Improvement of Key Agreement Scheme Using ESPAR Antenna

Takayuki Shimizu [1], Hisato Iwai [1], Hideichi Sasaoka [1],
[1] Department of Electronics, Doshisha University
Kyotanabe, Kyoto, 610-0321 Japan, {dth0172@mail4, iwai@mail, hsasaoka@mail}.doshisha.ac.jp

1. Introduction

Recently, secret key agreement schemes utilizing the characteristics of radio propagation have been proposed [1–3]. They are based on the reciprocity and the locality of the radio propagation characteristics. In particular, the secret key agreement scheme using an electronically steerable parasitic array radiator (ESPAR) antenna [4] is more effective for environments where the fluctuation of the radio propagation characteristics is slow such as indoor wireless LAN environments [2].

In the secret key agreement scheme using the ESPAR antenna, a secret key is generated based on a received signal strength indicator (RSSI) profile. However, in specific environments, there exist positions where the RSSI profiles of legitimate parties and an eavesdropper are highly correlated. Since the secret key is generated by the RSSI profile, the secret key of the legitimate parties might be estimated by the eavesdropper in the situation.

In this paper, we propose an improved key generation scheme in which appropriate RSSI values are selected to generate a key and also the carrier frequency to measure the RSSI is switched to enhance the security of the secret key agreement scheme.

2. Secret Key Agreement Scheme Using ESPAR Antenna

In this section, we describe the secret key agreement scheme using the ESPAR antenna [2]. The preconditions are set as follows. The legitimate parties are an access point (AP) equipped with the ESPAR antenna and a user terminal (UT) equipped with an omni-directional antenna. AP and UT can communicate at an identical frequency by using a method such as time division duplex (TDD).

Figure 1 shows the key generation procedure. Firstly, AP transmits one packet, then UT measures RSSI alternately, where the beam pattern of the ESPAR antenna of AP is fixed. Then, the beam pattern of the ESPAR antenna is switched randomly by changing the reactance values of the ESPAR antenna. This process is repeated until the sufficient length of RSSI profiles is obtained to generate the secret key. After making the RSSI profiles, they are binarized to generate key candidates, where the median of the RSSI profile is used as the threshold for the binalization. The generated raw key candidates, however, may contain some errors (discrepancy of the generated keys at the two legitimate parties) due to the noise and other effect at the receivers. To eliminate the errors, RSSIs around the threshold are removed. Furthermore, the remaining errors are corrected based on the syndromes of the key candidates by applying error correcting techniques. Thus, AP and UT can share an identical secret key.

3. Key Generation by Selecting RSSI

It has been clarified by means of ray-tracing analysis, in an indoor environment where there are no reflecting and scattering objects, the RSSI profiles of AP, UT and the eavesdropper are highly correlated if the eavesdropper is located at a position around the line between AP and UT. One of the causes is the effect of direct wave. If the directional gain for the direct wave is higher, the strength of the direct wave is dominant in both the RSSI of the legitimate party and that of the eavesdropper because the strength of the direct wave is substantially stronger than the reflected waves in the case. As a result, the dominance of the direct wave increases the correlation. In other words, the suppression of the influence of the direct wave decreases the correlation.

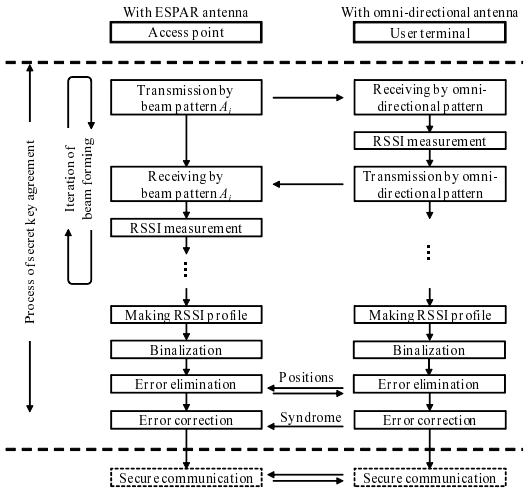


Figure 1: Key generation procedure

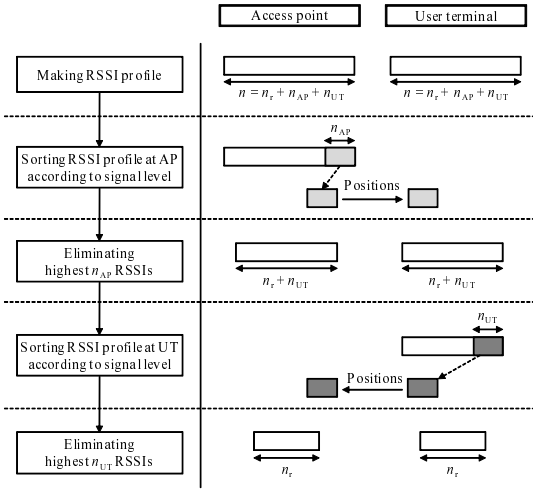


Figure 2: Procedure of selecting RSSI

To suppress the effect of the direct wave, we propose to select RSSIs to be used for the key according to the signal level of RSSI. In the proposed scheme, the higher RSSIs are eliminated before the binalization because they are mostly dominated by the strength of the direct wave. Figure 2 shows the procedure of selecting RSSI. Firstly, AP and UT measure RSSI profiles that is $n = n_r + n_{AP} + n_{UT}$ in length, where n_r, n_{AP} and n_{UT} denote the length of the RSSI profile after the elimination of the higher RSSIs, the numbers of the highest RSSIs to be eliminated at AP and UT, respectively. After that, AP sorts the RSSI profile according to the signal level, then eliminates the highest n_{AP} RSSIs. AP sends the eliminated positions to UT over a public channel, then UT eliminates the RSSIs at the identical positions to those at AP. Next, UT eliminates the highest n_{UT} RSSIs in the same way. AP also eliminates the identical positions to UT. The remaining RSSIs, which is more affected by the reflected waves, are used to generate the key as a new RSSI profile. By using the reflected waves primarily rather than the direct wave, the locality of the multipath fading is emphasized and the correlation can be improved.

In addition, we propose to switch the carrier frequency to further decrease the correlation. By switching the carrier frequency, positions where high correlation occurs are varied, so that the correlations of the positions are decreased. In the proposed scheme switching carrier frequency, the carrier frequency is switched every n_f RSSI measurements. Then, selecting RSSI is applied to each n_f RSSIs measured with an identical carrier frequency.

4. Simulation Result

4.1 Simulation Setting

A test equipment using ZigBee^{TM} [5], which conforms to IEEE802.15.4, of the secret key agreement scheme using ESPAR antenna have been developed [2]. Therefore, we carried out a numerical simulation assuming a model of IEEE802.15.4 to evaluate the performance of the proposed scheme.

Figure 3 shows the environment of the simulation. AP equipped with a 7-elements ESPAR antenna, UT equipped with an omni-directional antenna and the eavesdropper equipped with an omni-directional antenna are in the same room enclosed by concrete walls on four sides in which there are no reflecting and scattering objects. Throughout the simulation, the position of AP is fixed to the center of the room, (0.0 m, 0.0 m), and the position of UT is fixed to (3.0 m, 2.0 m). The eavesdropper is placed at 0.1 meters intervals all around the room as shown in Fig. 3, and tries to estimate the key of UT as a passive eavesdropper.

The parameters of the key generation are specified in Table 1. In the 2.4 GHz band of IEEE802.15.4, 16 channels is assigned in the spectrum, ranging from channel 11 (2.405 GHz) to channel 26 (2.480 GHz) with 5 MHz intervals from the center frequency of 2.405 GHz. In the proposed scheme without frequency switching (FS), the carrier frequency is fixed to 2.480 GHz. On the other hand, in the proposed scheme

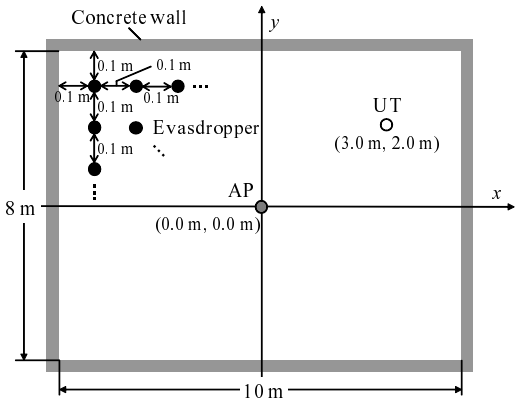
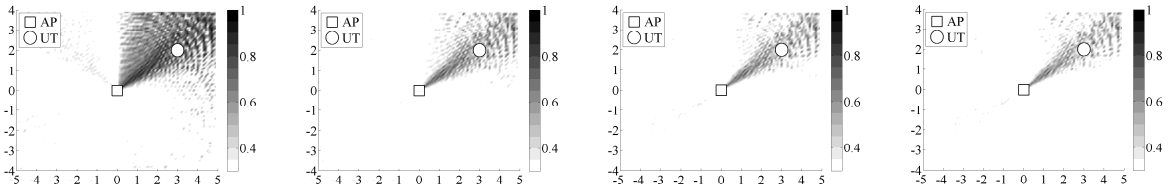


Figure 3: Simulation environment

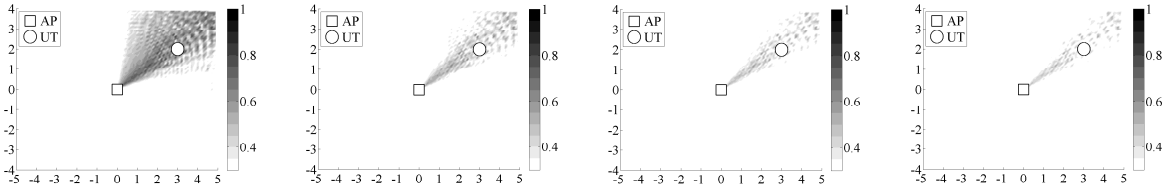
Table 1: Parameters of key generation

Carrier frequency	2.480 GHz (without FS) 2.405 – 2.480 GHz (with FS)
RSSI profile length	128, 256, 384, 512
Key length	128 bit
Channel model	Ray-tracing (Reflection: up to 6 times)
Reactance vector	Random



(a) $n = 128$ (b) $n = 256$ (c) $n = 384$ (d) $n = 512$

Figure 4: Correlation coefficient of RSSI profiles without frequency switching



(a) $n = 128$ (b) $n = 256$ (c) $n = 384$ (d) $n = 512$

Figure 5: Correlation coefficient of RSSI profiles with frequency switching

with FS, the carrier frequency is switched every $n_{\mathrm{f}} = n/16$ RSSI measurements to use up all 16 channels, where n denotes the total number of RSSI measurements. The resultant key length is fixed to 128 bits which corresponds to n_{r}, while the total number of RSSI measurements n is set to 128, 256, 384 and 512. In other words, the length of the RSSI profile after the is fixed to 128. The ray-tracing technique [6] is used to generate the propagation channel characteristics considering the effect of the reflections by the concrete walls. In the simulation of this paper, the effect of noise is ignored in order to focus on the discussion of the correlation due to the multipath. Since there is no effect of the noise, the elimination of the RSSIs around the median and the error correction in Fig. 1 are not performed.

4. 2 Correlation Coefficient of RSSI Profile

Figures 4 and 5 show the spatial distribution of the correlation coefficient between the RSSI profiles of UT and the eavesdropper in the room by the schemes without FS and with FS, respectively. In the conventional scheme, which corresponds to the scheme without FS and $n = 128$, positions along the line between AP and UT have the higher correlation coefficient due to the effect of the direct wave as shown in Fig. 4(a). Selecting RSSI by the proposed method decreases the correlation coefficient as shown in Fig. 4(b), (c) and (d). Furthermore, the correlation coefficient is more decreased by FS as shown in Fig. 5.

Figure 6 shows the complementary cumulative distribution function (CCDF) of the correlation co-

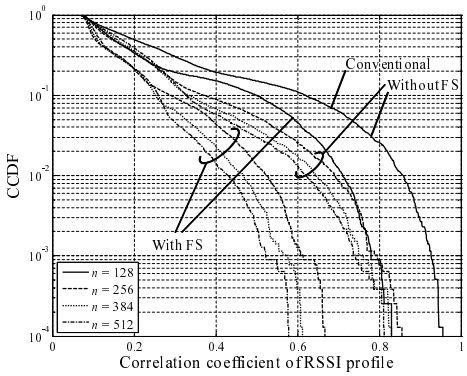


Figure 6: CCDF of the correlation coefficient

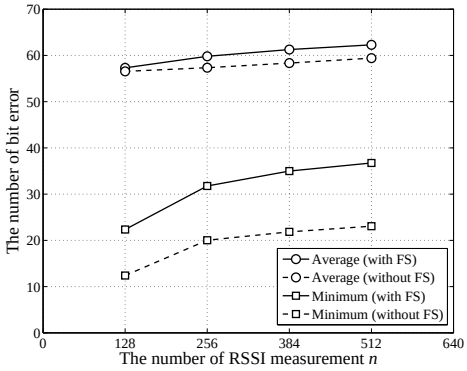


Figure 7: The number of the bit errors of key

efficient between the RSSI profiles of UT and the eavesdropper. The characteristics are obtained based on the spatial distribution of the correlation over the room as shown in Figs. 4 and 5. In the conventional scheme, there exist positions where the correlation coefficient are around 0.9 with the probability over 10^{-3}. By contrast, the correlation coefficient of the proposed scheme adopting FS with $n = 512$ is less than 0.6 at the highest.

4.3 Number of Bit Errors of Key

Figure 7 shows the number of the bit errors between the keys of UT and the eavesdropper, where the minimum and the average denote the minimum value and the average of the bit errors over all positions of the eavesdropper in the room, respectively. In the conventional scheme, the minimum number of the bit errors is approximately 12, which is not enough to ensure the security of the secret key agreement scheme. By contrast, the proposed scheme adopting FS with $n = 512$ realizes three times the minimum number of the bit errors of the conventional scheme.

5. Conclusions

We propose an improved key generation scheme for the secret key agreement scheme using the ESPAR antenna to enhance the security of the secret key agreement scheme. In the proposed scheme, RSSIs to be used to generate a key are selected in order to extract RSSIs more affected by the multipath. As the result of the simulation, the proposed scheme allows us to decrease the correlation between the RSSI profiles of the legitimate party and the eavesdropper, and increases the number of the bit errors at the eavesdropper.

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 and Propagation*, vol. 53, no. 11, pp. 3776–3784, Nov. 2005.

[3] Z. Li, W. Xu, R. Miller, and W. Trappe, “Securing wireless systems via lower layer enforcements,” in *Proc. 5th ACM Workshop on Wireless Security (WiSe’06)*, 2006, pp. 33–42.

[4] H. Kawakami and T. Ohira, “Electrically steerable passive array radiator (ESPAR) antennas,” *IEEE Antennas and Propagation Magazine*, vol. 47, no. 2, pp. 43–50, Apr. 2005.

[5] http://www.zigbee.org/.

[6] A. Goldsmith, *Wireless communications*. Cambridge University Press, 2005.