Experimental Validation of Wireless Secret Key Agreement Using Array Antennas

Takayuki Shimizu, ***Naoki Otani***, ***Takayasu Kitano***, ***Hisato Iwai***, and ***Hideichi Sasaoka***
Graduate School of Engineering, Doshisha University, 1-3 Tatara Miyakodani, Kyotanabe, Kyoto, 610-0321 Japan, {etj1101@mail4, dtk0156@mail4, eti1101@mail4, iwai@mail, hsasaoka@mail}.doshisha.ac.jp

Abstract

This paper considers the problem of wireless secret key agreement based on radio propagation characteristics, where two legitimate parties generate and share a secret key by exploiting the radio propagation characteristics between them in the presence of an eavesdropper. We developed an experimental system using array antennas to implement the wireless secret key agreement. In this paper, we present the experimental system and validate basic characteristics that are fundamental for the wireless secret key agreement, such as the reciprocity and position dependence of radio propagation characteristics, with the developed system.

1 Introduction

Wireless communication is vulnerable to security attacks due to the broadcast nature of the wireless medium. In recent years, there is an increasing interest in secret key agreement schemes exploiting radio propagation characteristics [1–5] as a way to provide security in the physical-layer of wireless communication systems. These schemes enable two legitimate parties to generate and share a secret key from the radio propagation characteristics between them based on the reciprocal property of radio propagation characteristics, which states that the two legitimate parties observe the same radio propagation characteristics. On the other hand, the radio propagation characteristics observed by an eavesdropper is almost uncorrelated with those of the legitimate parties due to the rapid decrease in the spatial decorrelation of radio propagation characteristics if the eavesdropper is located at a sufficient distance away from the legitimate parties, compared with the coherence distance. The generated secret key can be used as either a one-time pad key, or a secret key for existing symmetric-key encryption such as AES.

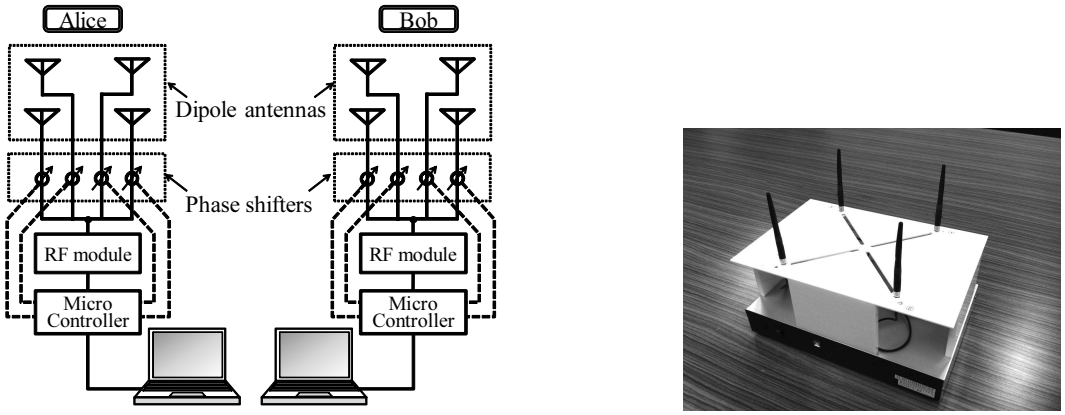
To study the feasibility of the wireless secret key agreement, we developed an experimental system using array antennas and conducted indoor experiments. In this paper, we present the experimental system and experimentally validate the reciprocity and position dependence of radio propagation characteristics.

2 Experimental System for Wireless Secret Key Agreement Using Array Antennas

We developed an experimental system for wireless secret key agreement using array antennas. Our experimental system consists of two stations named Alice and Bob, respectively. The block diagram of the experimental system and the snapshot of an experimental equipment are shown in Fig. 1. A ZigBee chip compliant with IEEE 802.15.4 standard is used as the communication device of each station. The frequency band used in the ZigBee chip is 2.4 GHz ISM band. The two stations have 4-elements square array antennas each. Each antenna element is connected with a phase shifter, and the phase shift of each antenna can be set from 0 rad to 2π rad. By setting the phase shift of each antenna at random, we can randomly change the antenna pattern, which results in random signal fluctuation at a receiver. The antenna spacing can be set from 6.25 cm to 18.75 cm, which corresponds to from $0.5\lambda_0$ to $1.5\lambda_0$ for the wavelength $\lambda_0 = 12.50$ cm of 2.4 GHz carrier frequency.

In this system, Alice and Bob communicate with each other at the same carrier frequency based on time division duplex (TDD). Alice and Bob transmit a probe packet and measure a received signal strength indicator (RSSI) of the packet alternately, and they iterate this process by randomly changing the phase shift of each antenna. The measured RSSI values are binarized to generate a secret key [2].

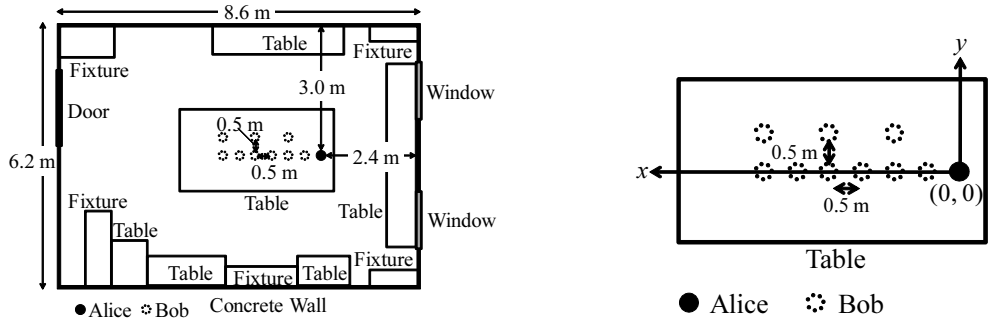
978-1-4244-6051-9/11/$26.00



(a) Block diagram of experimental system

(b) Snapshot of experimental equipment

Figure 1: Experimental system for wireless secret key agreement using array antennas.



(a) Sketch of experimental room

(b) Positions of Alice and Bob

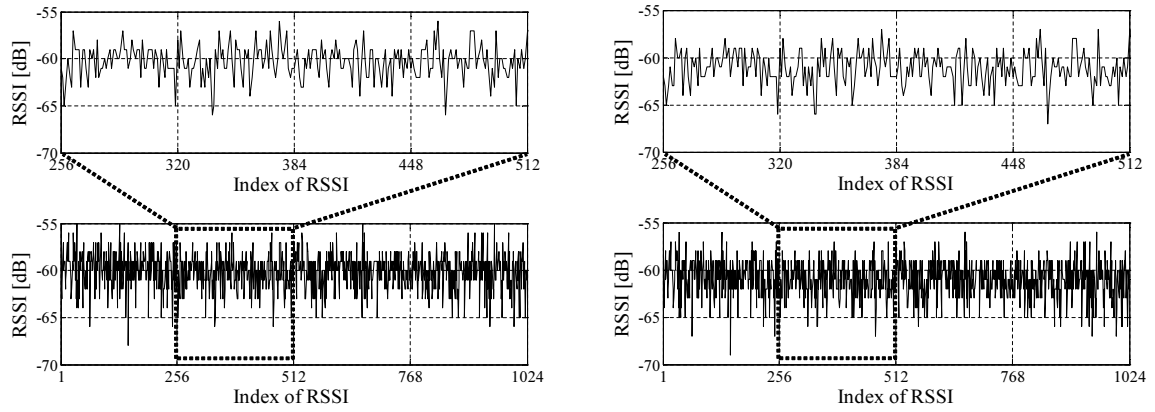
Figure 2: Sketch of experimental room and positions of Alice and Bob.

We conducted indoor experiments with the developed experimental system. A sketch of the experimental room is shown in Fig. 2. Alice and Bob were placed on the table located at the center of the room. Alice was fixed on the edge of the table, and Bob was placed at one of the points on the table as shown in Fig. 2(b). Throughout the experiments, the carrier frequency was set to 2.4 GHz, and the antenna spacing was set to 12.50 cm, which corresponds to the wavelength of 2.4 GHz carrier frequency. We measured 1024 samples of RSSI values for various positions of Bob. We randomly selected 1024 values from 0 to 2π for the phase shift of each antenna, and the same values were used at each position of Bob. The median of RSSI values is used as the threshold of binarization.

3 Experimental Results

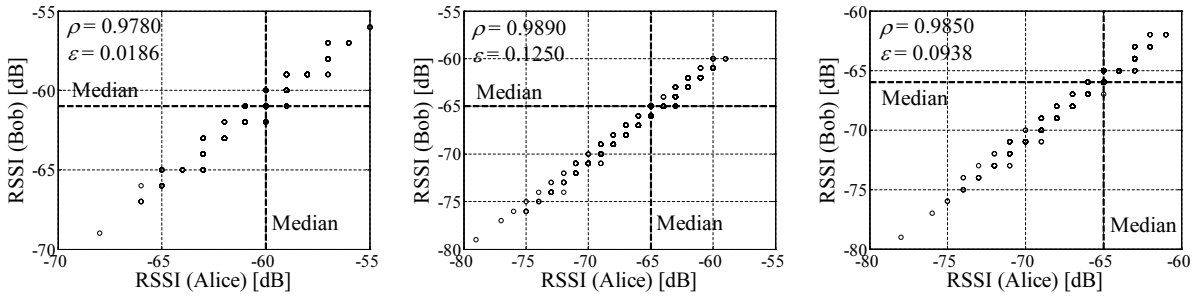
We conducted two types of experiments to validate basic characteristics that are fundamental for the wireless secret key agreement: the reciprocity and position dependence of radio propagation characteristics.

In the first experiment, we examined the reciprocity of radio propagation characteristics. Figure 3 shows the measured RSSI profiles of Alice and Bob, where Bob was placed at (1.0 m, 0.0 m). The measured RSSI profiles show significant changes due to the random antenna pattern, and the fluctuations of the two RSSI profiles are matched thanks to the reciprocal property. Figure 4 shows the scatter plots of the measured RSSI profiles of Alice and Bob for various locations of Bob. In this figure, the correlation coefficient of the



(a) RSSI profile of Alice (b) RSSI profile of Bob

Figure 3: RSSI profiles of Alice and Bob, where Bob was placed at (1.0 m, 0.0 m).

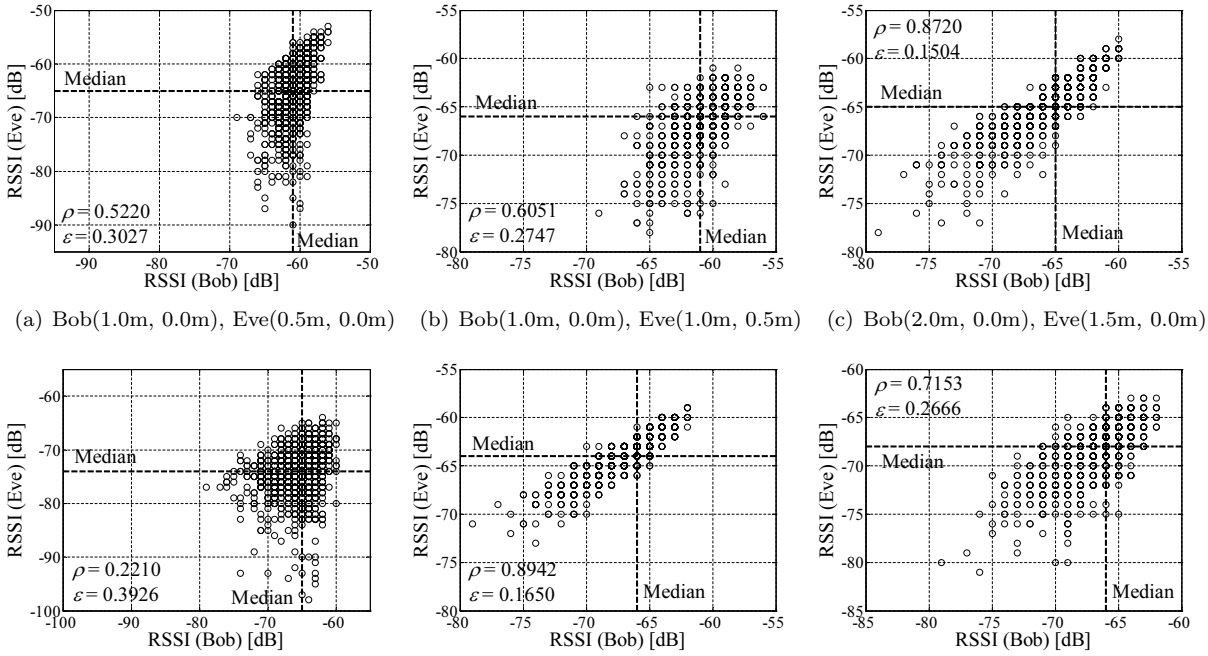


(a) Bob(1.0 m, 0.0 m) (b) Bob(2.0 m, 0.0 m) (c) Bob(3.0 m, 0.0 m)

Figure 4: Scatter plots of measured RSSI values of Alice and Bob.

RSSI profiles of Alice and Bob, denoted by ρ, and the bit disagreement rate of the generated secret keys of Alice and Bob, denoted by ε, are also indicated for each scatter plot. This result shows that the measured RSSI profiles of Alice and Bob are highly correlated, and the reciprocal property of radio propagation characteristics reasonably holds. Therefore, the bit disagreement rate is reasonably low. The discrepancy of the secret keys between Alice and Bob are corrected by applying error correcting techniques [2, 4].

In the second experiment, we examined the position dependence of radio propagation characteristics. In this experiment, Bob and an eavesdropper named Eve, who tries to estimate the secret key of the legitimate parties by eavesdropping Alice's packets, were placed at one of the dotted circles in Fig. 2(b), respectively. Then, Alice transmits packets with the random phase shifts of the array antennas, and Bob and Eve measure the RSSI values of Alice's packets. We assume that Eve knows the phase shifts of the array antennas of Bob and uses them in the same order of Bob, and therefore this situation is advantageous to Eve. Figure 5 shows the scatter plots of the measured RSSI profiles of Bob and Eve for various locations of Bob and Eve. In this figure, the correlation coefficient of the RSSI profiles of Bob and Eve, denoted by ρ, and the bit disagreement rate of the generated secret keys of Bob and Eve, denoted by ε, are also indicated for each scatter plot. It can be seen from this result that the correlation coefficient is high if Eve is located at a position on the line between Alice and Bob, e.g., the cases of Figs. 5 (c), (e). This is because the strength of the direct wave is dominant in the RSSI profiles. To decrease the correlation, some security enhancement techniques such as selecting RSSI values [6] need to be applied to this system.



(a) Bob(1.0m, 0.0m), Eve(0.5m, 0.0m) (b) Bob(1.0m, 0.0m), Eve(1.0m, 0.5m) (c) Bob(2.0m, 0.0m), Eve(1.5m, 0.0m)

(d) Bob(2.0m, 0.0m), Eve(2.0m, 0.5m) (e) Bob(3.0m, 0.0m), Eve(2.5m, 0.0m) (f) Bob(3.0m, 0.0m), Eve(3.0m, 0.5m)

Figure 5: Scatter plots of measured RSSI values of Bob and Eve.

4 Conclusion

We have shown a developed experimental system for wireless secret key agreement using array antennas. With the experimental system, we have validated basic characteristics that are fundamental for wireless secret key agreement: the reciprocity and position dependence of radio propagation characteristics. As the results of indoor experiments, it has been shown that the reciprocal property reasonably holds, whereas the position dependence does not always hold in the developed system.

References

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

[2] 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 Trans. Antennas Propag.*, vol. 53, no. 11, pp. 3776–3784, Nov. 2005.

[3] R. Wilson, D. Tse, and R. Scholtz, "Channel identification: secret sharing using reciprocity in UWB channels," *IEEE Trans. Inf. Forens. Security*, vol. 2, no. 3, pp. 364–375, Sept. 2007.

[4] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.

[5] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Trans. Inf. Forens. Security*, vol. 5, no. 2, pp. 240–254, June 2010.

[6] T. Shimizu, H. Iwai, and H. Sasaoka, "Improvement of key agreement scheme using ESPAR antenna," in *Proc. 2008 Int. Symp. Antennas Propag. (ISAP2008)*, Taipei, Taiwan, Oct. 2008, pp. 1–4.