Improvement of Tolerance for Eavesdropping in Wireless Key Agreement Scheme Using ESPAR Antenna Based on Interference Transmission

Masahiro ONISHI, Takayasu KITANO, Hisato IWAI, and Hideichi SASAOKA
Graduate School of Engineering, Doshisha University, Tatara Miyakodani, 1-3, Kyotanabe, Kyoto, 610-0394, Japan
E-mail: {dti0161@mail4, eti1101@mail4, iwai@mail, hsasaoka@mail}.doshisha.ac.jp

1. Introduction

Eavesdropping in wireless communications have become one of serious issues as wireless communications have become rapidly and widely used. As one of the countermeasures, a secret key agreement scheme based on radio propagation characteristics have been studied [1-2]. The scheme realizes key sharing without delivery nor pre-assignment of a secret key which has been a subject of the shared key encryption scheme. However, in environments where the fluctuation of the propagation characteristics is small such as an indoor environment, since the scheme generates a shared key utilizing the variation of the propagation characteristics, the generated key becomes simple and it can easily be deciphered by the third parties such as eavesdroppers. In order to solve the problem, a key agreement scheme using ESPAR (Electrically Steerable Parasitic Array Radiator) antenna [3] was proposed [2]. In the scheme, RSSI (Received Signal Strength Indicator) sequences having a large variation can be generated even in a static situation where the temporal variation of the propagation characteristics is slow and small. It has however been reported that, even using the scheme, there exist some locations where the correlation of the RSSI sequences between the legitimate stations and the eavesdropper is considerably high [4]. It is particularly serious when the environment has less reflecting and scattering objects such as fixture. If the eavesdropper is located at such locations, the shared key of the two legitimate stations may be stolen and the secret communication is impossible. To improve the tolerance for the eavesdropping, a modified method is proposed where RSSI values are selected according to the signal level [4].

In this paper, we propose a new countermeasure to reduce the high correlation of the RSSI sequences. A secret communication system equipped with multiple auxiliary antennas transmitting interference signals has been proposed [5]. We apply the principle of the system to the key agreement. In the proposed key agreement scheme, additional interference signals are simultaneously transmitted from the auxiliary antennas at legitimate AP (Access Point). The transmission from the multiple antennas is controlled to cancel the interference at the location of the legitimate UT (User Terminal) by weighting the transmission signals. The interference transmission decreases the correlation of the RSSI sequences between the legitimate stations and the eavesdropper (TP : Tapping Point). In this paper, the configuration of the proposed system is presented. Also the performance of the proposed scheme is quantitatively evaluated through computer simulations.

2. Secret key agreement scheme using ESPAR antenna

In this chapter, the principle of the existing secret key agreement scheme using an ESPAR antenna [2] is presented. Here we assume the channels between AP, UT and TP are multipath fading channel, AP is equipped with ESPAR antenna and UT and TP with an omni-directional. The procedure of the key generation of the scheme is schematically presented in Fig. 1. In the scheme, the transmission and the reception of the signal to measure RSSI are alternately done at AP and UT. During one turn of the transmission and the reception, the directional pattern of the ESPAR antenna is fixed. After one turn finishes, the directional pattern is electrically varied and new RSSI is measured at the both stations. The variation of the RSSI values are identical at the two stations owing to the reciprocity of the radio propagation whereas it is different at the other locations due to the small spatial correlation of the multipath fading if the location is apart from one of the two legitimate stations for more than half wavelength. It is the fundamental principle of the key agreement scheme based on radio propagation characteristics. If a key is generated based on the RSSI sequences, a common key can be shared at the both legitimate stations, while it cannot be estimated at TP. To obtain a digital key, the RSSI values are binarized by the median value of the RSSI distribution. The key may include some discrepancies generated by noise, measuring errors,

and the other factors. Therefore in usual cases information reconciliation process is required to eliminate the discrepancies. By the above procedure, a secret key can securely be shared without any transmission of the information of the key itself. The prototype system based on the scheme is developed to present the feasibility of the scheme [2]. The appearances of AP and UT of the prototype are shown in Fig. 2.

3. Proposed key agreement scheme using interference transmission

Figure 3 shows the simulated spatial distribution of the cross correlation coefficient of the RSSI sequences between UT and TP assuming the existing key agreement scheme using ESPAR antenna. The assumed environment is a rectangular room whose size is 8m x 10m. The detailed simulation assumptions are presented in the following chapter. It can be seen from the figure that there exist locations where the correlation is significantly high. The most of them are spread in the direction from AP to UT.

In order to eliminate the locations where the high correlation is observed, we consider a new scheme where, in addition to the ESPAR antenna, AP is equipped with additional multiple omni-directional antennas to transmit the interference to jam the monitor at TP. The interference signal is weighted by weighting factors at the transmission to cancel themselves each other at the reception of UT. At the other locations however the interference is not cancelled because the channel characteristics are different from those between AP and UT. Owing to the interference, the correlation of the RSSI sequences can be decreased. Figure 4 schematically shows the configuration of the proposed scheme. The signal to measure the RSSI values, $s_s(t)$, are transmitted from the ESPAR antenna while the interference signal, $s_i(t)$, is from n omni-directional antennas. The interference signals are transmitted only at AP's transmission timing and it is turned off at the reception of AP. Hereinafter, the noise is omitted to focus the discussion on the tolerance of the proposed scheme for eavesdropping.

In the proposed scheme, the signal to the k-th interference antenna is multiplied by a weighting factor w_k. Representing the channel between the ESPAR antenna and the UT antenna as h_0 and the channel between the k-th interference antenna and UT as h_k, the received signal at UT is expressed as

$$r(t) = h_0 \cdot s_s(t) + \sum_{k=1}^{n} (w_k \cdot h_k) \cdot s_i(t). \tag{1}$$

To avoid generating the interference to UT, the following condition must be satisfied.

$$\sum_{k=1}^{n} w_k \cdot h_k = 0. \tag{2}$$

At the position of TP, the receiving signal, $r_e(t)$, is expressed by the following expression.

$$r_e(t) = h_{e0} \cdot s_s(t) + \sum_{k=1}^{n} (w_k \cdot h_{ek}) \cdot s_i(t), \tag{3}$$

where h_{e0} represents the channel between the ESPAR antenna and TP and h_{ek} between the k-th interference antenna and TP, respectively. At TP, the following condition similar to Eq. (2) is not always satisfied and the interference signal jams the reception of the measuring signal.

$$\sum_{k=1}^{n} w_k \cdot h_{ek} = 0. \tag{4}$$

To satisfy Eq. (2), a variety of combinations of weighting factors can be assumed. However, by anyone of them, the locations where the RSSI correlations are considerably high other than the UT location cannot perfectly be removed due to the nature of the multipath fading. In a multipath fading environment, a very unique point exists where very deep fade is observed. The occurrence probability is very small but some small probability does exist. If the propagation path of TP is accidentally in such a situation, the jamming by the interference does not effectively work. To solve the problem, temporal variation of the weighting factors is adopted in this scheme. Here we consider the following weights.

$$w_k = (\alpha_1 - \alpha_n)\frac{1}{h} \quad (\text{for } k = 1), \qquad (\alpha_k - \alpha_{k-1})\frac{1}{h_k} \quad (\text{for } k > 1), \tag{5}$$

where α_ks are an arbitrary values. Substituting Eq. (5) into the left term of Eq. (2), we obtain

$$\sum_{k=1}^{n} w_k \cdot h_k = (\alpha_1 - \alpha_n)\frac{1}{h_1} h_1 + (\alpha_2 - \alpha_1)\frac{1}{h_2} h_2 + \cdots + (\alpha_n - \alpha_{n-1})\frac{1}{h_n} h_n = 0. \tag{6}$$

From the above derivation, we find the interference is cancelled at the location of UT even if α_ks are temporally varied. Even by changing α_ks temporally, and, as the results, changing w_ks temporally, the existence of the high RSSI correlation cannot be eliminated, but such positions can be temporally varied. It means the interference is spread over time. If the temporal variation of the weighting factors are done during the generation period of the key, the interference is equally given to all locations other than the location of UT. It eliminates the generation of the unique location where the high correlation of the RSSI sequences is observed.

Note that, to use the weights of Eq. (5), the channel between AP and UT must be known at the transmission of AP. So we assume the channel is estimated prior to measuring RSSI values.

4. Performance analysis of proposed system

To evaluate the performance of the proposed system, computer simulations are carried out assuming an indoor environment. The assumed room is shown in Fig. 5. As it is reported that the high correlation is observed particularly in environments having less obstacles, we assume an empty room as the worst case scenario to the key agreement. The positions of AP and UT are fixed while the position of TP is changed in the room to obtain the spatial distribution. The simulation parameters are summarized in Table 1. The channels between AP, UT and TP are calculated by 2-dimensional ray-tracing. To reduce the effect of the noise, averaging process over several RSSI values are adopted in this scheme. In the simulation, the averaging count is 32.

Figure 6 shows the spatial distribution of the RSSI correlation. In the figure, SIR, the measuring signal to the sum of the interference transmission power raito, is varied. In the calculation of Fig. 6, noise is not considered to focus on the correlation characteristics. Comparing Figs. 3 and 5, it is seen that the high RSSI correlation are reduced by the proposed system. To clearly show the improvement, Fig. 7 shows the cumulative distribution of the RSSI correlation between UT and TP. SIR is assumed 0dB in the proposed system. Using the conventional scheme, RSSI correlation more than 0.9 is observed with 10^{-3} location probability. On the other hand, at the same probability, the correlation becomes less than 0.3 when the proposed system is adopted.

In the evaluation of the above characteristics, the noise effect is omitted. To calculate the weighting factors of Eq. (5), the channel coefficients are required. In actual communication environments where the noise exists, the channel estimation is not perfectly done. If the estimated channel includes errors, the interference cancelling does not operate as expected and the key agreement performance between AP and UT is degraded. Figure 8 shows the key agreement ratio between AP and UT when SNR is varied. We assume TDD transmission between the two and the channel are estimated by transmitting a channel estimation signal from UT to AP. Here we define SNR as the ratio of the channel estimation signal power to the noise power at AP reception. In the figure, two cases of the proposed scheme, with and without the averaging process (32 counts), are assumed. It can be seen from the figure that the influence of the noise is significant in the proposed system. It indicates the estimation accuracy of the channel greatly affects the key agreement performance. However, the degradation is overcome when the averaging is adopted. The averaging operation is actually implemented in the prototype system shown in Fig. 2, so the proposed system is feasible in actual communication systems.

5. Conclusion

A technical subject in the key agreement scheme using ESPAR antenna is discussed in the paper. In the scheme, there exist some locations where high RSSI correlation is observed. To resolve the problem, a new scheme utilizing the interference transmission from multiple auxiliary antennas is proposed. By quantitative analysis via computer simulations, it is shown that the high correlation can be reduced by the proposed system. Although there is a possibility that the key agreement performance between legitimate stations deteriorates since the proposed scheme utilizes the unnecessary interference transmission, it can successfully be overcome by adopting appropriate SNR improvement techniques such as the averaging.

References

[1] J.E. Hershey, et al., IEEE Trans. Commun., vol.43, no.1 pp.3-6, Jan. 1995.
[2] T. Aono, et al., IEEE Trans. Antennas and Propagation, vol.53, no.11, p.3776-3748, Nov. 2005.
[3] H. Kawakami, et.al., IEEE Antennas and Propagation Magazine, vol. 47, no. 2, pp.43-50,Apr. 2005.
[4] T. Shimizu, et al., Proc. ISAP2008, TP-A03, 1644987, Oct. 2008.
[5] X. Tang, et.al., Proc. ISIT2008, pp.389-393, July. 2008.

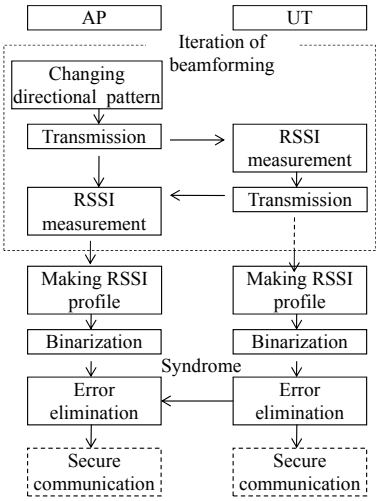

Fig. 1 Procedure of key agreement scheme using ESAPR antenna.

Table 1 Simulation parameters.

Propagation model	2-dimensional ray tracing
Material of wall	Concrete
Antenna	AP:7-element ESPAR (RSSI measurement) and Omni (interference), UT and TP: Omni
Carrier frequency	2.48GHz
Key length	128bit

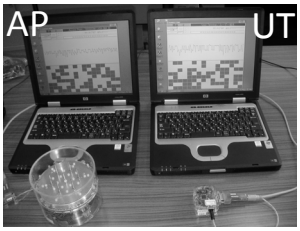

Fig. 2 Prototype system.

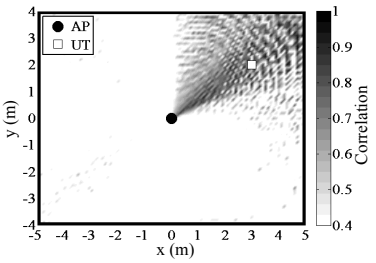

Fig. 3 Spatial distribution of RSSI correlation in existing scheme.

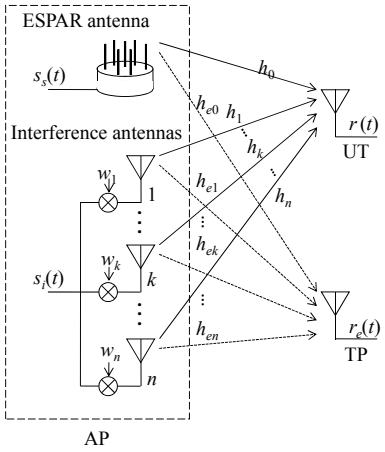

Fig. 4 Configuration of proposed system.

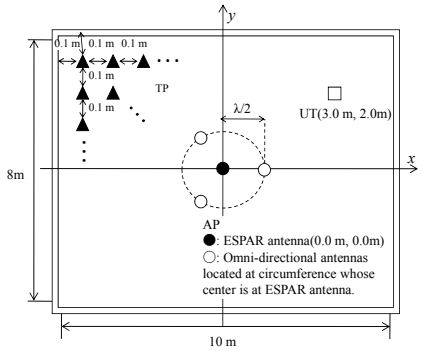

Fig. 5 Simulation environment.

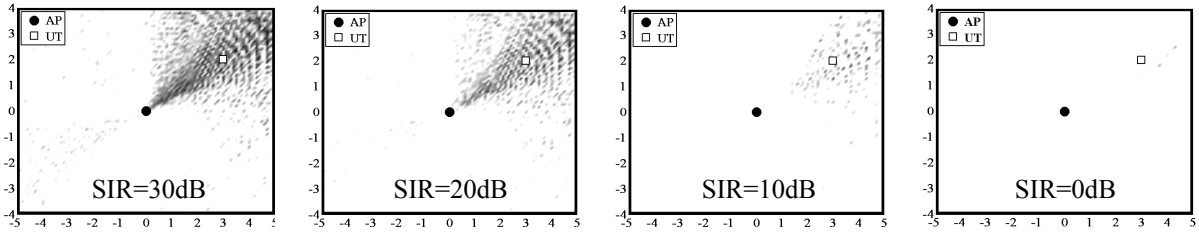

Fig. 6 Spatial distribution of RSSI correlation using proposed system.

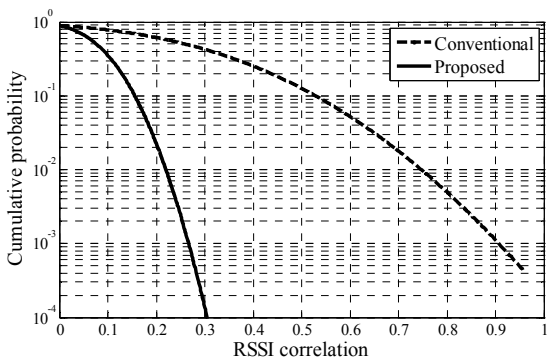

Fig. 7 Cumulative distribution of RSSI correlation.

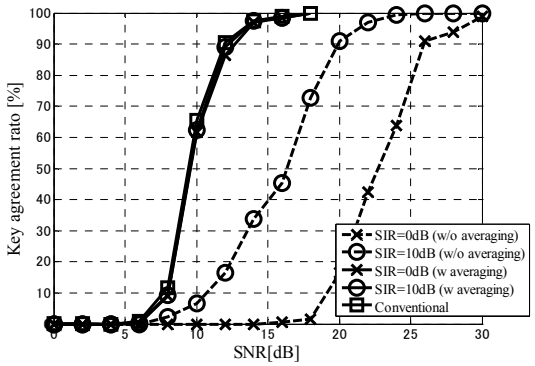

Fig. 8 Key agreement ratio between AP and UT.