Evaluation of Tolerance of Eavesdropping of Wireless Secret Key Agreement Using Array Antennas by FDTD Method

Akira Nishida, Takayuki Shimizu, Hisato Iwai, and Hideichi Sasaoka
Graduate School of Engineering, Doshisha University
Tatara, Miyakodani, 1-3, Kyotanabe, Kyoto, 610-0394, Japan
E-mail: {dtl0157@mail4, etj1101@mail4, iwai@mail, hsasaoka@mail}.doshisha.ac.jp

Abstract
A key agreement scheme using radio propagation characteristics is proposed as a new wireless security technique. The performance has been analysed primarily by Ray-tracing. For more effective analysis, we propose to adopt FDTD. As an example, we show the evaluated results of spatial correlation of RSSI sequences.

Keywords: FDTD Propagation analysis Secret key agreement Ray-tracing

1. Introduction

In recent years, a secret key agreement based on radio propagation characteristics has been studied as a way to ensure security of wireless communication [1]. The method enables us to generate and share a secret key without distributing actual keys, by using the unique properties of a wireless channel the reciprocity and the position dependence of radio propagation characteristics. One known problem of the method is that in environments where the fluctuation of the propagation characteristics is small such as an indoor environment, the generated key becomes simple and it can be easily deciphered by the third parties such as eavesdroppers. To solve the problem, the key agreement schemes using beam-steerable antennas such as an ESPAR (Electrically Steerable Parasitic Array Radiator) antenna [2] and array antennas [3] have been proposed.

In the performance analysis of the wireless key agreement schemes such as the tolerance characteristics against eavesdropping, the positions of access point (AP) and user terminal (UT) are generally fixed in certain locations and more general spatial characteristics where the stations are located at various points were not evaluated, since the Ray-tracing method is used in the analysis. Ray-tracing is a method to calculate path characteristics such as path gain and phase rotation by using simple geometrical assumptions. Although by the method propagation characteristics can easily be obtained in relatively simple environments, it requires a heavy calculation load to realize the estimation with high accuracy in more complicated situations such as actual indoor rooms or outdoor environments. Moreover the calculated propagation path in Ray-tracing is between specific transmitting and receiving points. In order to obtain spatial characteristics in a certain area, the calculation of tracing rays must be repeated and it requires significant computational load proportional to the number of the receiving points. Therefore, we can say Ray-tracing is not well-suited to the detailed analysis where more general spatial characteristics are considered. For this analysis, finite difference time domain (FDTD) method is more useful, since by the method detailed spatial characteristics can be calculated at once, although it needs considerably large amount of computational power and memory for a single calculation.

In this paper, in order to present the effectiveness of the FDTD method to calculate the propagation characteristics in the wireless key agreement schemes, we evaluate the tolerance of eavesdropping of the wireless key agreement scheme using array antennas [3] as an example of such analysis.
2. Wireless Secret Key Agreement Using Array Antennas and Analysis of Tolerance for Eavesdropping

In this chapter, we present the procedure of the generation of the key candidate sequence using array antennas. Also, the system model to analyse the tolerance for eavesdropping is presented.

2.1 Secret key generation procedure by using array antennas

We assume two legitimate users communicate each other using the same frequency for both uplink and downlink transmission such as time division duplex (TDD) and the propagation channels between them are multipath fading channels.

The procedure of the key generation of the wireless key agreement using array antennas is presented in Fig. 1. In this method, the secret information to generate key is the variation of the received signal strength indicator (RSSI) of the propagation channel between the two radio stations. They use the information as a common and exclusive source to generate the secret keys. In the scheme, the transmission and reception of the signal to obtain an RSSI value are alternately done at AP and UT. We assume the two stations have array antennas and, to vary the antenna patterns, the phases of the transmitted and received signals are variable by the phase shifters inserted at the antennas’ feeding line. During one turn of the transmission and the reception, the patterns of the array antennas at both AP and UT are fixed. After finishing one turn, the antenna pattern is varied and new RSSI value is measured at both stations. They iterate this process by randomly changing the phase shift of each antenna to vary their antenna patterns and generate RSSI sequences. By binarizing their RSSI sequences, they generate their candidate sequences for the secret keys.

After the generation of the key candidates, they eliminate the discrepancy of key candidates to improve the key-sharing success rate. The elimination of the discrepancy is realized by error correction technique [4], error deletion technique [2] and so on.

2.2 System model for analysis of tolerance of eavesdropping

The system model assumed in this paper is shown in Fig. 2. We assume 4-element array systems at AP, UT and the eavesdropper called tapping point (TP). The propagation channel among them is assumed a multipath fading environment and AP and UT communicate with each other at the same frequency based on TDD. The antenna patterns of AP and UT are varied by changing the phase shift of each antenna randomly in the range from 0 to 2π (rad.). By the variation, random signal fluctuation at a receiver can be artificially obtained and the RSSI sequences are generated.

We assume TP also generates the RSSI sequences based on the propagation channel between AP and TP. As a prerequisite, we assume TP knows the phase shifts at UT and uses the same values to control the antenna pattern at TP. That is, TP has the identical antenna pattern to that of UT. Thus the evaluation is advantageous to TP, which is a usual assumption for security analysis. If the RSSI sequences of the two legitimate stations and TP are similar, the shared key of the two legitimate stations may be stolen and the secret communication is impossible. To evaluate the tolerance for eavesdropping, we calculate the cross correlation coefficient of the RSSI sequences between UT and TP.
3. Calculation of Spatial Distribution of RSSI Correlation by FDTD

In the past, propagation characteristics in the performance evaluation of the wireless key agreement have been analysed by the Ray-tracing technique. By the method, estimation of propagation characteristics of a path between two certain points can be done. Therefore, in order to obtain spatial distribution by Ray-tracing, it is necessary to calculate the propagation characteristics between every pair of transmission and reception points individually. Moreover, in a complicated environment such as actual indoor rooms having many objects, the amount of the calculation increases exponentially. On the other hand, FDTD is a method to obtain the direct solution of Maxwell's equations [5]. The method divides analysis area into a finite rectangular grid and calculates the whole space at once. Thus, it is useful to estimate the spatial propagation characteristics in more detail.

Here we show that the same characteristics can be obtained by FDTD and Ray-tracing. We evaluate the spatial distribution of the correlation of the RSSI sequences between UT and TP. The environmental model is shown in Fig. 3. Here we assume a simple empty room where the size is 10 m \times 8 m and the analysis is done in 2-dimensional plane. AP is located at the center of the room (0, 0) and UT is located at (3, 2). The location of TP is changed at every point with 0.01 m separation. We calculate the propagation characteristics in the environment by FDTD and Ray-tracing and obtain the cross correlation coefficient of the RSSI sequences between UT and TP for around 800,000 points in total. Parameters used in the both calculations are listed in Table 1. It should be noted that the calculation by Ray-tracing is done at point by point, while by FDTD the calculations are done at once.

<table>
<thead>
<tr>
<th>Calculation procedure</th>
<th>2-dimensional Ray-tracing (up to 6 reflections are considered), 2-dimensional FDTD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antenna</td>
<td>4-element square array antennas (antenna separation = 0.1 m)</td>
</tr>
<tr>
<td>Carrier frequency</td>
<td>2.4 GHz</td>
</tr>
<tr>
<td>Key length</td>
<td>128 bit</td>
</tr>
</tbody>
</table>

The spatial distributions of the RSSI correlation between UT and TP are shown in Fig. 4. Figures 4(a) and 4(b) show the spatial distributions using FDTD and Ray-tracing, respectively. By comparing them, it is seen that the both spatial correlations are completely the same. This result shows that the analysis by FDTD provides the identical propagation characteristics to that by Ray-tracing in this case.

By FDTD we can get the detailed spatial characteristics of the correlation by the calculation of huge number of receiving points, such as around 80,000 points, at once, while Ray-tracing requires the calculation to estimate those characteristics at point by point against such numerous receiving points.

Fig. 3 Environmental model.

Fig. 4 Spatial distribution of RSSI correlation (UT: (3,2)).
4. Statistical Evaluation of Spatial Distribution of Correlation

As stated in the previous chapter, by FDTD detailed spatial characteristics can easily be obtained in comparison with Ray-tracing. Therefore, we can effectively evaluate more general characteristics of the spatial distribution of the RSSI sequences between UT and TP for different points of the stations. Figures 5(a) and 5(b) show the spatial distribution of the correlation of the RSSI sequences by FDTD where UT is located at different positions from that in Fig. 4.

Here we show the correlation characteristics by FDTD where UT is located at every point of a reticular pattern with 0.5 m separation in the room (285 points). We use CDF (Cumulative Distribution Function) over the room to show the characteristics more quantitatively. Figure 6 shows CDF of the correlation over the room. In the figure, the light lines represent the CDF of the RSSI correlations for different positions of UT and the black line represents the average of them. The figure shows that when the value of the correlation of the RSSI sequences between UT and TP is 0, CDF are varied from 0.3 to 0.75 according to the difference of the positions of UT. However the average value of CDF over the whole room is around 0.5. As shown here, the average spatial characteristics over a wide area can easily and effectively be obtained by the FDTD analysis. It is beneficial to improve the wireless key agreement technique by numerical evaluations.

5. Summary

In this paper, we have presented that the FDTD method is effective for performance analysis of the wireless key agreement scheme. By the method, detailed spatial characteristics can easily be calculated and it contributes to obtain the average characteristics in a wide area effectively.

References