, and Section 4 shows the effectiveness of the proposed method. Finally, we conclude this paper and discuss our future tasks in Section 5 .

2 Reciprocity of radio wave propagation and fluctuation of RSSI

In this section, we show that legitimate users (Alice and Bob) can observe similar variations of RSSI values because of the reciprocity of radio wave propagation. First, we consider the variation of RSSI values. Second, we introduce the reciprocity of radio wave propagation. Finally, in actual experiments, we confirm that the variation of RSSI values observed by one legitimate user is similar to that by the other.

2.1 Variation of RSSI values

RSSI values fluctuate because of various causes. We summarize these causes as follows.

Cause1: Distance between sender and receiver

Cause2: Multipath fading

Cause3: Noise

Cause1 means that the RSSI value is closely correlated to the distance between legitimate users, i.e., the changes in the distance cause the variation of RSSI values. The RSSI value is high when the distance is short. In contrast, it is low when the distance is long or some obstacles exist between them.

A receiver receives radio waves from a transmitter through both direct and indirect paths (i.e., multipath). The direct wave interferes with the multipath wave, which leads to attenuation of the direct wave. This phenomenon is called ”fading.” The impact of fading varies with differences in the transmission distance between direct and indirect paths. Cause2 means that fading causes variations in RSSI values. Cause3 means that RSSI values fluctuate because of noise, which is dependent on employed devices, white noise, and others.

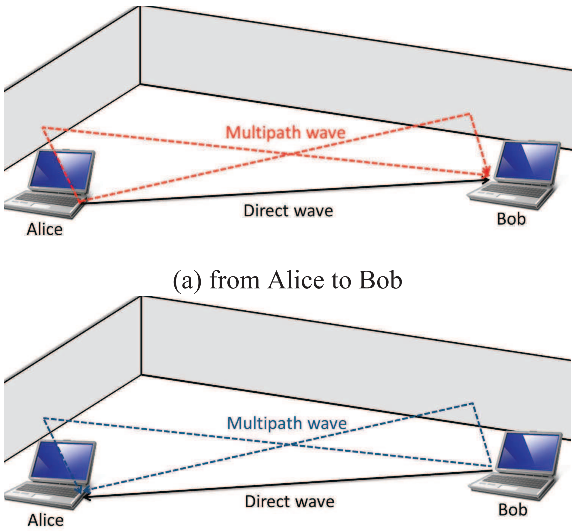
2.2 Reciprocity of radio wave propagation

Radio wave propagation traverses the same path in both directions, from Alice to Bob (Fig.1-(a)) and from Bob to Alice (Fig.1-(b)), unless either of them or any surrounding objects are moved. This is called the ”reciprocity of radio wave propagation.”

2.3 Preliminary experiment

Both devices can observe the same variation of RSSI values in environments in which the reciprocity of radio wave propagation works well. This similar variation of RSSI values in both directions is mainly due to Cause1 and Cause2, as was described in Section 2.1. In this section, we conduct an experiment with existing equipment and confirm that this works well in real world environments.

We prepared a quiet room (6 meters × 12 meters) and deployed three laptops: Alice (transmitter), Bob (receiver), and Eve (eavesdropper), as shown in Figure 2. Using a ping command, Alice sent 1000 ICMP echo request packets to Bob every 1.0 s and Bob replied to each packet with an ICMP echo reply packet. During this period, Alice shook her device to change the radio channel and recorded the RSSI values and sequence numbers for the packets in the reply. On the other hand, Bob and Eve recorded those parameters for the request packets. Figure 3 illustrates the positional relation between a laptop and an antenna, and the way that Alice shook her laptop. We used Atheros devices as wireless



(a) from Alice to Bob

(b) from Bob to Alice

Figure 1: Transmission path for radio signal between Alice and Bob.

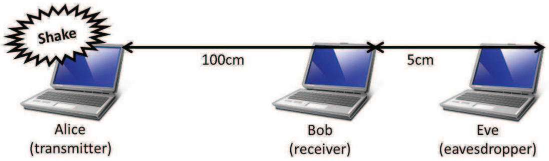
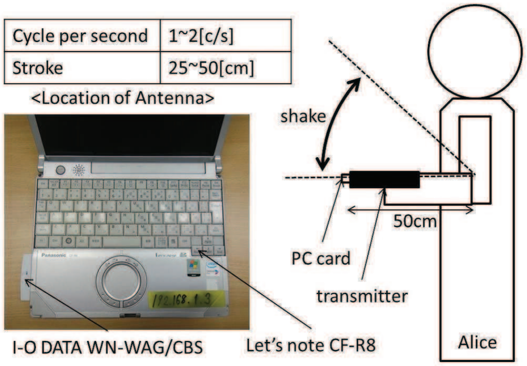


Figure 2: Location of terminal devices in this preliminary experiment

network cards, operating in the IEEE802.11a band. In addition, to avoid interference during the observations, we turned off all additional functions, such as diversity.

Figure 4 shows the variations of the RSSI values observed in this experiment. The vertical axis represents the RSSI value, and the horizontal axis represents the sequence number. Closed diamonds, triangles, and squares indicate the RSSI values recorded by Alice ($RSSI_{Ab}$ profile), Bob ($RSSI_{Ba}$ profile), and Eve ($RSSI_{Ca}$ profile), respectively. The recordings made by Eve were covert. It is clear from Figure 4 that legitimate users can observe similar fluctuations even in real environmental conditions. However, the fluctuations in $RSSI_{Ab}$ and $RSSI_{Bc}$ are not identical because Alice and Bob were not able to simultaneously transmit and receive the signals using typical commercial wireless transceivers. We also consider noise to be a factor contributing to these gaps. In this experiment, the deviation was small, since the round trip time (RTT) was much shorter than the time required for changing channels. In addition, the impact of Cause1 and Cause2 was much



Cycle per second	1~2[c/s]
Stroke	25~50[cm]

Figure 3: Method for mounting antenna and shaking terminal device

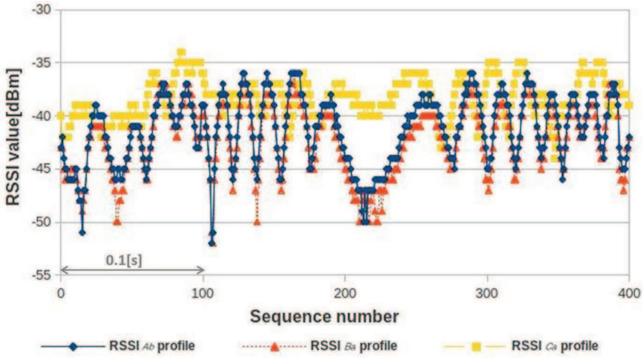


Figure 4: Fluctuation of observed RSSI values in this preminary experiment

more significant than that of Cause3. It is widely recognized that the fluctuation is an uncontrollable random phenomena. This makes it very difficult for it to be estimated by eavesdroppers. However, eavesdroppers can observe RSSI variations that correlate well with those of legitimate users, who may be present at a location less than a few wavelengths from either of them, as was the case with Eve in Figure 2.

3 Proposed method

In this section, we describe our proposed scheme, which provides legitimate users with common information generated into the secret key using RSS-based secret key extractions, as in [1, 8, 9, 10]. The secret key also makes it difficult for an eavesdropper to carry out sniffing attacks. The main idea of our proposed method is to use a bandpass filter to extract only common fluctuations and eliminate the part of the RSSI variation that is vulnerable to eavesdropping. First, we explain the method for making RSSI profiles which are used to generate common information. Second, we discuss the implementation of the bandpass filter.

3.1 Procedure for making RSSI profiles

In this study, we call records for a tuple of two items: RSSI value and its sequence number ”RSSI profile.” We describe below instructions for making an RSSI profile.
[**Procedure for making an RSSI profile**]

Step1: Either or both users shake their devices.

Step2: During shaking, the transmitter sends an ICMP echo request packet to a receiver as often as needed to a predetermined set.

Step3: Whenever the receiver gets the request packet, the receiver replies with an ICMP echo reply packet to the transmitter.

Step4: The receiver records the RSSI value and sequence number for these request packets.

Step5: The transmitter records those parameters for the reply packets.

Each legitimate user makes an RSSI profile in accordance with these steps. In the next section, we will explain how to extract common information from this RSSI profile. To get closer common information, it is recommended that the transmitter sends a request packet more frequently and that the RTT be shorter. In the next section, we show that the transmitter has to send more than $2 \times \beta$ request packets every second.

3.2 Extraction of common information with a bandpass-filter

In this section, we propose a filtering technique to extract correlated common information that exists for legitimate users from the RSSI profiles. More specifically, we analyze the RSSI profile on the frequencies and reduce unsuitable frequencies in the spectrum using the discrete Fourier transform (DFT). In this study, ”unsuitable frequencies” can be estimated by eavesdroppers.

In Section 2.1, we discussed the fluctuations that occur. The result of analyzing the fluctuations of the RSSI profile in the frequency domain is shown in Figure 5, which shows that fluctuation1 and fluctuation2 have almost the same variation of RSSI values between the legitimate users owing to the reciprocity of radio wave propagation. These variations gradually decline with increasing frequency. In contrast, fluctuation3 is observed as a different variation. If white noise exists, it has a constant power over the entire range of

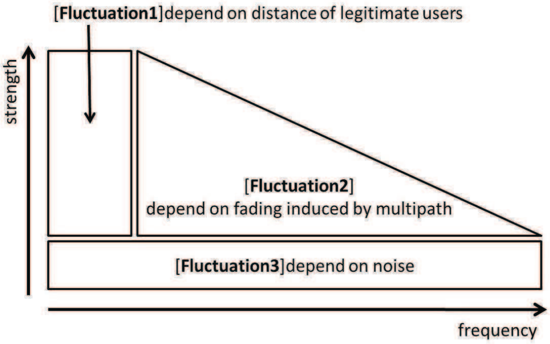

[Fluctuation1]depend on distance of legitimate users
strength
[Fluctuation2]
depend on fading induced by multipath
[Fluctuation3]depend on noise
frequency

Figure 5: Modeling variation of RSSI values in the frequency domain

frequencies. Therefore, for high frequencies, the noise decreases the correlation of the RSSI profile between legitimate users. On the other hand, for low frequencies, the variation is likely to be estimated by eavesdroppers. For these reasons, we propose using a bandpass filter that allows only frequencies from α Hz to β Hz. In our method, α and β are customized parameters.

4 Evaluation

In this section, we discuss the effectiveness of our proposed scheme in a real environment. In particular, we confirm that our scheme reduces the correlation of the RSSI variation between the eavesdropper and legitimate users, even when the eavesdropper is very close to either of the legitimate users or on the axis of the signal connecting the legitimate users. In [6, 7], it was reported that in these positions, eavesdroppers are able to obtain RSSI variations that agree well with those of legitimate users. First, we explain about data sets used in this evaluation. Second, we select the customized parameters of the bandpass filter (α and β) and evaluate our scheme with the correlation coefficient.

4.1 Data set

We made many sets of RSSI profiles for this evaluation. The procedure for making RSSI profiles was described in Section 3. In this evaluation, we used setting values and environment similar to those used in Section 2.1, except for the distance between Bob and Eve, i.e., Eve is placed on the line connecting Alice and Bob. More specifically, we placed Eve at 30 points between 1 and 100 cm and made 10 sets of RSSI profiles for each point. We show an adversary model of this evaluation as follows. We follow the model as described in [5].

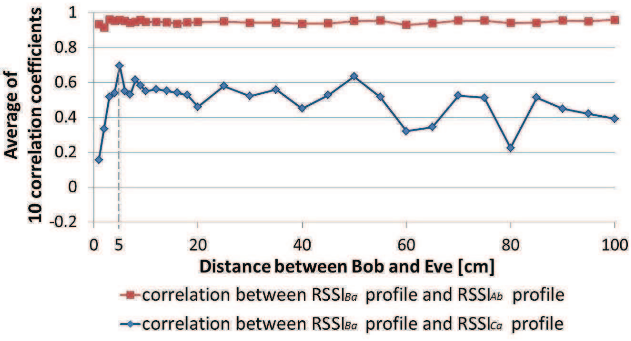


Figure 6: Relation between correlation coefficient and distance before using bandpass-filter

[**Adversary model**]

- Eve can listen to the communication between Alice and Bob.
- Eve knows our proposed scheme and the parameters used in our scheme.
- Eve can observe RSSI values everywhere.
- Eve is a passive adversary who cannot carry out a person-in-the-middle attack.

4.2 Parameter setup

Figure 6 shows the relationship between the strength of the correlation and Eve's position. We employ the correlation coefficient as a metric to evaluate the correlation strength. Closed diamonds represent the correlation coefficient between Alice and Bob, and closed squares represent that between Bob and Eve. From the figure, we observe that Eve can estimate a part of the legitimate RSSI profile, when she is on the line between Alice and Bob. In particular, Eve's RSSI profile has the highest correlation when the distance between Bob and Eve was 5 cm (nearly equal to one wavelength of 5 GHz). We focus on this point and select appropriate values for α and β.

We filtered the RSSI profiles ($RSSI_{Ab}$, $RSSI_{Ba}$, and $RSSI_{Ca}$) that were observed when the distance between Bob and Eve was 5 cm, with the bandpass filter allowing only frequencies from α Hz to β Hz. We call these outputs of the bandpass filter "common information." The effect of the tuning parameters (α and β) on the correlation coefficient between legitimate common information are exhibited in Figure 7. In Figure 8, we also show the correlation coefficient between the common information for Bob and Eve. When α is less than five, although the correlation between the legitimate common information

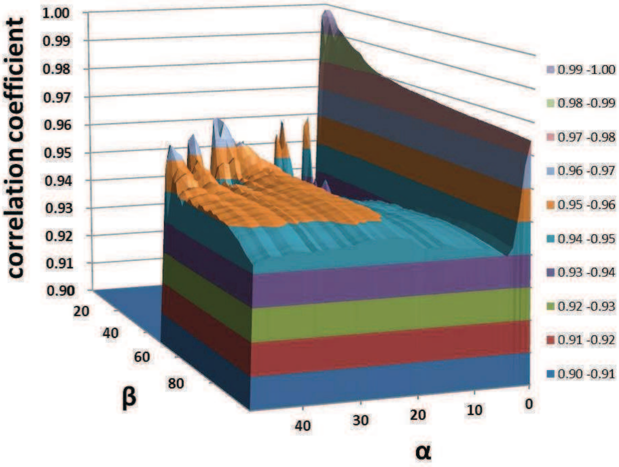


Figure 7: Effect of bandpass-filter on correlation between Alice and Bob

is high, the correlation between that of Eve and Bob is also high. Conversely, both correlations are low when α is high. Moreover, few frequencies pass the filter for sufficient common information to be generated when the range between α and β is small. We examine the best parameters when the difference in the correlation coefficient for legitimate common information and that of Bob and Eve is the highest. As a result, we found that the best-case scenario occurs when α equals 20 and β equals 80. In this evaluation, we determine the effectiveness of the bandpass filter using these values.

4.3 Effectiveness of bandpass filter

We filter the RSSI profiles that are observed in the preliminary experiment with the bandpass filter (α = 20, β = 80). The results are shown in Figure 9, which shows that the correlation between either of the legitimate users and the eavesdropper decreases after filtering. Furthermore, we observe that legitimate users can extract delicate changes of channels since the filter eliminates against the direct wave. This will contribute to increasing the speed with which information is generated.

Similarly, we filter all data sets obtained with the bandpass filter and generate common information. Figure 10 shows the relationship between the correlation of the common information and Eve's location. When compared with Figure 6, it is obvious that the inclusion of the bandpass filter can decrease the correlation between either the legitimate users and eavesdropper, without degrading the correlation between legitimate users.

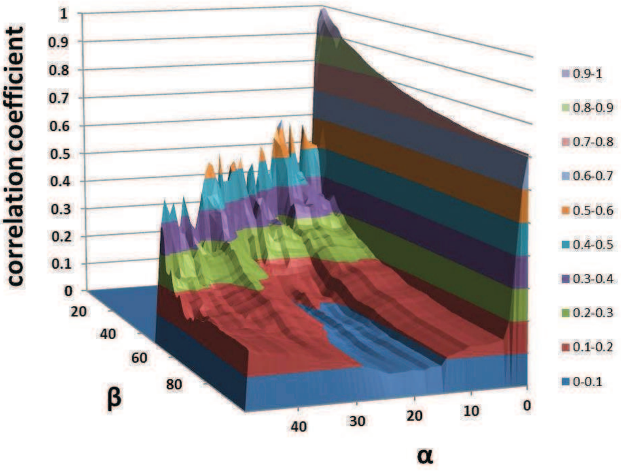


Figure 8: Effect of bandpass-filter on correlation between Bob and Eve

5 Conclusion

We resolved the problem that allowed eavesdroppers at specific positions in certain environments to obtain RSSI values that were highly correlated with those of legitimate users. This occurred when generating secret keys from RSSI variations on the wireless channel. In particular, we used a bandpass filter to make RSSI profiles which were generated into secret keys that were more robust to eavesdropping. Our bandpass filter eliminates vulnerable fluctuation and noise. We also conducted evaluations by performing actual experiments. Our experimental results indicate that our scheme can make it difficult for eavesdroppers to estimate the secret key, without degrading the correlation between legitimate common information. If our scheme is applied to approaches proposed in [1, 8, 9, 10], we can realize more robust secret keys. Also, our scheme appears to increase the speed with which secret keys are generated.

However, we have evaluated the proposed method in only a few environments. This makes our scheme more applicable to the evaluation of the proposed method in various kinds of environments. For example, we evaluate the proposed method in various rooms that have different dimensions and noise using both heterogeneous PC cards and laptops by shaking and setting in other ways, changing the positional relation between legitimate users, and so on. In the future, we will consider applying the proposed method to the automatic selection of tuning parameters with noise levels and analyze the most suitable approaches that generate secret keys from RSSI fluctuation.

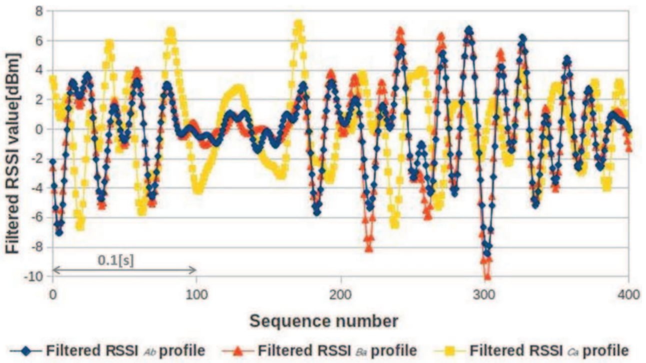


Figure 9: Result of filtering RSSI profiles in preliminary experiment

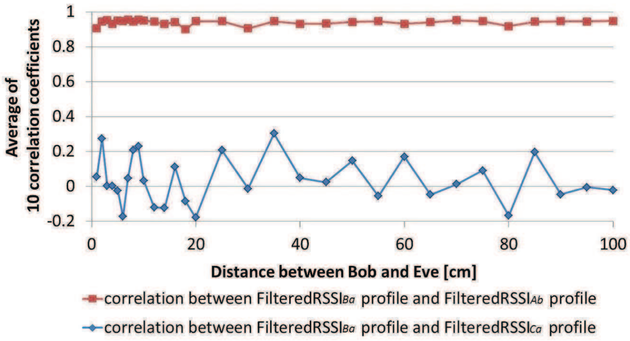


Figure 10: Relation between correlation coefficient and distance after using bandpass-filter

References

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

[2] T. Nishino, H. Iwai and H. Sasaoka. "A study on Secret Key Agreement Scheme in Multi-Antenna System Based on Radio Propagation Characteristics," *IEICE*, Vol. 108, No. 445, pp. 373–378, 2009.

[3] A. Kitaura, T. Sumi, T. Tango, H. Iwai and H. Sasaoka. "A Secret Key Agreement Scheme Based on Multipath Time Delay in UWB System," *Communication Technology, 2006. ICCT '06. International Conference on,* pp. 1-4, 2006.

[4] A. Kitaura, H. Sasaoka, "A scheme of Private Key Agreement Based on the Channel Characteristics in OFDM land mobile radio," *Electronics and Communications in Japan,* Vol. 88, No. 9, 2005.

[5] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N Patwari, 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,* pp. 321–332, 2009.

[6] S. Kwamura, T. Shimizu, H. Iwai and H. Sasaoka. "Position Dependence of Key Capacity in Secrete Key Agreement Scheme Using ESPAR Antenna," *International Symposium on Antennas and Propagation (ISAP2009),* 2009.

[7] M. Onishi, T. Kitano, Iwai and H. Sasaoka. "Improvement of Tolerance for Eavesdropping in Wireless Key Agreement Scheme Using ESPAR Antenna Based on Interference Transmission," *International Symposium on Antennas and Propagation (ISAP2009),* 2009.

[8] 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,* pp. 128–139, 2008.

[9] M. A. Tope and J. C. McEachen. "Unconditionally securecommunications over fading channels," *In Military Communications Conference (MILCOM 2001),* Vol. 1, pp. 54–58, 2001.

[10] 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,* pp. 401–410, 2007.