Position Dependence of Key Capacity in Secret Key Agreement Scheme Using ESPAR Antenna

Shunichi Kawamura, Takayuki Shimizu, Hisato Iwai, and Hideichi Sasaoka
Graduate School of Engineering, Doshisha University
Kyotanabe, Kyoto, 610-0321 Japan,
{dti0124@mail4, etj1101@mail4, iwai@mail, hsasaoka@mail}.doshisha.ac.jp

1. Introduction

As a way to ensure security on wireless communication, a secret key agreement scheme exploiting the unique properties of the wireless medium, the reciprocity of radio propagation and the irregularity of multipath fading, is being proposed [1-3]. The method enables two legitimate users to share a secret key without distributing the actual key, by using the radio propagation channel between the two as a common and exclusive source of randomness upon which a secret key could be derived.

As an application of this scheme to environments where the radio propagation characteristics are static, a method employing a variable directivity antenna called the ESPAR antenna [4] has been known to be effective. In this method, secret keys are generated from received signal strength indicator (RSSI) sequences of legitimate users. One known problem of this method is that in environments with simple radio propagation characteristics such as a rectangular room of concrete with no fixtures, the strength of the direct wave becomes the dominant factor affecting the fluctuation of the RSSI, thus increasing the chance for eavesdroppers located near the path of such waves to estimate the secret key.

Since all previous considerations of the aforementioned scheme has been done with environments where the legitimate users are in line-of-sight, this paper aims to illustrate how the location of eavesdroppers affect the secrecy of keys generated with the scheme, in a radio propagation environment with no clearly dominant wave. The key capacity in respect to the position of the eavesdropper in such environment is shown using computer simulations.

2. Secret Key Agreement Scheme Using ESPAR Antenna

As a prerequisite, we assume the legitimate access point (AP) with an ESPAR antenna and the legitimate user terminal (UT) with an omni-directional antenna, which communicates with a method using the same frequency for both uplink and downlink transmission such as time division duplex (TDD).

The key agreement procedure is shown in Fig. 1. The procedure mainly consists of two phases, and in the first phase, the RSSI sequence is created. First, AP sets the directional pattern of the ESPAR antenna to a certain pattern. AP and UT then measure their RSSIs corresponding to this antenna pattern by sending measurement signals to each other. Next, AP changes its antenna pattern, and the two measure each other's RSSIs corresponding to this new pattern. This process is repeated until an RSSI sequence with sufficient length is obtained. The second phase is concerned with generating candidates for the secret key from the RSSI sequences and eliminating the discrepancy of the candidates so that AP and UT end up with the same key. As a first step in this phase, AP and UT binarize their RSSI sequences using the median value as a threshold to form candidates for the final secret key respectively. We must take notice here that while the reciprocity of radio propagation between AP and UT stays true, the RSSI sequences of the legitimate users are not necessarily identical due to various factors such as measurement deviation and noise, and keys derived from those RSSI subsequently have the possibility of disagreement. To eliminate this disagreement, techniques like deleting data close to the threshold, which are likely to cause errors, and estimating the mismatched bits using error correction codes have been demonstrated [2]. The

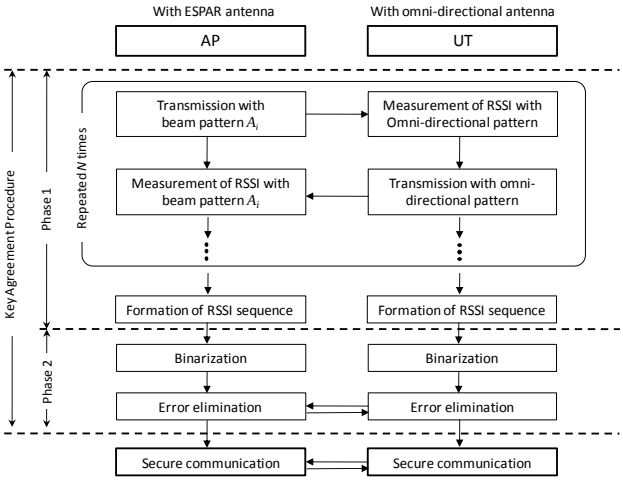

Fig. 1 Key agreement procedure.

secret key agreement procedure is completed by agreeing AP and UT's keys with such methods.

3. Secret Key Capacity

As an indication for the secrecy of shared keys, the secret key capacity is used. The definition of the secret key capacity is as follows. First, we consider Alice and Bob who can communicate through a public channel, and Eve who can passively wire-tap all of Alice and Bob's communications through the public channel. Alice and Bob have quantized keys with some correlation to each other, X and Y, respectively, and Eve has a quantized key Z with some correlation to X and Y. The secret key capacity of X and Y with respect to Z, denoted $S(X;Y||Z)$, is the maximum rate in which Alice and Bob can agree upon a secret key S using the public channel, while keeping the rate at which Eve obtains information about S arbitrary small. Giving a theoretical expression to the key capacity is a problem yet to be solved, and it is expressed with an upper and a lower bound [5]

$$\min\big(I(X;Y|Z), I(X;Y)\big) \geq S(X;Y||Z) \geq \max\big(I(X;Y) - I(X;Z), I(X;Y) - I(Y;Z)\big).$$

Under the condition $X = Y$,

$$S(X;Y||Z) = I(X;Y|Z),$$

and the key capacity becomes equal to the conditional mutual information of X and Y with respect to Z.

4. Simulation System

4.1 System Model

As a model for wireless communication, we consider a network consisting of three wireless terminals; AP, the access point with an 7-element ESPAR antenna, UT, a legitimate user terminal with omni-directional antenna and TP, an eavesdropper having a terminal capable of equal performance as UT with an omni-directional antenna.

4.2 Environmental Model

For the environmental model, we consider a case where l scatterers are located with an equal interval throughout the perimeter of a circle with a radius of 10m as shown in Fig. 2. The polar coordinate of the i-th scatterer (r, θ_i) can be described as

$$(r, \theta_i) = \left(10, \frac{2\pi}{l}(i-1) + \frac{\pi}{2}\right),$$

where θ_i denotes the angle of the i-th scatterer. AP is located at the center of the circle (0.0m, 0.0m)

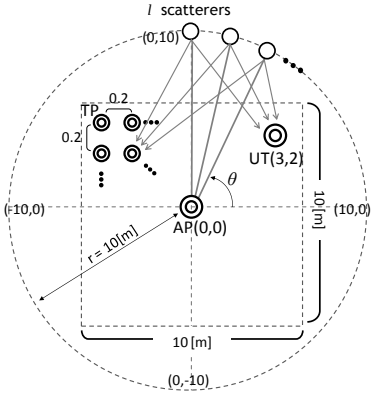

Fig. 2 Environmental model.

Table 1 Simulation parameters.

Carrier frequency	2.484 GHz
Propagation model	Scatterer model Considering distance decay and phase shift
Reactance vector of ESPAR antenna	Random
Key length	10^4 bit

and UT at (3.0m, 2.0m). TP is arranged in a reticular pattern with each position 0.2m apart from each other, inside a 10m by 10m square with AP being in the middle. The key capacity of the legitimate users in respect to every position of TP is calculated. In this model, we suppose radio waves from a transmission point are scattered to all directions by each scatterer once and reach the receiving point. Direct waves and multiple scattering are not taken into account. In other words, in the case of l scatterers, there exist exactly l multipaths between AP and any given position of UT/TP, in which waves are always transmitted from or received by AP with an angular interval of $2\pi/l$. Moreover, only distance decay and phase shift is considered for each path, and attenuation caused by scatterers is not considered, which means the reflection coefficients are always a unit value for arbitrary direction of the incidence and the reflection. Parameters used in the simulation are listed in Table 1. On how antenna pattern of the 7-element ESPAR antenna is chosen, though it is reported that using multi-robed antenna patterns would increase the safety of the shared key [6], the reactance vector of the 6 varactors, which determines the antenna pattern, is set randomly. Finally, in order to focus the discussion on the evaluation of the secrecy of the key particularly against eavesdropping, noise is non-existent throughout the simulation, meaning the secret key of the legitimate users always match.

5. Simulation Results

The spatial distribution of the key capacity is shown in Fig. 3. The variable l stands for the number of the scatterers. From Figs. 3 (a) and (b), it could be observed that for a small number of l, the spatial distribution of the key capacity take on a distinctive symmetric pattern. By looking at Figs. 3 (a) through (f), as l increases, the number of the positions with low key capacity decreases and the spatial distribution of positions with low key capacity becomes closer to random, suggesting the eavesdroppers are less likely to estimate the secret key. However, by comparing Figs. 3 (e) and (f), the change in the number of positions with low key capacity has stopped. To clearly show the characteristics, the CDF (Cumulative Distribution Function) of the key capacity with different values l is shown in Fig. 4. It can be said from the figure that the number of positions with low key capacity decreases steadily from $l = 2$ to $l = 10$. Then, for the values of l greater than 10, the number of positions with low key capacity increases compared to the case of $l = 10$. The reason why the increase in the number of waves after $l = 10$ makes the key capacity to decrease, could be thought of as follows. For l greater than 10, the angular interval of the transmitting waves from AP to each scatterer becomes small, likely causing the adjacent paths to fall into the same peak of the ESPAR antenna's beam pattern. As a result, these adjacent waves together could be considered as a single composite wave. Since the strength of this pseudo-composite wave depends on the phase relation of each consisting wave, in some cases a composite wave with high strength should be formed. In such case, the composite wave acts similar to a dominant wave like the direct wave in line-of-sight environments, and causes the key capacity to decrease for certain positions. To emulate this situation, the case of $l = 10$ with each wave experiencing independent Rayleigh fading is plotted also in Fig. 4. From the figure, the CDF curve for l greater than 10 falls close to the case of $l = 10$ with Rayleigh fading , suggesting that the above assumption to be credible.

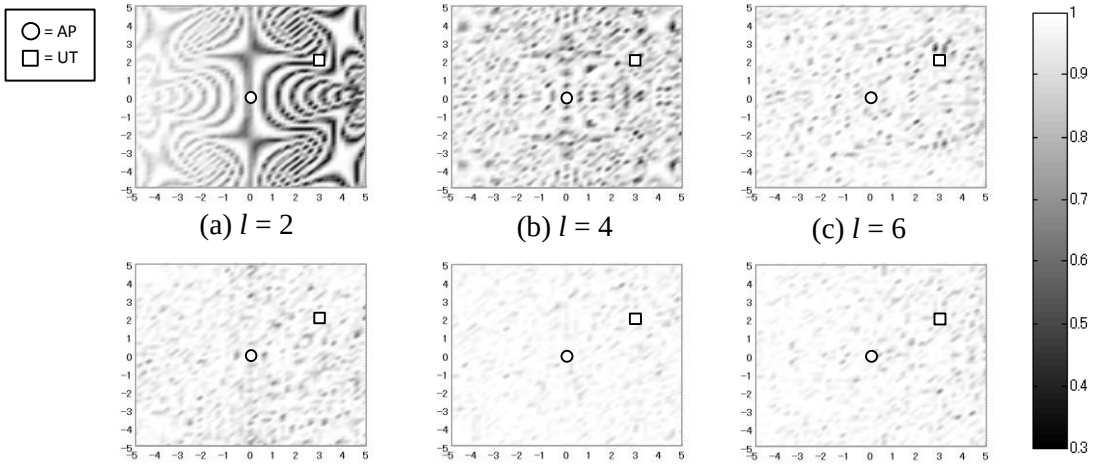

Fig. 3 Spatial distribution of key capacity.

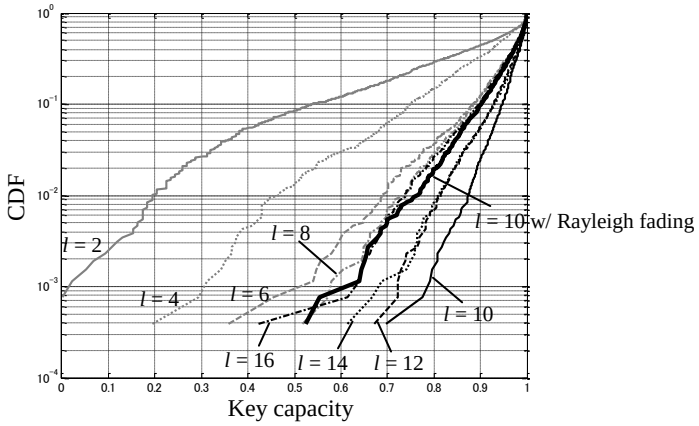

Fig. 4 CDF of key capacity.

6. Conclusion

Spatial distribution of the key capacity of keys generated with the secret key agreement scheme using ESPAR antenna in an environment with no dominant waves has been shown. From the simulation results, it has been suggested that a 7-element ESPAR antenna with its antenna pattern set randomly is capable of controlling 10 waves transmitted with an equal angular interval to increase the key capacity.

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. 47, no. 2, pp.43-50, Apr 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] Ueli M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Information Theory*, vol.39, no.3, pp. 733-742, May 1993.

[6] H. Mori, H. Sasaoka, T. Ohira, "A study for making optimal antenna pattern for making secret key based on space correlation of the strength of received signal," *IEICE Technical Report*, AP2003-188, pp.47-52, Nov. 2003. (in Japanese)