Estimation of Fading Characteristics Based on Multiple Observed Signals at Different Locations

Keisuke Inoue, Hisato Iwai, and Hideichi Sasaoka
Department of Electronics, Doshisha University
Kyotanabe, Kyoto, 610-0321 Japan, {dth0116@mail4, iwai@mail, hsasaoka@mail}.doshisha.ac.jp

1. Introduction

Wireless communications have become popular and are used in various environments such as outdoor, offices, homes, etc. As the use of the wireless communications becomes common, security issues have become one of the most important technical subjects. In order to realize secure communications, cryptographic techniques have been developed and are popularly used in various communication systems. Typical examples of the techniques are the common key scheme and the public key scheme. The common key scheme requires less processing resources therefore it is appropriate to be used in small wireless terminals. However, in the scheme, a problem lies in how to share a secret key avoiding eavesdrop of the key. On the other hand, the public key scheme does not require key sharing. But, in usual cases, it requires large amount of processing and it is not suitable for the wireless communications.

A new wireless security technique based on wireless propagation characteristics has been proposed in order to solve the problems [1,2]. It is based on the reversibility and the locality of the wireless propagation characteristics to generate a common encryption key sequence between two wireless stations without pre-assignment and sharing of the key. The generated key can be used to realize secure secret wireless communications.

The security performance of the technique has been analyzed in a viewpoint of encryption [3], however it has not been discussed from a viewpoint of radio propagation. The security of the technique relies on the fact that the received signal can not be estimated from a remote point where the distance from the target point of the estimation is larger than the correlation length of the multipath fading environment. However it may be possible if the eavesdropper uses a higher performance receiving system such as directional antennas or multiple antenna systems, etc.

In this paper, we therefore discuss the possibility to break the locality, i.e., to estimate the received signal at a distant location in a multipath fading environment. We attempt to estimate the received signal characteristics based on the observed signals at multiple different points at a certain distance from the target. The principle of the estimation technique is firstly introduced and the estimation performance of the technique is then evaluated quantitatively via computer simulations. Also the performance when the estimation parameters such as the distance between the observed and the estimated points are varied is analyzed. The mechanism of the estimation methods is clarified through the analysis assuming a simpler propagation model. In order to clarify the estimation performance in more practical environments, we also consider a noisy channel model. From the results of the analysis we conclude it is difficult to precisely estimate the received signal from remote multiple observation points.

2. Estimation of Channel Characteristics at Distant Receiving Point

2.1 System model

Figure 1 presents the estimation system model considered in this paper. Here we discuss a two-dimensional case as shown in the figure. Assuming N observation points are placed on a circle with equal separation angle and the target receiver where the signal is estimated is at the center of the circle. The radius of the circle is expressed by R and the azimuth angle of the n-th observation point, γ_n, is $2\pi n/N$ (n=0, …, N-1), where N is the number of the observation points. The position of

the n-th observation point is expressed by P_n and the received signal at P_n by Z_n. We assume the received signals at all Z_ns are detected at the ideally-simultaneous moment as the reception at the target.

2.2 Estimation scheme

The concept of the estimation scheme is presented in Fig. 2. We assume a hypothetical incident wave from the direction δ_m in the estimation, where m is a serial number of the hypothetical incident wave. When a plain wave is assumed, the signal at the target point is estimated from the received signal at P_n (=Z_n) as $Z_n\exp(-jkR\cos(\delta_m-\gamma_n))$, where k is the wavenumber. By taking the average over N observation points, the estimated received signal at the center, $\hat{X}_m$, is obtained by the following formula :

$$\hat{X}_m = \frac{1}{N}\sum_{n=0}^{N-1} Z_n \exp\left(-jkR\cos\left(\delta_m - \gamma_n\right)\right). \tag{1}$$

The process of Eq.(1) is similar to that in the interferometry to search a direction of arrival. As the angle δ_m, we assume $2\pi m/M$ (m=0, …, M-1), where M is the number of the hypothetical incident waves. When M is sufficiently large, there exist some δ_ms which are almost identical to the incident angle of one of the arriving waves. At the angles, the absolute value of $\hat{X}_m$ becomes large, while in the other angles it is small and can be neglected.

Finally, $\hat{X}_m$ is averaged over M to obtain the estimated received signal at the target, $\hat{X}$, expressed as the following formula considering it is composed of all multipath waves :

$$\hat{X} = \frac{1}{M}\sum_{m=0}^{M-1} \hat{X}_m . \tag{2}$$

In the encryption-key sharing scheme, it utilizes the fluctuation of the signal level and does not require the absolute level [1,2]. Therefore, in the next chapter on the quantitative analysis, we discuss $|\hat{X}|/|X|$ where X is the reference signal at the target point (=the actual signal).

3. Quantitative Analysis of Estimation Performance

In this chapter, we evaluate the performance of the estimation scheme presented in the previous chapter. It is analyzed via computer simulations assuming fading environments.

3.1 Performance evaluation in multipath model

To calculate Z_n and X, we assume a multipath model shown in Fig.3. We assume 5 plain arriving waves as multipath waves where the noise effect can be neglected. The received phase at the target of each wave is randomly given according to the uniform distribution in [0, 2π). To simplify the calculation, we assume the 5 multipath waves have the same amplitude. The directions of arrival of the 5 waves are also randomly selected in the range [0, 2π) with the uniform distribution. 100 independent trials are examined. The variation generated by the different trials can be understood as the variation due to the change of the fading environment.

Figures 4 and 5 show the actual and estimated signal variations in the simulation when the number of the observation points, N, is 20 and 40, respectively. In these figures, the radius of the observation circle R is 4λ, where λ is the wavelength of the radio wave. The bold lines in the figures indicate the ratio of the estimated signal level over the actual. It can be seen from the figure that when N=40 the variation at the target is successfully estimated while when N=20 it is not. From the two figures, it is seen that, when N is sufficiently large, the estimation scheme successfully works to obtain the signal fluctuation at the target point. We next attempt to clarify the dependence of the performance on the variation of the estimation parameters. For the purpose, it is required to quantify the accuracy of the estimation by any quantitative indicator. Here we adopt the cross correlation of the signal fluctuations of the estimated and the actual signals. For example, the correlation in Fig. 5 is almost 1 while it is small in Fig. 4. Figure 6 presents the correlation characteristics when N is changed. In the figure, R and M are 4λ and 1000, respectively. In this case, around 30 observation points are required for successful estimation. Figure 7 shows the correlation when R is varied. N is

fixed to 100 in the figure. From these figures, we expect there exists a relationship between the maximum of R and the minimum of N to achieve the estimation.

3.2 Analysis in a single wave model

It can be seen from Fig. 7 that, when R is less than around 15λ, the estimation is perfect, whereas, when it is over the value, the estimation suddenly and drastically degrades. To analyze such characteristics, we consider a simpler single wave model. In the model the received phase at the target and the direction of the arrival of the wave is randomly given according to the uniform distribution in [0, 2π). Figure 8 shows the estimated amplitude and phase of $\hat{X}$ when R is changed. In the figure, N and M are 100 and 1000 respectively. In this paper, since our objectives are to show the safety of the encryption-key sharing scheme, we assume the worst case scenario for the scheme and sufficiently large value of M (=1000). Figure 8 (b) shows the probability where the phase is correctly estimated. In our preliminary analysis, it was made clear that, in the single wave model, there are only two possibilities for the estimated phase, the correct phase and the perfectly opposite phase. Therefore we adopt the probability of the correct estimation to characterize the accuracy of the phase estimation. The figure shows the averaged amplitude decreases with the periodical variation as R increases. The estimation of the phase is always perfect as long as R is smaller than 15λ, whereas the probability decreases when R is larger than 15λ. From the analysis it is seen that the incorrect estimation of the phase leads to unsuccessful estimation of the received signal.

3.3 Estimation performance in a noisy channel

It can be seen from the comparison of Figs. 7 and 8 that the estimation performance depends only on the correctness of the phase estimation and not on the amplitude variation. However as presented in Fig. 8 (a), the magnitude of the estimated signal decreases as R increase. Also the large periodical variation characteristics are observed. Therefore in a practical environment it is expected that the estimation deteriorated when the noise effect is taken into account. Figure 9 shows the correlation when noise exists in the channel. In the figure, N and M are 100 and 1000. SNR, signal power to noise power ratio, is 0, 20 and 40dB. It can be seen from the figure that it is difficult to precisely estimate a signal even when multiple antennas are used where there exists noise.

4. Summary

In this paper, we discuss a technique to estimate the received signal at a certain distance from observation points in a multipath fading environment. It is presented that the estimation can be realized when the system parameters satisfies a certain conditions. But in a more practical environment where the noise effect exists, precise estimation is difficult even when a multiple antenna system is used. It shows the eavesdropping of the encryption-key generated by the key sharing scheme based on radio propagation characteristics is practically difficult.

5. Figures

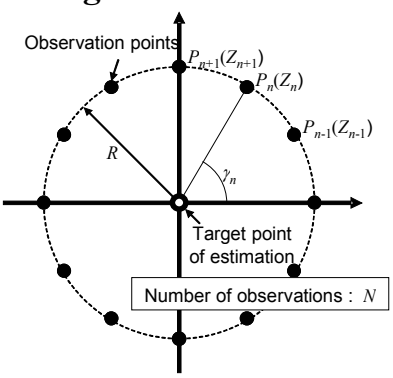


Fig.1 System model.

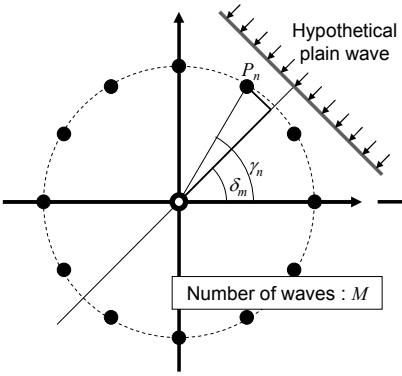


Fig.2 Estimation model.

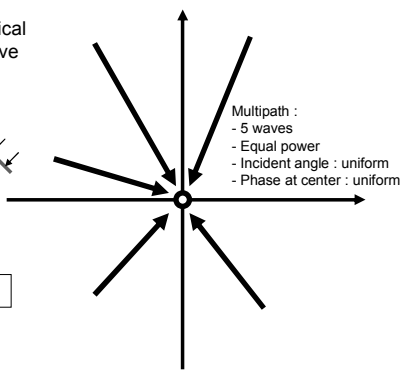


Fig.3 Multipath model.

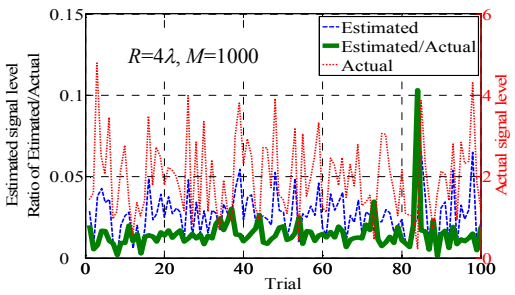


Fig.4 Actual and estimated signal variations. (N=20)

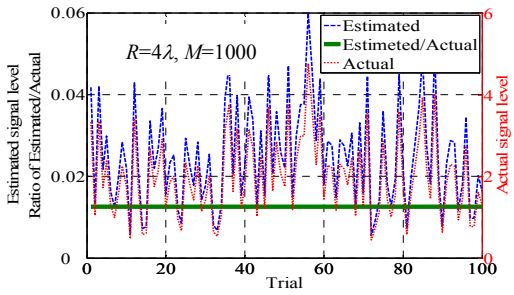


Fig.5 Actual and estimated signal variations. (N=40)

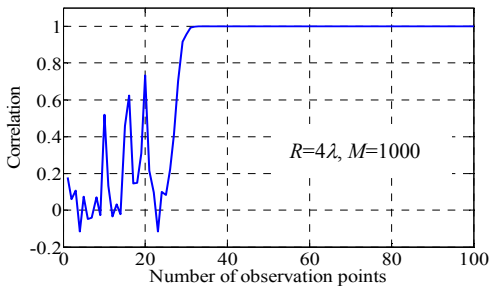


Fig.6 Correlation characteristics when number of observation points is changed.

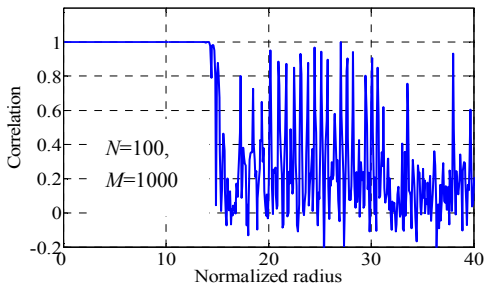
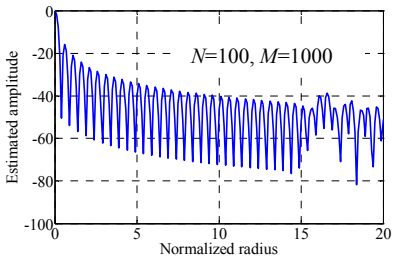
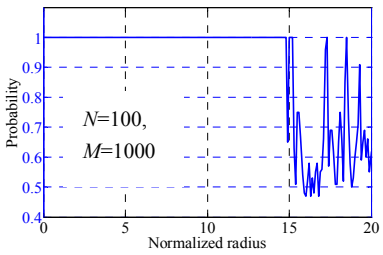


Fig.7 Correlation characteristics when radius of observation circle is changed.



(a) Amplitude



(b) Phase

Fig.8 Estimated amplitude and probability of correct estimation of phase.

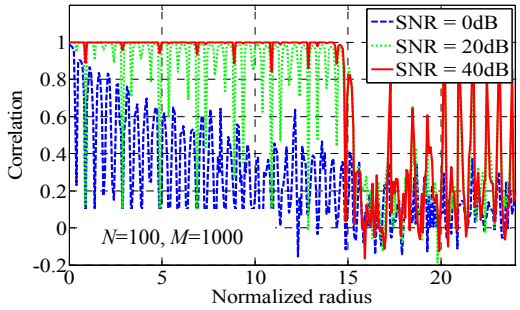


Fig.9 Correlation characteristics in a noisy channel.

References

[1] A. Kitaura, et.al., "A scheme of private key agreement based on the channel characteristic in OFDM land mobile radio", Electronics and Commun. in Japan, Part 3, Vol.88, 9, 2005.

[2] T. Aono, et.al., "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels", IEEE Trans. Antennas and Propagat., AP-53, 11, pp.3776-3784. 2005.

[3] H. Imai, et.al., "On the possibility of key agreement using variable directional antenna", The 1st. Joint Workshop on Information Security 2006, JWIS2006, Seoul, Korea, pp.153-167, Sep. 2006.