# A Key Generation Technique Using Array Antenna Beam Selection

Satoru Aikawa, Masahiko Maeda and Tohru Iwai
Graduate School of Engineering, University of Hyogo,
2167, Shosha, Himeji-shi, Hyogo, 671-2280 Japan
E-mail: aikawa@eng.u-hyogo.ac.jp

## 1. Introduction

Recently, secret key generation schemes for wireless communication systems using propagation performance are researched. RSSI, signal strength indications received at AP (Access Point) and UT (User Terminal) are same value in TDD systems because of reciprocity theorem, and are controlled by the array antenna pattern. However, RSSI at TP (Tapping Point) is not same as RSSI at AP or UT that depend on their location.

The secret keys are generated from binarized RSSIs. This paper describes a method for improving the probability of key agreement between AT and UT by using array antennas control.

## 2. Proposed key generation technique

Binarized key bits of AP and UT generated from RSSIs near the binarizing threshold are easy to disagree. A ratio of key bits agreement is depending on the difference between RSSI and threshold value.

The RSSIs near the threshold are deleted to decrease the disagreement rate. Furthermore, Forward Error Correction Syndrome is used between the AP and UT. However, bit deleting schemes need additional bits than necessary key bit length.

We propose antenna pattern control to decrease the occurring probability of the RSSIs near the threshold. In this scheme, only the antenna patterns whose RSSIs are high or low value are selected for key generation.

## 3. System construction

AP and UT estimate DOA (Direction of Arrival) each other at first. Antenna patterns for main-beam or null to DOA are selected. Directions are controlled in AP and UT independently. The adaptive array antennas of AP and UT are controlled using MMSE (Minimum Mean Square Error), and LP (Liner Prediction).

A terminal's (AP or UT) array antenna trains the maximal directions on the

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

other terminal's (UT or AP) in 71% and the minimal directions in 39%. Therefore, the probability of facing maximal direction each other is 50%. The threshold is settled under the RSSI in case of maximal direction facing. The Probability of RSSI is shown in Fig.1.

## 4. Evaluation

We evaluated the proposed scheme in terms of the rate of the deleted RSSIs near threshold and the conditional mutual information.

$P_a$ means antenna pattern limited rate. It is a ratio of selecting antenna pattern that RSSIs are high or low values. $P_d$ means RSSI deleted rate near the threshold.

The procedure of the key generation is shown in Fig. 2. BCH (31, 21, 5) double error correction code is utilized to decrease disagreement rate. AP makes a syndrome generated from key bits and sends it to UT. UT compares it with its own syndrome. If the syndromes are not same, UT corrects the disagreement bit according to the syndromes.

Privacy Amplification (PA) is also utilized to increase the conditional mutual information. Degeneracy rate of the PA is 1/8. Antenna pattern under the condition as Table1 is shown in Fig3.

Disagreement rates in cases of ordinary scheme and proposed scheme are shown in Fig.4 and Fig.5 respectively. Proposed scheme need 0.6 of deleting rate for $10^{-5}$ of disagreement rate before FEC, however, ordinary scheme need 0.7. Therefore proposed scheme is effective to decrease RSSI measurement times.

## 5. Safety Evaluation

We simulate mutual information of the regular AP and UT to select the parameter sets ($P_a$ and $P_d$) which satisfy 0.90 bit/round. Fig.6 show mutual information as color bar under the simulation condition in Table 1. Parameter sets A, B, C and D shown in Table2 and Fig6 satisfied key agreement rate between AP and UT. We also simulate the conditional mutual information with TP location. The rate of TP location where the information is less than 0.90 bit /round is used to evaluate the safety. The location rates by parameter sets A, B, C are almost 53%, but the rate by parameter set D is 65%. Therefore parameter sets A, B, C are selected.

The conditional mutual information map is used to evaluate parameter set. The map shows the conditional mutual information with TP location as color. The room is 10X10m size and AP and UT are settled at position of (0m, 0m) and (2m, 2m). Fig.7 is the map in case of parameters C. The unsafely place can be decrease with FEC and PA.

## 6. Conclusion

A key generation technique using array antenna beam selection was proposed to decrease the occurring probability of the RSSIs near the threshold.

Terminals estimate DOA and control direction when the keys are generated. We evaluate the key agreement probability and conditional mutual information and show the effect of the proposed scheme.

## References

[1] M.MAEDA, T. Iwai, S. Aikawa, "SAFETY EVALUATION OF A KEY GENERATION SPEED-UP TECHNIQUE FOR SECRET KEY AGREEMENT SCHEME USING ARRAY ANTENNA, "  AP-RASC2010.

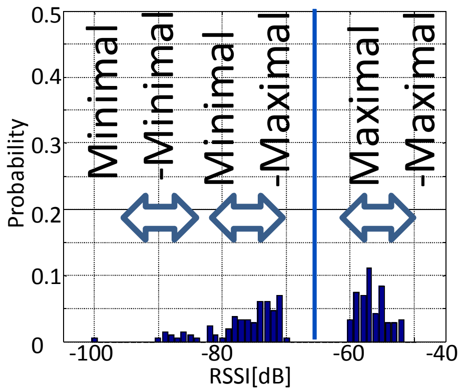

Fig. 1 Probability of RSSIs

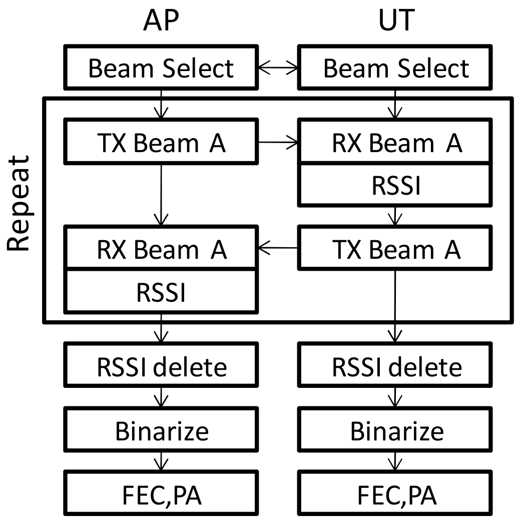

Fig. 2 Key Generation Procedure

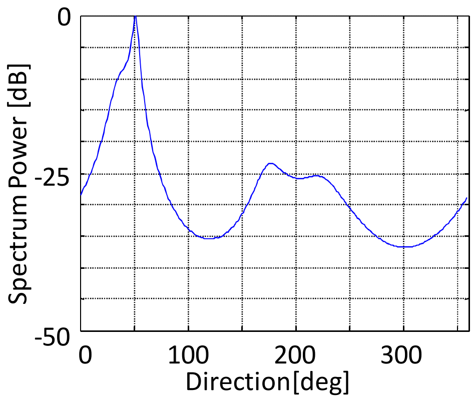

Fig.3 Spectrum Strength
by LP Estimation of Angular

Table 1 Simulation Condition

| | |
|---|---|
| Room size | 10m × 8m |
| AP position | (0 m ,0 m) center |
| UT position | ( 2.0 m , 2.0 m ) |
| Frequency | 2.4 GHz |
| Key Length | 128bit |
| AP,UT | 3 Circular Array |
| PA degeneration | 1/8 |
| Tapping Point | omni direction |
| FEC | BCH(31 , 21 , 5) |

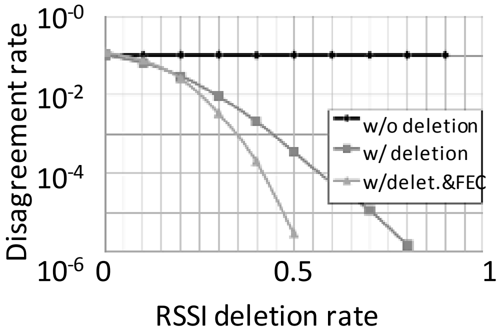

Fig.4 Disagreement rate
vs. RSSI deletion rate (ordinary)

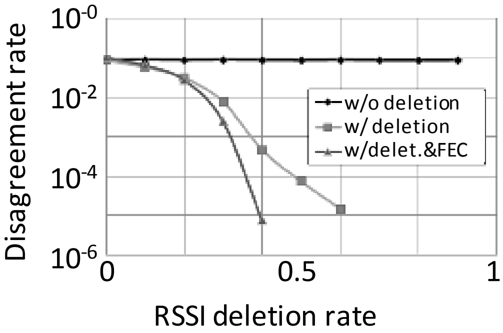

Fig.5 Disagreement rate
vs. RSSI deletion rate (proposed)

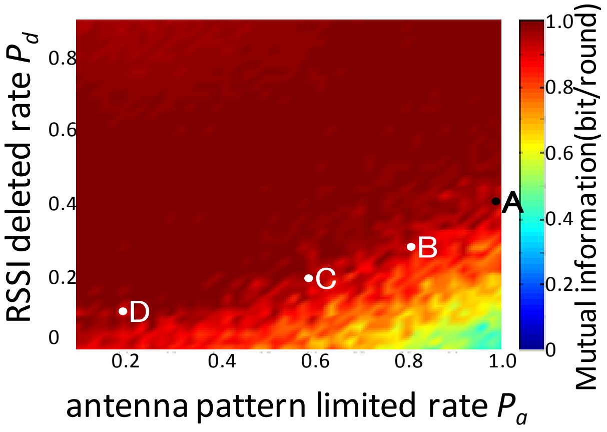

Fig.6Mutual information by Pa and Pd

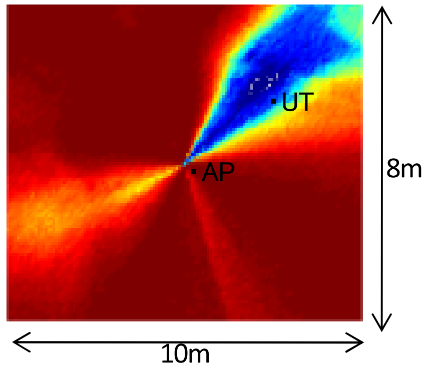

Fig.7 Conditional mutual information
in simulation environment

Table2 Parameter sets

| | $P_a$ | $P_d$ |
|---|---|---|
| A | 100% | 40% |
| B | 80% | 30% |
| C | 60% | 20% |
| D | 20% | 10% |