Impact of Direct-Path Wave on Imac in Secret Key Agreement System Using ESPAR Antennas

Tadafumi Yoshida, ***Takafumi Saito***, ***Katsuhiro Fujiki***, ***Kazumasa Uematsu***, ***Hideyuki Uehara***, and ***Takashi Ohira***

Toyohashi University of Technology, 1-1 Hibarigaoka Tenpaku-cho Toyohashi-shi, 441-8580, Japan
E-mail:{yoshida, saito, fujiki}@comm.ee.tut.ac.jp, {uehara, ohira}@tut.jp

Abstract

Current cryptography may be potentially decrypted by an extremely high performance computer. More secure key sharing schemes are expected. One possible solution is secret key agreement system which makes use of Electrically Steerable Parasitic Array Radiator (ESPAR) antenna. In this scheme ideally, by using wave propagation characteristics, eavesdropper cannot guess secret key from regular terminals. Actually however, eavesdropper has chances to guess the key if he is located on the line of direct-path wave between regular terminals. In our study, we evaluate the impact of direct-path wave on Information mutual anti-tapping condition (Imac) under a noisy channel.

1 Introduction

Wireless secret key agreement system, which uses reciprocity and location dependence of wave propagation, and radio wave fluctuation induced by ESPAR antenna, has been studied [1]. High anti-tapping tolerance is desired in this system. We had reported improvement of anti-tapping tolerance by eliminating direct-path wave under noiseless environment [2]. This paper uncovers impact of anti-tapping tolerance to eliminate direct-path wave under noisy environment.

2 Secret Key Agreement System Using ESPAR Antennas

We assume that secret key is generated in a room (8m × 10m), where regular terminal 1 (RT1) , regular terminal 2 (RT2), and eavesdropper (EV) are located. Regular terminal 1 and Regular terminal 2 have an ESPAR antenna, and eavesdropper has an omni-directional antenna. These assumptions are shown in Figure 1. Figure 2 shows how to generate and share a secret key in secret key agreement system using ESPAR antennas between RT1 and RT2. RT1 and RT2 select their antennas' directivity, respectively. RT1 and RT2 measure Received Signal Strength Indicator (RSSI) by sending and receiving radio wave each other. RSSIs measured by both regular terminals are equal if characteristic of channel and directivity are kept unchanged. Regular terminals memorize the measured RSSIs, and measure RSSI again after changing directivity, respectively. The memorized RSSI profile is binarized after repeating this process key length times. Because of location dependence of wave propagation, RSSI profile between regular terminals differs from that received at eavesdropper. Therefore eavesdropper cannot steal full information of the generated

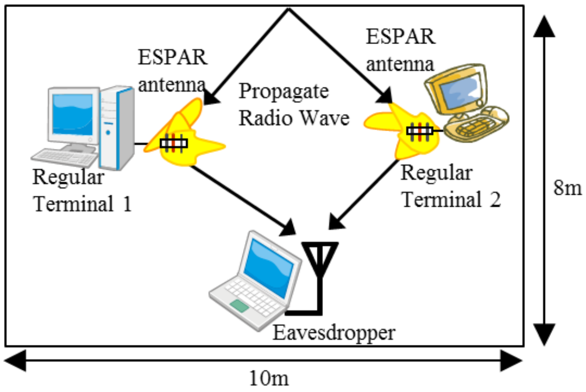

Figure 1: Assumed System Configuration in a Room

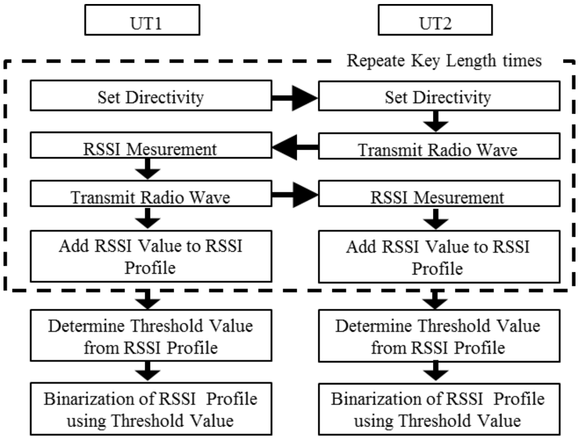
UT1
UT2
Repeate Key Length times
Set Directivity
Set Directivity
RSSI Mesurement
Transmit Radio Wave
Transmit Radio Wave
RSSI Mesurement
Add RSSI Value to RSSI Profile
Add RSSI Value to RSSI Profile
Determine Threshold Value from RSSI Profile
Determine Threshold Value from RSSI Profile
Binarization of RSSI Profile using Threshold Value
Binarization of RSSI Profile using Threshold Value

Figure 2: Key Sharing Procedure

978-1-4244-6051-9/11/$26.00 ©2011 IEEE

secret key between regular terminals, but eavesdropper can steal part of the secret key using received RSSI profiles.

3 ESPAR antenna

ESPAR antenna is variable directivity antenna which consists of one fed element and one or more parasitic elements [3, 4]. ESPAR antenna can change it's directivity to control the currents on fed and parasitic element using varactors. Figure 3 shows 3-element ESPAR antenna which has output impedance z_s and open voltage v_s for sending mode. ESPAR antenna's admittance matrix is expressed in Eq. (1). y_{00} is fed element self admittance, y_{01} and y_{10} are fed and parasitic element mutual admittance, y_{11} is parasitic mutual admittance. K is the number of parasitic elements.

$$\mathbf{Y} = y_{00}\mathbf{U_0} + y_{01}\big(\mathbf{P_0} + \mathbf{P_0}^T\big) + y_{11}\bar{\mathbf{U_0}} + \sum_{k=2}^{K} y_{1k}\bar{\mathbf{U_0}}\big(\mathbf{Q_{k-1}} + \mathbf{Q_{k-1}}^T\big)\bar{\mathbf{U_0}} \tag{1}$$

$$\mathbf{U_k} = \mathbf{diag}[\delta_k, \delta_{k-1}, \ldots, \delta_{k-K}], \quad \bar{\mathbf{U_k}} = \mathbf{I} - \mathbf{U_k} \tag{2}$$

$$\mathbf{P_k} = [0, u_k, \ldots, u_k], \quad \mathbf{Q_k} = [u_k, u_{k+1}, \ldots, u_{k+K}] \tag{3}$$

$$\mathbf{u_k} = [\delta_k, \delta_{k-1}, \ldots, \delta_{k-K}]^T, \quad \mathbf{0} = [0, \ldots, 0]^T \tag{4}$$

ESPAR antenna's directional array factor is expressed in Eq. (5). θ is elevation angle. ϕ is azimuth angle. λ is free space wavelength. Re indicates real part of a complex number. $\mathbf{X_{var}}$ is diagonal matrix made of reactance of varactors.

$$D\big(\theta, \phi\big) = a\big(\theta, \phi\big)^T \mathbf{w} \tag{5}$$

$$\mathbf{w} = 2r_s\tilde{\mathbf{Y}}u_0, \quad \mathrm{a}\big(\theta, \phi\big) = [1, e^{j\psi_1}, e^{j\psi_2}, \ldots, e^{j\psi_K}]^T \tag{6}$$

$$r_s = \mathrm{Re}(z_s), \quad \psi_k = \frac{2\pi d}{\lambda}\cos\theta\cos\Big(\phi - 2\frac{k-1}{K}\pi\Big) \tag{7}$$

$$\tilde{\mathbf{Y}} = \Big(\mathbf{Y}^{-1} + z_s\mathbf{U_0} + j\mathbf{X_{var}}\Big), \quad \mathbf{X_{var}} = \mathbf{diag}[0, x_1, x_2, \ldots, x_k] \tag{8}$$

4 Imac (Information mutual anti-tapping condition)

Under noisy environment, Signal Noise Ratio (SNR) degrades if we eliminate the direct-path wave. This leads to reduction of the amount of information that can be shared between regular terminals, as well as the amount of information stolen by eavesdropper. Imac can take into account these influences. Imac is defined in Eq. (10), and depicted region B in Figure 4. In Figure 4, the circle of region (A+B+D+E) has 1 bit information, and the other two circles have 1 bit information, respectively. We define probabilities p_1 to p_8 as shown in Table 1. In case of Table 1, Imac is expressed in Eq. (11) too.

Table 1: Combination of Key 1bit and Probabilities

Regular Terminal 1	0	0	0	1	0	1	1	1
Regular Terminal 2	0	0	1	0	1	0	1	1
Eavesdropper	0	1	0	0	1	1	0	1
Probabilities	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8

$$H(p) = -p\log_2(p) - (1-p)\log_2(1-p) \tag{9}$$

$$\mathrm{Imac} = \mathrm{H(RT1;EV)} - \mathrm{H(RT1|RT2,EV)} \tag{10}$$

$$\begin{aligned} \mathrm{Imac} = \quad & (p_1+p_3+p_4+p_7)H\Big((p_1+p_3)/(p_1+p_3+p_4+p_7)\Big) \\ & +(p_2+p_5+p_6+p_8)H\Big((p_2+p_5)/(p_2+p_5+p_6+p_8)\Big) \\ & -(p_1+p_3)H\Big(p_1/(p_1+p_3)\Big) - (p_2+p_5)H\Big(p_2/(p_2+p_5)\Big) \\ & -(p_4+p_7)H\Big(p_4/(p_4+p_7)\Big) - (p_6+p_8)H\Big(p_6/(p_6+p_8)\Big) \end{aligned} \tag{11}$$

5 Simulation

We compare Imac in the presence of and without direct-path wave. Specification of simulation is shown in Table 2. We assume that secret key is generated in a room (8m × 10m), where user terminals are located in a random way while eavesdropper is located at the middle point between them. A 2-dimensional ray tracing is applied. Secret keys are generated at 5000 points and Imac is calculated from 5000 sets of the secret key. Only regular terminals suffer from noise inside, while eavesdropper does not do.

Figure 5 shows the result of simulation. As the result, we confirm that Imac is successfully improved by 0.255 by eliminating the direct-path wave under an environment with transmission power to receiver noise ratio 140 dB. Under noisy environment with more than 80dB of transmission power to receiver noise ratio, anti-tapping tolerance is high when the direct-path wave is eliminated. This is because the decreasing amount of the stolen information by EV is bigger than that of the shared information between regular terminals. Under this environment, the share information between regular terminals is high. Under noisy environment with the range of transmission power to receiver noise ratio from 60dB to 80dB, anti-tapping tolerance is low when direct-path wave is eliminated. This is because the decreasing amount of the shared information between regular terminals is bigger than that of the stolen information by EV. Under this environment, the share information between regular terminals is low.

Table 2: Specification of Simulation

Room Size	10m× 8m
Characteristics of Wall	Concrete Relative Permittivity=6.76 Relative Permeability=1 Electrical Conductivity=0.023 S/m
Transmission Power To Receiver Noise Ratio	from 40 to 140dB
Regular User's Antenna	3-element ESPAR Antenna
Reactance Range	from -300Ω to 300Ω
Point for Regular user	Randomly
Eavesdropper's antenna	Omni-directional Antenna
Transmission Power	1W
Key Length	32bit
Key Generation Method	Binarization using Median
Key Generation Times Each Noise	5000 Times
Reflection Path Model	2-dimentional Ray Tracing
Reflection Times	Three Times
Poralization	Vertical

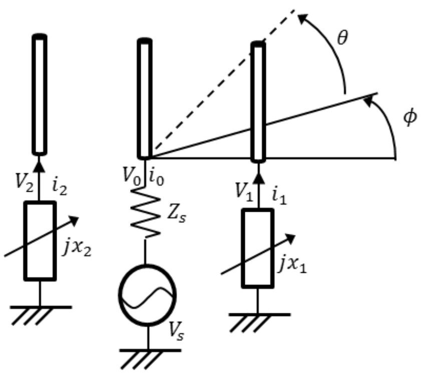

Figure 3: 3-element ESPAR antenna

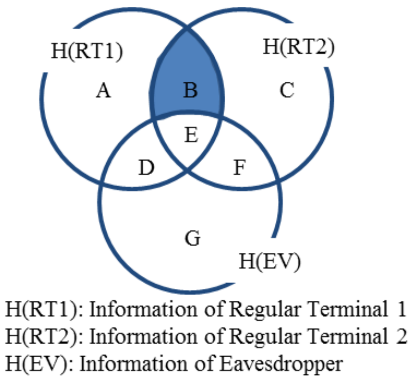
H(RT1)
H(RT2)
A
B
C
E
D
F
G
H(EV)
H(RT1): Information of Regular Terminal 1
H(RT2): Information of Regular Terminal 2
H(EV): Information of Eavesdropper

Figure 4: Graphical Definition of Imac

6 Conclusion

We have simulated the impact of direct-path wave under noisy environment in wireless key agreement system using ESPAR antennas. Under noisy environment, anti-tapping tolerance is improved by eliminating the direct-path wave more than transmission power to receiver noise ratio 85dB. Anti-tapping tolerance is decreased in the range of transmission power to receiver noise ratio from 60dB to 85dB.

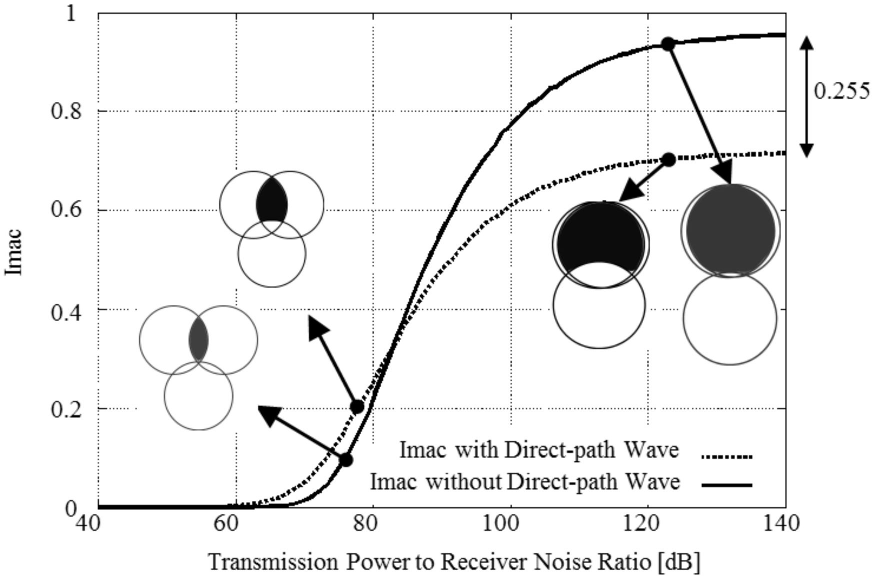

Figure 5: Simulated Imac for with and without the Direct-path Wave

References

1. Tomoyuki Aono, Keisuke Higuchi, Takashi Ohira, Bokuji Komiyama , and Hideichi Sasaoka, “Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels, ” IEEE Transaction on Antennas Propagation, vol. 53, no. 11, pp. 3776-3784, Nov. 2005.

2. Takafumi Saito, Kazumasa Uematsu, Taku Hasegawa, Hideyuki Uehara and Takashi Ohira, “A New Scheme for Anti-Tapping Tolerance Enhancement in Wireless Secret Key Generator Utilizing Horizontally-Polarized ESPAR Antennas, ” AP-RASC’10, Toyama, Japan, Sep. 2010.

3. Tskashi Ohira, Kyouichi Iigusa “Electronically Steerable Parasitic Array Radiator Antenna,” IEICE Trans. C, vol. J87-C, No. 1, pp. 12-31, Jan. 2004.

4. H. Kawakami and T. Ohira, ”Electronically steerable passive array radiator (ESPAR) antennas”, IEEE Antennas Propagation Magazine, 47, 2, pp.43-50. Apr. 2005.